Documentación de StorageGRID 11,8

StorageGRID 11.8

NetApp
March 19, 2024

Tabla de contenidos

Documentación de StorageGRID 11,8

Dispositivos StorageGRID

Vaya a. "Documentación del dispositivo StorageGRID" Para saber cómo instalar, configurar y mantener dispositivos de almacenamiento y servicios de StorageGRID.

Notas de la versión

Obtenga información específica de versión sobre problemas solucionados y problemas conocidos.

Inicie sesión en el sitio de soporte de NetApp en "Vea o descargue un archivo PDF" Que contiene las notas de la versión de StorageGRID 11,8.

Comience a utilizar un sistema StorageGRID

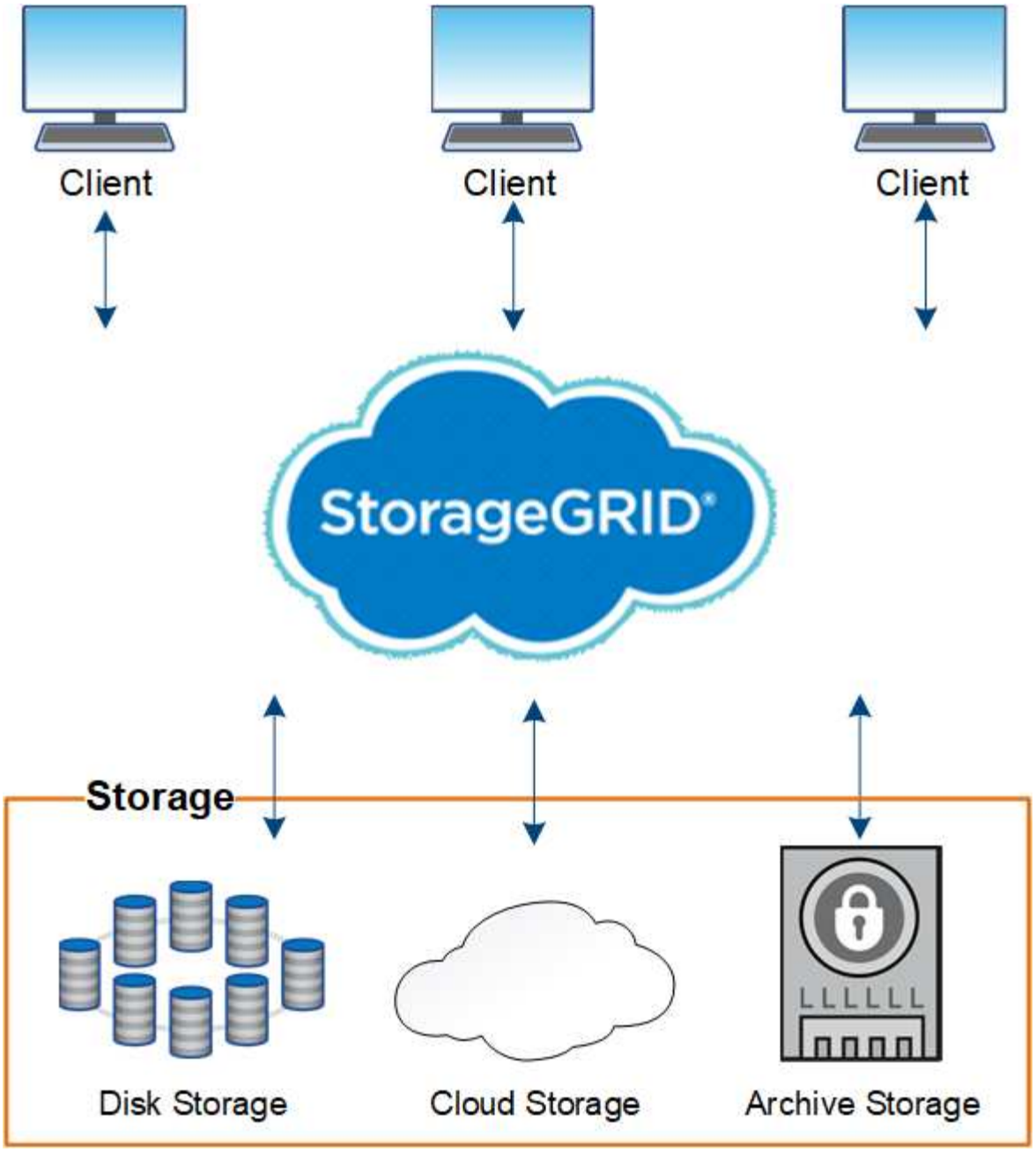
Más información sobre StorageGRID

¿Qué es StorageGRID?

NetApp® StorageGRID® es una suite de almacenamiento de objetos definido por software que admite una amplia gama de casos de uso en entornos multicloud públicos, privados e híbridos. StorageGRID ofrece compatibilidad nativa con la API de Amazon S3 y proporciona innovaciones líderes en el sector, como la gestión automatizada del ciclo de vida, para almacenar, proteger y conservar datos no estructurados de forma rentable durante largos periodos.

StorageGRID proporciona almacenamiento seguro y duradero para datos no estructurados a escala. Las políticas integradas de gestión del ciclo de vida basadas en metadatos optimizan la ubicación de los datos a lo largo de toda su vida. El contenido se sitúa en la ubicación adecuada, en el momento justo y en el nivel de almacenamiento adecuado para reducir los costes.

StorageGRID se compone de nodos heterogéneos, redundantes y distribuidos geográficamente, que se pueden integrar con las aplicaciones de cliente existentes y de próxima generación.



La compatibilidad con los nodos de archivo está obsoleta y se eliminará en una versión futura. El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades.

Ventajas de StorageGRID

Algunas de las ventajas del sistema StorageGRID son:

- Escalable de forma masiva y fácil de usar un repositorio de datos distribuido geográficamente para datos no estructurados.
- Protocolos de almacenamiento de objetos estándar:
  - Simple Storage Service (S3) de Amazon Web Services

- OpenStack Swift

> Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.

- Habilitado para el cloud híbrido. La gestión del ciclo de vida de la información (ILM) basada en políticas almacena objetos en clouds públicos, incluidos Amazon Web Services (AWS) y Microsoft Azure. Los servicios de la plataforma StorageGRID permiten la replicación de contenido, la notificación de eventos y la búsqueda de metadatos de objetos almacenados en clouds públicos.
- Protección de datos flexible que garantiza la durabilidad y la disponibilidad. Se pueden proteger los datos mediante replicación y códigos de borrado por capas. La verificación de datos en reposo y en tránsito garantiza la integridad a largo plazo.
- Gestión dinámica del ciclo de vida de los datos para ayudar a gestionar los costes de almacenamiento. Puede crear reglas de ILM que gestionen el ciclo de vida de los datos a nivel del objeto, personalizando la localidad de los datos, la durabilidad, el rendimiento, el coste y y tiempo de retención.
- Alta disponibilidad del almacenamiento de datos y algunas funciones de gestión, con equilibrio de carga integrado para optimizar la carga de datos en todos los recursos de StorageGRID.
- Compatibilidad con varias cuentas de inquilino de almacenamiento para segregar los objetos almacenados en su sistema por diferentes entidades.
- Numerosas herramientas para supervisar el estado del sistema StorageGRID, incluidas un completo sistema de alertas, un panel gráfico y Estados detallados para todos los nodos y sitios.
- Soporte para puesta en marcha basada en software o hardware. Puede implementar StorageGRID en cualquiera de los siguientes elementos:
  - Equipos virtuales que se ejecutan en VMware.
  - Motores de contenedor en hosts Linux.
  - Dispositivos a medida StorageGRID.
    - Los dispositivos de almacenamiento proporcionan almacenamiento de objetos.
    - Los dispositivos de servicios proporcionan servicios de administración de grid y equilibrio de carga.
- Cumplir con los requisitos de almacenamiento pertinentes de estas normativas:
  - Comisión de valores y Bolsa (SEC) en 17 CFR, sección 240.17a-4(f), que regula a los miembros de bolsa, corredores o distribuidores.
  - Ley de la Autoridad reguladora de la Industria financiera (FINRA), regla 4511(c), que desafía el formato y los requisitos de medios de la normativa SEC 17a-4(f).
  - Commodity Futures Trading Commission (CFTC) en la regulación 17 CFR, sección 1.31(c)-(d), que regula el comercio de futuros de materias primas.
- Operaciones de mantenimiento y actualización no disruptivas. Mantenga el acceso al contenido durante los procedimientos de actualización, ampliación, retirada y mantenimiento.
- Gestión de identidades federada. Se integra con Active Directory, OpenLDAP u Oracle Directory Service para la autenticación de usuarios. Admite el inicio de sesión único (SSO) con el estándar Security Assertion Markup Language 2.0 (SAML 2.0) para intercambiar datos de autenticación y autorización entre StorageGRID y Active Directory Federation Services (AD FS).

Clouds híbridos con StorageGRID

Utilice StorageGRID en una configuración de cloud híbrido implementando gestión de

datos condicionada por políticas para almacenar objetos en pools de almacenamiento de cloud, aprovechando los servicios de plataforma StorageGRID y organizando los datos en niveles desde ONTAP a StorageGRID con FabricPool de NetApp.

Pools de almacenamiento en cloud

Los pools de almacenamiento en cloud permiten almacenar objetos fuera del sistema StorageGRID. Por ejemplo, es posible que desee mover objetos a los que se accede con poca frecuencia a un almacenamiento en cloud de bajo coste, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o el nivel de acceso de archivado en el almacenamiento de Microsoft Azure Blob. O bien, es posible que desee mantener un backup en cloud de objetos de StorageGRID, que pueden utilizarse para recuperar datos perdidos debido a un fallo del volumen de almacenamiento o del nodo de almacenamiento.

También es compatible el almacenamiento de partners de terceros, incluido el almacenamiento en disco y en cinta.

> No se puede usar Cloud Storage Pools con FabricPool debido a la latencia añadida de recuperar un objeto del destino de Cloud Storage Pool.

Servicios de plataforma S3

Los servicios de plataforma S3 le dan la posibilidad de usar servicios remotos como extremos para la replicación de objetos, notificaciones de eventos o la integración de búsquedas. Los servicios de plataforma operan con independencia de las reglas de ILM del grid, y se habilitan para bloques individuales de S3. Se admiten los siguientes servicios:

- El servicio de replicación de CloudMirror hace automáticamente mirroring de los objetos especificados en un bloque de S3 de destino, que puede estar en un segundo sistema Amazon S3 o en un segundo sistema StorageGRID.
- El servicio de notificación de eventos envía mensajes sobre las acciones especificadas a un punto final externo que admite la recepción de eventos de Simple Notification Service (Amazon SNS).
- El servicio de integración de búsqueda envía metadatos de objetos a un servicio de Elasticsearch externo, lo que permite buscar, visualizar y analizar los metadatos con herramientas de terceros.

Por ejemplo, podría usar la replicación de CloudMirror para reflejar registros de clientes específicos en Amazon S3 y, a continuación, aprovechar los servicios de AWS para realizar análisis de los datos.

Organización en niveles de datos de ONTAP mediante FabricPool

Puede reducir el coste del almacenamiento de ONTAP organizando en niveles los datos en StorageGRID utilizando FabricPool. FabricPool permite organizar los datos en niveles de forma automática en niveles de almacenamiento de objetos de bajo coste, tanto dentro como fuera de las instalaciones.

A diferencia de las soluciones de organización por niveles manual, FabricPool reduce el coste total de propiedad mediante la automatización de la organización en niveles de los datos para reducir el coste del almacenamiento. Ofrece las ventajas de la rentabilidad del cloud organizando en niveles en clouds públicos y privados incluyendo StorageGRID.

Información relacionada

- "¿Qué es Cloud Storage Pool?"
- "Gestione los servicios de la plataforma"

- "Configure StorageGRID para FabricPool"

Arquitectura de StorageGRID y topología de red

Un sistema StorageGRID consta de varios tipos de nodos de grid en uno o varios sitios de centros de datos.

Consulte "descripciones de los tipos de nodos de cuadrícula".

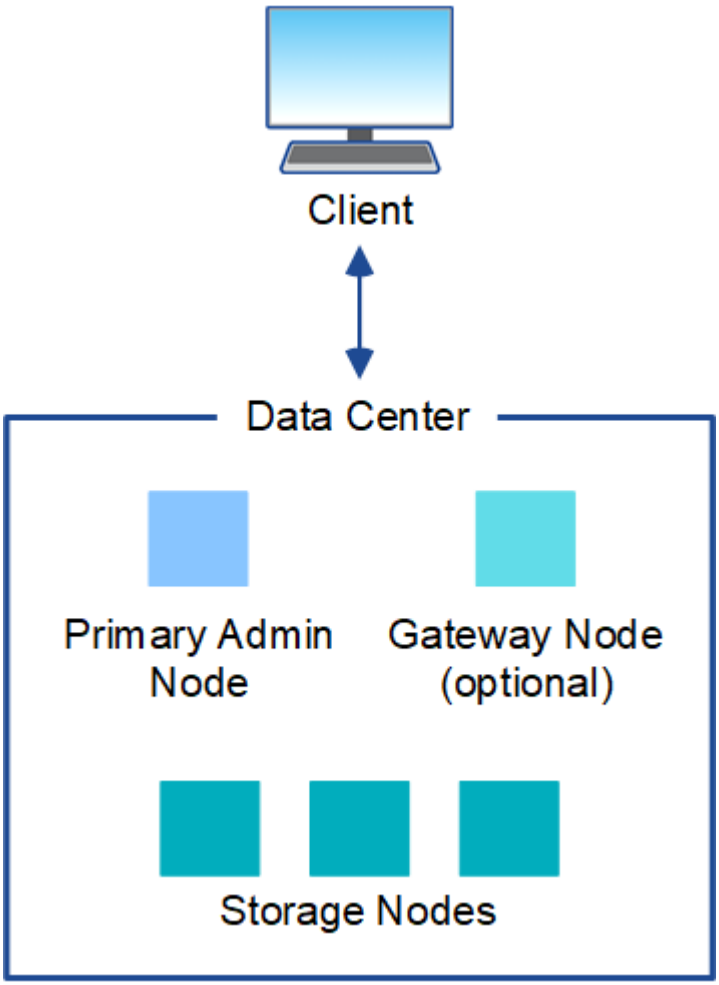
Para obtener información adicional sobre la topología de red, los requisitos y las comunicaciones de grid de StorageGRID, consulte "Directrices sobre redes".

Topologías de puesta en marcha

El sistema StorageGRID se puede poner en marcha en un solo centro de datos o en varios sitios de centros de datos.

Sitio único

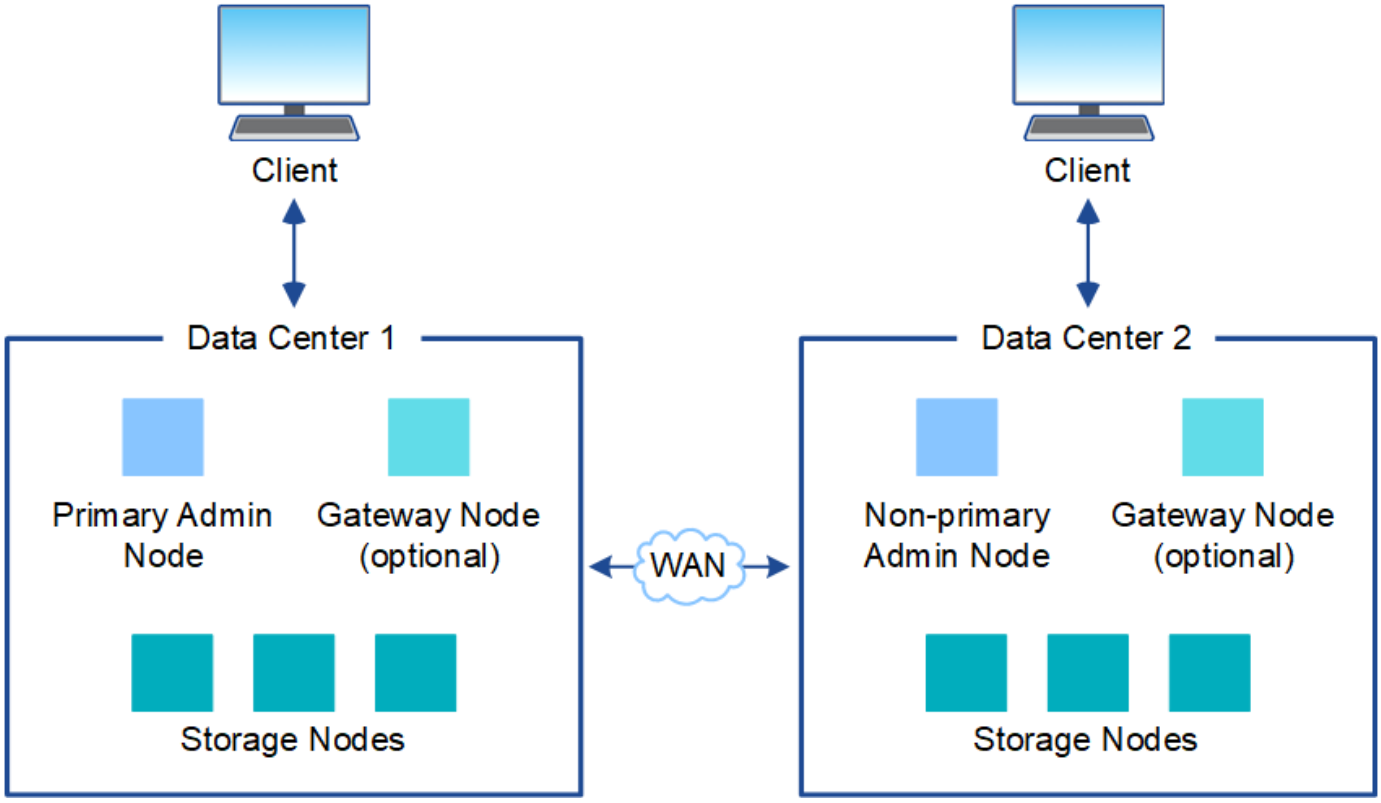
En una puesta en marcha con un único sitio, la infraestructura y las operaciones del sistema StorageGRID están centralizadas.



Múltiples sitios

En una implementación con varios sitios, se pueden instalar diferentes tipos y números de recursos de StorageGRID en cada sitio. Por ejemplo, es posible que se necesite más almacenamiento en un centro de datos que en otro.

Con frecuencia, se ubican en distintas ubicaciones geográficas en diferentes dominios de fallo, como una línea de fallo de terremotos o un flujo de inundación. El uso compartido de datos y la recuperación ante desastres se consigue mediante la distribución automatizada de datos a otros sites.



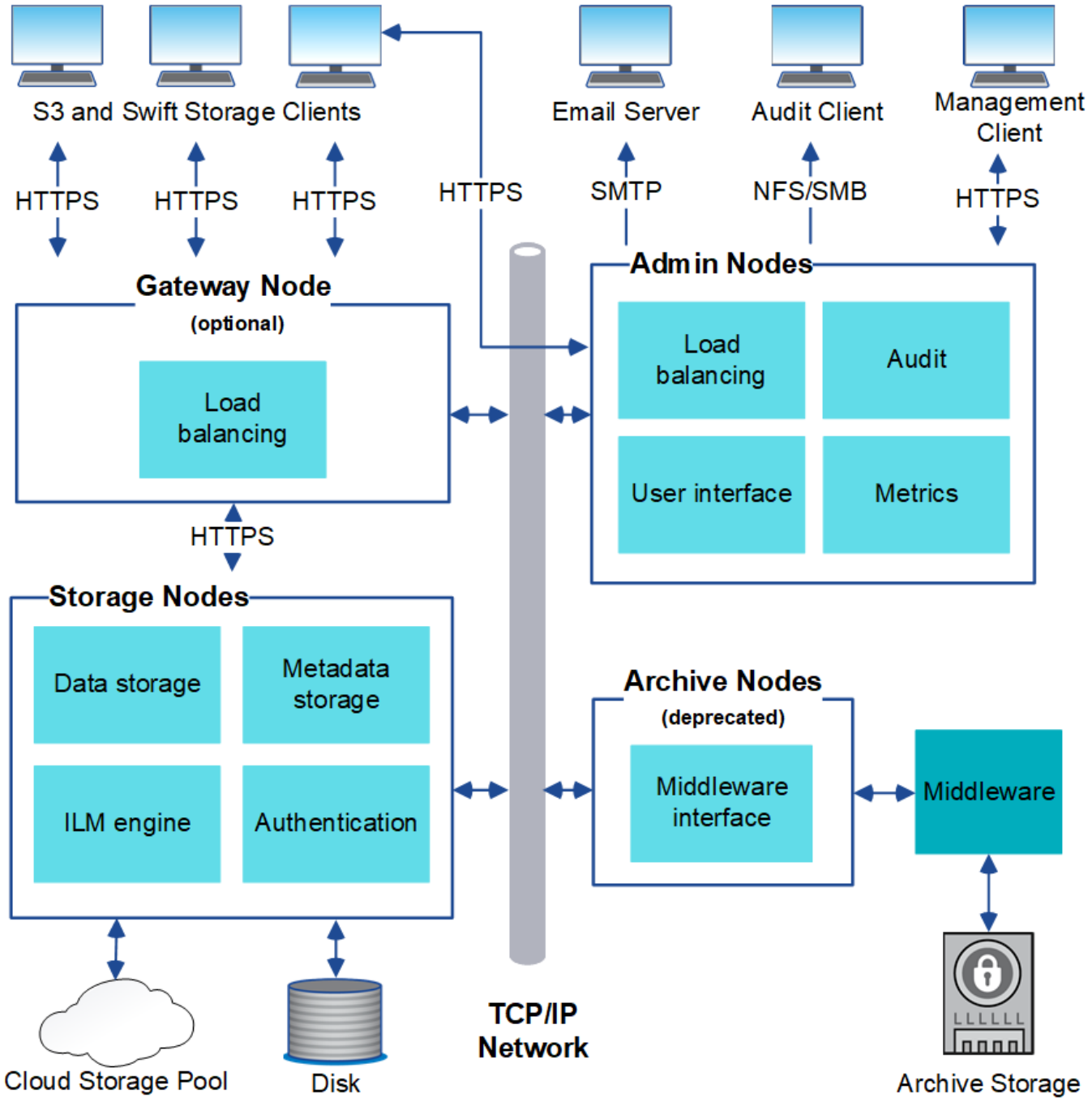
También pueden existir varios sitios lógicos en un único centro de datos y así permitir el uso de replicación distribuida y código de borrado para aumentar la disponibilidad y la resiliencia.

Redundancia de nodos de grid

En una puesta en marcha de un único sitio o de varios sitios, de manera opcional, puede incluir más de un nodo de administración o un nodo de puerta de enlace para obtener redundancia. Por ejemplo, puede instalar más de un nodo de administración en un solo sitio o en varios sitios. Sin embargo, cada sistema StorageGRID solo puede tener un nodo de administrador principal.

Arquitectura del sistema

Este diagrama muestra cómo se organizan los nodos de cuadrícula en un sistema StorageGRID.



Los clientes de S3 y Swift almacenan y recuperan objetos en StorageGRID. Otros clientes se usan para enviar notificaciones por correo electrónico, para acceder a la interfaz de gestión de StorageGRID y, opcionalmente, para acceder al recurso compartido de auditoría.

Los clientes S3 y Swift pueden conectarse a un nodo de puerta de enlace o un nodo de administrador para usar la interfaz de equilibrio de carga en los nodos de almacenamiento. De manera alternativa, los clientes S3 y Swift pueden conectarse directamente a los nodos de almacenamiento mediante HTTPS.

Los objetos pueden almacenarse en StorageGRID en nodos de almacenamiento basados en software o en hardware, o en pools de almacenamiento en cloud, que constan de bloques S3 externos o contenedores de almacenamiento de Azure Blob.

Nodos de grid y servicios

Nodos y servicios de grid: Información general

El elemento básico de un sistema StorageGRID es el nodo de Grid. Los nodos contienen servicios, que son módulos de software que proporcionan un conjunto de funcionalidades a un nodo de grid.

Tipos de nodos de cuadrícula

El sistema StorageGRID utiliza cuatro tipos de nodos de grid:

Nodos de administración

Proporcione servicios de gestión como la configuración, la supervisión y el registro del sistema. Cuando inicia sesión en Grid Manager, se conecta a un nodo de administración. Cada grid debe tener un nodo de administrador primario y puede tener nodos de administrador no primarios adicionales para la redundancia. Puede conectarse a cualquier nodo de administrador y cada nodo de administrador muestra una vista similar del sistema StorageGRID. Sin embargo, se deben realizar los procedimientos de mantenimiento usando el nodo de administración principal.

Los nodos de administración también se pueden usar para equilibrar la carga del tráfico de clientes S3 y Swift.

Consulte "¿Qué es un nodo de administración?"

Nodos de almacenamiento

Gestione y almacene metadatos y datos de objetos. Cada sitio del sistema StorageGRID debe tener al menos tres nodos de almacenamiento.

Consulte "¿Qué es un nodo de almacenamiento?"

Nodos de puerta de enlace (opcionales)

Proporcione una interfaz de equilibrio de carga que las aplicaciones cliente puedan utilizar para conectarse a StorageGRID. Un equilibrador de carga dirige sin problemas a los clientes a un nodo de almacenamiento óptimo, de modo que el fallo de los nodos o incluso de todo un sitio sea transparente.

Consulte "¿Qué es un nodo de puerta de enlace?"

Nodos de archivado (obsoleto)

Proporcionar una interfaz opcional a través de la cual los datos de objetos se pueden archivar en cinta.

Consulte "¿Qué es un nodo de archivado?"

Nodos de hardware y software

Los nodos StorageGRID se pueden poner en marcha como nodos de dispositivo StorageGRID o como nodos basados en software.

Nodos del dispositivo StorageGRID

Los dispositivos de hardware StorageGRID están especialmente diseñados para su uso en un sistema StorageGRID. Algunos dispositivos se pueden usar como nodos de almacenamiento. Otros dispositivos se pueden usar como nodos de administrador o nodos de puerta de enlace. Puede combinar nodos de dispositivos con nodos basados en software o poner en marcha grids de dispositivo completamente diseñados

que no tengan dependencias en hipervisores externos, almacenamiento ni hardware de computación.

Consulte lo siguiente para obtener más información sobre los dispositivos disponibles:

- "Documentación del dispositivo StorageGRID"
- "Hardware Universe de NetApp"

Nodos basados en software

Los nodos de grid basados en software se pueden poner en marcha como máquinas virtuales de VMware o en motores de contenedor en un host Linux.

- Máquina virtual (VM) en VMware vSphere: Consulte "Instale StorageGRID en VMware".
- En un motor de contenedores en Red Hat Enterprise Linux: Consulte "Instalar StorageGRID en Red Hat Enterprise Linux".
- Dentro de un motor de contenedores en Ubuntu o Debian: Consulte "Instalar StorageGRID en Ubuntu o Debian".

Utilice la "Herramienta de matriz de interoperabilidad de NetApp (IMT)" para determinar las versiones compatibles.

Durante la instalación inicial de un nuevo nodo de almacenamiento basado en software, puede especificar que solo se utilice para "almacenar metadatos".

Servicios de StorageGRID

A continuación, se muestra una lista completa de los servicios StorageGRID.

Servicio	Descripción	Ubicación
Promotor de servicios de cuenta	Proporciona una interfaz para que el servicio Load Balancer pueda consultar el Servicio de cuenta en hosts remotos y proporciona notificaciones de cambios de configuración de Load Balancer Endpoint al servicio Load Balancer.	Servicio de equilibrio de carga en los nodos de administración y de puerta de enlace
ADC (Controlador de dominio administrativo)	Mantiene información de topología, proporciona servicios de autenticación y responde a las consultas de los servicios LDR y CMN.	Al menos tres nodos de almacenamiento que contienen el servicio ADC en cada sitio
AMS (Sistema de Gestión de Auditoría)	Supervisa y registra todos los eventos y transacciones auditados del sistema en un archivo de registro de texto.	Nodos de administración
ARCO (Archivo)	Ofrece la interfaz de gestión con la que se configuran las conexiones a un almacenamiento de archivado externo, como cloud a través de una interfaz S3 o una cinta a través del middleware TSM.	Nodos de archivado

Servicio	Descripción	Ubicación
Cassandra Reaper	Realiza reparaciones automáticas de metadatos de objetos.	Nodos de almacenamiento
Servicio CHUNK	Gestiona datos codificados de borrado y fragmentos de paridad.	Nodos de almacenamiento
CMN (nodo de gestión de configuración)	Gestiona las configuraciones de todo el sistema y las tareas de grid. Cada grid tiene un servicio CMN.	Nodo de administrador principal
DDS (almacén de datos distribuidos)	Interactúa con la base de datos de Cassandra para gestionar los metadatos de objetos.	Nodos de almacenamiento
DMV (Data Mover)	Mueve los datos a extremos de cloud.	Nodos de almacenamiento
IP dinámica (dynip)	Supervisa la cuadrícula para los cambios dinámicos de IP y actualiza las configuraciones locales.	Todos los nodos
Grafana	Se utiliza para la visualización de métricas en Grid Manager.	Nodos de administración
Alta disponibilidad	Gestiona las IP virtuales de alta disponibilidad en los nodos configurados en la página High Availability Groups. Este servicio también se conoce como servicio de keepalived.	Nodos de administración y puerta de enlace
Identidad (no)	Federe las identidades de usuario de LDAP y Active Directory.	Nodos de almacenamiento que usan el servicio ADC
Árbitro Lambda	Gestiona solicitudes S3 Select ObjectContent.	Todos los nodos
Equilibrador de carga (nginx-gw)	Proporciona el equilibrio de carga del tráfico de S3 y Swift desde los clientes a los nodos de almacenamiento. El servicio Load Balancer se puede configurar a través de la página de configuración Load Balancer Endpoints. Este servicio también se conoce como servicio nginx-gw.	Nodos de administración y puerta de enlace
LDR (enrutador de distribución local)	Gestiona el almacenamiento y la transferencia de contenido dentro de la cuadrícula.	Nodos de almacenamiento

Servicio	Descripción	Ubicación
Daemon de Control de Servicio de Información MISCd	Proporciona una interfaz para consultar y gestionar servicios en otros nodos y para gestionar configuraciones de entorno en el nodo, como consultar el estado de los servicios que se ejecutan en otros nodos.	Todos los nodos
nginx	Actúa como mecanismo de autenticación y comunicación segura para que varios servicios de grid (como Prometheus y Dynamic IP) puedan comunicarse con servicios de otros nodos a través de las API HTTPS.	Todos los nodos
nginx-gw	Activa el servicio Load Balancer.	Nodos de administración y puerta de enlace
NMS (Sistema de gestión de redes)	Activa las opciones de supervisión, generación de informes y configuración que se muestran a través de Grid Manager.	Nodos de administración
Persistencia	Administra los archivos del disco raíz que deben persistir durante un reinicio.	Todos los nodos
Prometheus	Recopila métricas de series temporales de los servicios en todos los nodos.	Nodos de administración
RSM (máquina de estado replicado)	Garantiza que las solicitudes de servicio de la plataforma se envíen a sus respectivos extremos.	Nodos de almacenamiento que usan el servicio ADC
SSM (Monitor de estado del servidor)	Supervisa las condiciones del hardware e informa al servicio NMS.	Hay una instancia presente en cada nodo de cuadrícula
Recolector de rastreo	Realiza la recogida de seguimiento para recopilar información que el soporte técnico utiliza. El servicio de recopilación de rastreo utiliza el software Jaeger de código abierto.	Nodos de administración

¿Qué es un nodo de administración?

Los nodos de administración, que proporcionan servicios de gestión como configuración, supervisión y registro del sistema. Los nodos de administración también se pueden usar para equilibrar la carga del tráfico de clientes S3 y Swift. Cada grid debe tener un nodo de administrador primario y puede tener cualquier cantidad de nodos de administrador no primarios por motivos de redundancia.

Diferencias entre los nodos de administración primario y no principal

Cuando inicia sesión en el administrador de grid o en el administrador de inquilinos, se conecta a un nodo de administración. Puede conectarse a cualquier nodo de administrador y cada nodo de administrador muestra una vista similar del sistema StorageGRID. Sin embargo, el nodo de administración principal proporciona más funcionalidad que los nodos de administración no principales. Por ejemplo, la mayoría de los procedimientos de mantenimiento se deben realizar desde los nodos de administración principales.

En la tabla se resumen las capacidades de los nodos ADMIN principales y no principales.

Funcionalidades	Nodo de administrador principal	Nodo de administrador no primario
Incluye la AMS servicio	Sí	Sí
Incluye la CMN servicio	Sí	No
Incluye la NMS servicio	Sí	Sí
Incluye la Prometheus servicio	Sí	Sí
Incluye la SSM servicio	Sí	Sí
Incluye la Equilibrador de carga y.. Alta disponibilidad servicios	Sí	Sí
Compatible con Interfaz del programa de aplicaciones de gestión (api de gestión)	Sí	Sí
Se puede utilizar para todas las tareas de mantenimiento relacionadas con la red, por ejemplo, el cambio de dirección IP y la actualización de servidores NTP	Sí	No
Puede realizar un reequilibrio de EC tras la ampliación del nodo de almacenamiento	Sí	No
Se puede utilizar para el procedimiento de restauración de volúmenes	Sí	Sí
Puede recoger archivos de registro y datos del sistema de uno o más nodos	Sí	No
Envía notificaciones de alerta, paquetes AutoSupport y capturas SNMP e informa	Sí. Actúa como el remitente preferido.	Sí. Actúa como remitente en espera.

Nodo de administración de remitente preferido

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, las capturas

e informes SNMP y las notificaciones de alarmas heredadas.

En operaciones normales del sistema, solo el remitente preferido envía notificaciones. Sin embargo, el resto de los nodos de administración supervisan el remitente preferido. Si se detecta un problema, otros nodos de administración actúan como *remitentes en espera*.

Es posible que se envíen varias notificaciones en los siguientes casos:

- Si los nodos de administración pasan a ser “indistribuidos” entre sí, tanto el remitente preferido como los remitentes en espera intentarán enviar notificaciones, y es posible que se reciban varias copias de las notificaciones.
- Si el remitente en espera detecta problemas con el remitente preferido y comienza a enviar notificaciones, es posible que el remitente preferido recupere su capacidad para enviar notificaciones. Si esto ocurre, es posible que se envíen notificaciones duplicadas. El remitente en espera dejará de enviar notificaciones cuando ya no detecte errores en el remitente preferido.

> Cuando prueba los paquetes AutoSupport, todos los nodos de administración envían la prueba. Cuando prueba las notificaciones de alerta, debe iniciar sesión en cada nodo de administrador para verificar la conectividad.

Servicios primarios para nodos de administración

En la siguiente tabla se muestran los servicios principales de los nodos de administrador; sin embargo, esta tabla no enumera todos los servicios de nodo.

Servicio	Función de la tecla
Sistema de Gestión de Auditoría (AMS)	Realiza un seguimiento de la actividad y los eventos del sistema.
Nodo de gestión de configuración (CMN)	Gestiona la configuración en todo el sistema.
[[alta disponibilidad]]Alta disponibilidad	Administra direcciones IP virtuales de alta disponibilidad para grupos de nodos de administración y nodos de puerta de enlace. **Nota:** este servicio también se encuentra en los nodos Gateway.
Equilibrador de carga	Proporciona el equilibrio de carga del tráfico de S3 y Swift desde los clientes a los nodos de almacenamiento. **Nota:** este servicio también se encuentra en los nodos Gateway.
Interfaz de programa de aplicaciones de gestión (mgmt-api)	Procesa las solicitudes de la API de gestión de grid y la API de gestión de inquilinos.
Sistema de gestión de redes (NMS)	Proporciona funcionalidad para Grid Manager.

Servicio	Función de la tecla
Prometeo	Recopila y almacena métricas de series temporales de los servicios en todos los nodos.
Monitor de estado del servidor (SSM)	Supervisa el sistema operativo y el hardware subyacente.

¿Qué es un nodo de almacenamiento?

Los nodos de almacenamiento gestionan y almacenan metadatos y datos de objetos. Los nodos de almacenamiento incluyen los servicios y procesos necesarios para almacenar, mover, verificar y recuperar datos y metadatos de objetos en el disco.

Cada sitio del sistema StorageGRID debe tener al menos tres nodos de almacenamiento.

Tipos de nodos de almacenamiento

Todos los nodos de almacenamiento que se instalaron antes de StorageGRID 11,8 almacenan tanto los objetos como los metadatos de esos objetos. A partir de StorageGRID 11,8, se puede elegir el tipo de nodo de almacenamiento para los nuevos nodos de almacenamiento basados en software:

Nodos de almacenamiento de objetos y metadatos

De manera predeterminada, todos los nodos de almacenamiento nuevos instalados en StorageGRID 11,8 almacenarán objetos y metadatos.

Nodos de almacenamiento solo de metadatos (solo nodos basados en software)

Puede especificar que se utilice un nuevo nodo de almacenamiento basado en software para almacenar solo metadatos. También puede añadir un nodo de almacenamiento basado en software solo de metadatos al sistema StorageGRID durante la ampliación del sistema StorageGRID.

> ⓘ Solo puede seleccionar el tipo de nodo de almacenamiento cuando se instala inicialmente el nodo basado en software o cuando se instala el nodo basado en software durante la ampliación del sistema StorageGRID. No puede cambiar el tipo después de completar la instalación del nodo.

Por lo general, no es necesario instalar un nodo solo de metadatos. Sin embargo, el uso de un nodo de almacenamiento exclusivamente para metadatos puede tener sentido si el grid almacena una gran cantidad de objetos pequeños. La instalación de capacidad de metadatos dedicada proporciona un mejor equilibrio entre el espacio necesario para una gran cantidad de objetos pequeños y el espacio necesario para los metadatos de todos esos objetos.

Al instalar un grid con nodos solo de metadatos basados en software, el grid también debe contener un número mínimo de nodos para el almacenamiento de objetos:

- Para un grid de sitio único, hay al menos dos nodos de almacenamiento configurados para objetos y metadatos.
- Para un grid de varios sitios, al menos un nodo de almacenamiento por sitio está configurado para objetos y metadatos.

Los nodos de almacenamiento basados en software muestran una indicación solo de metadatos para cada

nodo solo de metadatos en todas las páginas que enumeran el tipo de nodo de almacenamiento.

Servicios principales para nodos de almacenamiento

En la siguiente tabla se muestran los servicios principales de los nodos de almacenamiento; sin embargo, esta tabla no enumera todos los servicios de los nodos.

> Algunos servicios, como el servicio ADC y el servicio RSM, normalmente solo existen en tres nodos de almacenamiento de cada sitio.

Servicio	Función de la tecla
Cuenta (acct)	Administra cuentas de arrendatario.
Controlador de dominio administrativo (ADC)	Mantiene la topología y la configuración en todo el grid. **Detalles** El servicio de controlador de dominio administrativo (ADC) autentica los nodos de grid y sus conexiones entre sí. El servicio ADC está alojado en un mínimo de tres nodos de almacenamiento en un sitio. El servicio ADC mantiene la información de topología, incluida la ubicación y disponibilidad de los servicios. Cuando un nodo de cuadrícula requiere información de otro nodo de cuadrícula o una acción que debe realizar otro nodo de cuadrícula, se pone en contacto con un servicio de ADC para encontrar el mejor nodo de cuadrícula para procesar su solicitud. Además, el servicio ADC conserva una copia de los paquetes de configuración de la implementación de StorageGRID, lo que permite que cualquier nodo de grid recupere la información de configuración actual. Para facilitar las operaciones distribuidas e iaterradas, cada servicio ADC sincroniza certificados, paquetes de configuración e información sobre servicios y topología con los otros servicios ADC del sistema StorageGRID. En general, todos los nodos de grid mantienen una conexión al menos a un servicio de ADC. De este modo se garantiza que los nodos grid accedan siempre a la información más reciente. Cuando los nodos de grid se conectan, almacenan en caché los certificados de otros nodos de grid, lo que permite que los sistemas continúen funcionando con los nodos de grid conocidos incluso cuando un servicio ADC no está disponible. Los nuevos nodos de grid solo pueden establecer conexiones mediante un servicio ADC. La conexión de cada nodo de cuadrícula permite al servicio ADC recopilar información de topología. Esta información sobre los nodos de grid incluye la carga de CPU, el espacio en disco disponible (si tiene almacenamiento), los servicios admitidos y el ID de sitio del nodo de grid. Otros servicios solicitan al servicio ADC información de topología a través de consultas de topología. El servicio ADC responde a cada consulta con la información más reciente recibida del sistema StorageGRID.

Servicio	Función de la tecla
Cassandra	Almacena y protege los metadatos de objetos.
Cassandra Reaper	Realiza reparaciones automáticas de metadatos de objetos.
Segmento	Gestiona datos codificados de borrado y fragmentos de paridad.
Transmisor de datos (dmv)	Transfiere datos a Cloud Storage Pools.
Almacén de datos distribuidos (DDS)	Supervisa el almacenamiento de metadatos de objetos. **Detalles** Cada nodo de almacenamiento incluye el servicio de almacén de datos distribuidos (DDS). Este servicio interactúa con la base de datos Cassandra para realizar tareas en segundo plano sobre los metadatos de objetos almacenados en el sistema StorageGRID. El servicio DDS realiza un seguimiento del número total de objetos ingeridos en el sistema StorageGRID, así como del número total de objetos ingeridos a través de cada una de las interfaces compatibles del sistema (S3 o Swift).
Identidad (no)	Federe las identidades de usuario de LDAP y Active Directory.

Servicio	Función de la tecla
Router de distribución local (LDR)	Procesa las solicitudes del protocolo de almacenamiento de objetos y gestiona los datos de objetos en el disco.

Servicio	Función de la tecla
Máquina de estado replicada (RSM)	Garantiza que las solicitudes de servicios de la plataforma S3 se envíen a sus respectivos puntos finales.
Monitor de estado del servidor (SSM)	Supervisa el sistema operativo y el hardware subyacente.

parte del trabajo duro del sistema StorageGRID al manejar las cargas de transferencia de datos y las funciones de tráfico de datos.

El servicio LDR se encarga de las siguientes tareas:

- Consultas
- Actividad de gestión de la vida útil de la información (ILM)
- Eliminación de objetos
- Almacenamiento de datos de objetos
- Transferencias de datos de objetos desde otro servicio LDR (nodo de almacenamiento)
- Gestión del almacenamiento de datos
- Interfaces de protocolo (S3 y Swift)

El servicio LDR también asigna cada objeto S3 y Swift a su GUID único.

Almacenes de objetos

El almacenamiento de datos subyacente de un servicio LDR se divide en un número fijo de almacenes de objetos (también conocidos como volúmenes de almacenamiento). Cada almacén de objetos es un punto de montaje independiente.

Los almacenes de objetos de un nodo de almacenamiento se identifican mediante un número hexadecimal entre 0000 y 002F, que se conoce como el ID del volumen. El espacio se reserva en el primer almacén de objetos (volumen 0) para los metadatos de objetos en una base de datos de Cassandra; todo el espacio restante en ese volumen se usa para los datos de objetos. El resto de almacenes de objetos se utilizan exclusivamente para datos de objetos, lo que incluye copias replicadas y fragmentos codificados para borrado.

Protección de metadatos

StorageGRID almacena metadatos de objetos en una base de datos de Cassandra, que se conecta con el servicio LDR.

Para garantizar la redundancia y, por lo tanto, la protección contra la pérdida, se mantienen tres copias de metadatos de objetos en cada sitio. Esta replicación no puede configurarse y se realiza de forma automática. Para obtener más información, consulte "Gestione el almacenamiento de metadatos de objetos".

¿Qué es un nodo de puerta de enlace?

Los nodos de puerta de enlace proporcionan una interfaz de equilibrio de carga dedicada que las aplicaciones cliente S3 y Swift pueden utilizar para conectarse con StorageGRID. El equilibrio de carga maximiza la velocidad y la capacidad de conexión mediante la distribución de la carga de trabajo entre varios nodos de almacenamiento. Los nodos de puerta de enlace son opcionales.

El servicio de equilibrador de carga de StorageGRID se proporciona en todos los nodos de administración y todos los nodos de puerta de enlace. Realiza la terminación de las solicitudes de cliente de Seguridad de capa de transporte (TLS), inspecciona las solicitudes y establece nuevas conexiones seguras a los nodos de almacenamiento. El servicio de equilibrador de carga dirige sin problemas a los clientes a un nodo de almacenamiento óptimo, de modo que el fallo de nodos o incluso un sitio completo sea transparente.

Configure uno o más puntos finales del equilibrador de carga para definir el protocolo de puerto y red (HTTPS o HTTP) que las solicitudes de cliente entrantes y salientes utilizarán para acceder a los servicios del equilibrador de carga en los nodos de gateway y administración. El extremo de equilibrio de carga también define el tipo de cliente (S3 o Swift), el modo de enlace y, opcionalmente, una lista de inquilinos permitidos o bloqueados. Consulte "Consideraciones que tener en cuenta al equilibrio de carga".

Según sea necesario, puede agrupar las interfaces de red de varios nodos de gateway y nodos de administración en un grupo de alta disponibilidad (HA). Si falla la interfaz activa en el grupo HA, una interfaz de backup puede gestionar la carga de trabajo de la aplicación cliente. Consulte "Gestione grupos de alta disponibilidad".

Servicios principales para nodos de puerta de enlace

La siguiente tabla muestra los servicios principales para los nodos de puerta de enlace; sin embargo, esta tabla no enumera todos los servicios de nodo.

Servicio	Función de la tecla
Alta disponibilidad	Administra direcciones IP virtuales de alta disponibilidad para grupos de nodos de administración y nodos de puerta de enlace. **Nota:** este servicio también se encuentra en los nodos de administración.

Servicio	Función de la tecla
Equilibrador de carga	Proporciona un equilibrio de carga de capa 7 del tráfico de S3 y Swift de clientes a nodos de almacenamiento. Este es el mecanismo de equilibrio de carga recomendado. **Nota:** este servicio también se encuentra en los nodos de administración.
Monitor de estado del servidor (SSM)	Supervisa el sistema operativo y el hardware subyacente.

¿Qué es un nodo de archivado?

La compatibilidad con los nodos de archivo está obsoleta y se eliminará en una versión futura.

> La compatibilidad con los nodos de archivo está obsoleta y se eliminará en una versión futura. El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades.
>
> La opción Cloud Tiering - Simple Storage Service (S3) también queda obsoleta. Si está utilizando un nodo de archivado con esta opción, "Migre sus objetos a un pool de almacenamiento en la nube" en su lugar.
>
> Además, debe eliminar los nodos de archivado de las políticas de ILM activas en StorageGRID 11,7 o versiones anteriores. La eliminación de datos de objetos almacenados en nodos de archivado simplificará las actualizaciones futuras. Consulte "Trabajar con reglas de ILM y políticas de ILM".

Servicios principales para nodos de archivado

La siguiente tabla muestra los servicios principales para los nodos de archivado; sin embargo, esta tabla no enumera todos los servicios de nodo.

Servicio	Función de la tecla
Archivo (ARC)	Se comunica con un sistema de almacenamiento en cinta externo Tivoli Storage Manager (TSM).
Monitor de estado del servidor (SSM)	Supervisa el sistema operativo y el hardware subyacente.

Cómo StorageGRID gestiona los datos

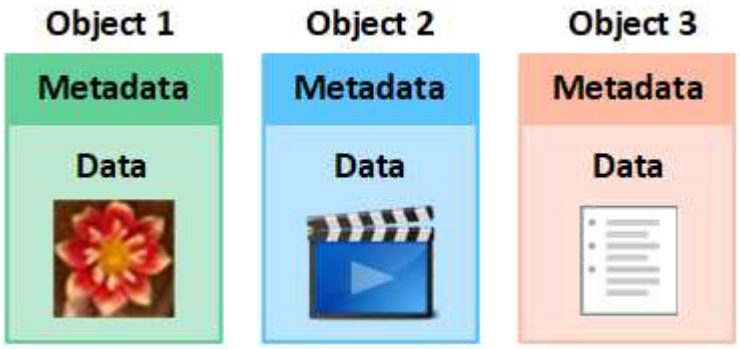
Qué es un objeto

Con el almacenamiento de objetos, la unidad de almacenamiento es un objeto, en lugar de un archivo o un bloque. A diferencia de la jerarquía de árbol de un sistema de

archivos o almacenamiento basado en bloques, el almacenamiento de objetos organiza los datos en un diseño plano y sin estructura.

El almacenamiento de objetos separa la ubicación física de los datos del método utilizado para almacenar y recuperar esos datos.

Cada objeto de un sistema de almacenamiento basado en objetos tiene dos partes: Datos de objetos y metadatos de objetos.



¿Qué son los datos de objetos?

Los datos del objeto pueden ser cualquier cosa; por ejemplo, una fotografía, una película o un registro médico.

¿Qué son los metadatos de objetos?

Los metadatos de objetos son cualquier información que describa un objeto. StorageGRID utiliza metadatos de objetos para realizar un seguimiento de las ubicaciones de todos los objetos en el grid y gestionar el ciclo de vida de cada objeto a lo largo del tiempo.

Los metadatos de objetos incluyen información como la siguiente:

- Metadatos del sistema, incluidos un ID único para cada objeto (UUID), el nombre del objeto, el nombre del bloque de S3 o el contenedor Swift, 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 hora en que se modificó por última vez el objeto.
- La ubicación actual de almacenamiento de cada copia de objeto o fragmento con código de borrado.
- Todos los metadatos de usuario asociados con el objeto.

Los metadatos de objetos son personalizables y ampliables, por lo que es flexible para las aplicaciones.

Para obtener información detallada sobre cómo y dónde almacena StorageGRID metadatos de objetos, vaya a. "Gestione el almacenamiento de metadatos de objetos".

¿Cómo se protegen los datos de objetos?

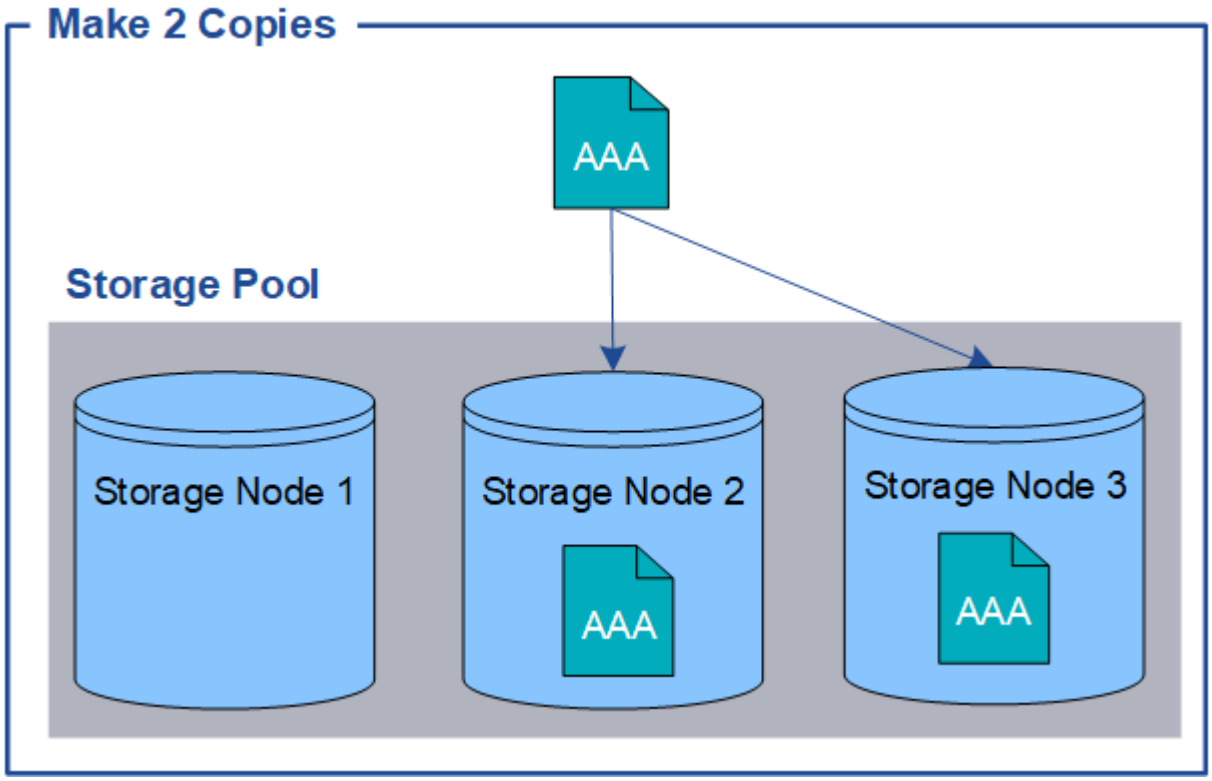
El sistema StorageGRID ofrece dos mecanismos para proteger los datos de objetos contra la pérdida: La replicación y la codificación de borrado.

Replicación

Cuando StorageGRID enlaza objetos con una regla de gestión del ciclo de vida de la información (ILM) que se configura para crear copias replicadas, el sistema crea copias exactas de datos de objetos y los almacena en

nodos de almacenamiento, nodos de archivado o pools de almacenamiento en el cloud. Las reglas de ILM determinan el número de copias realizadas, dónde se almacenan esas copias y durante el tiempo que el sistema retiene. Si se pierde una copia, por ejemplo, como resultado de la pérdida de un nodo de almacenamiento, el objeto sigue disponible si existe una copia en otro lugar del sistema StorageGRID.

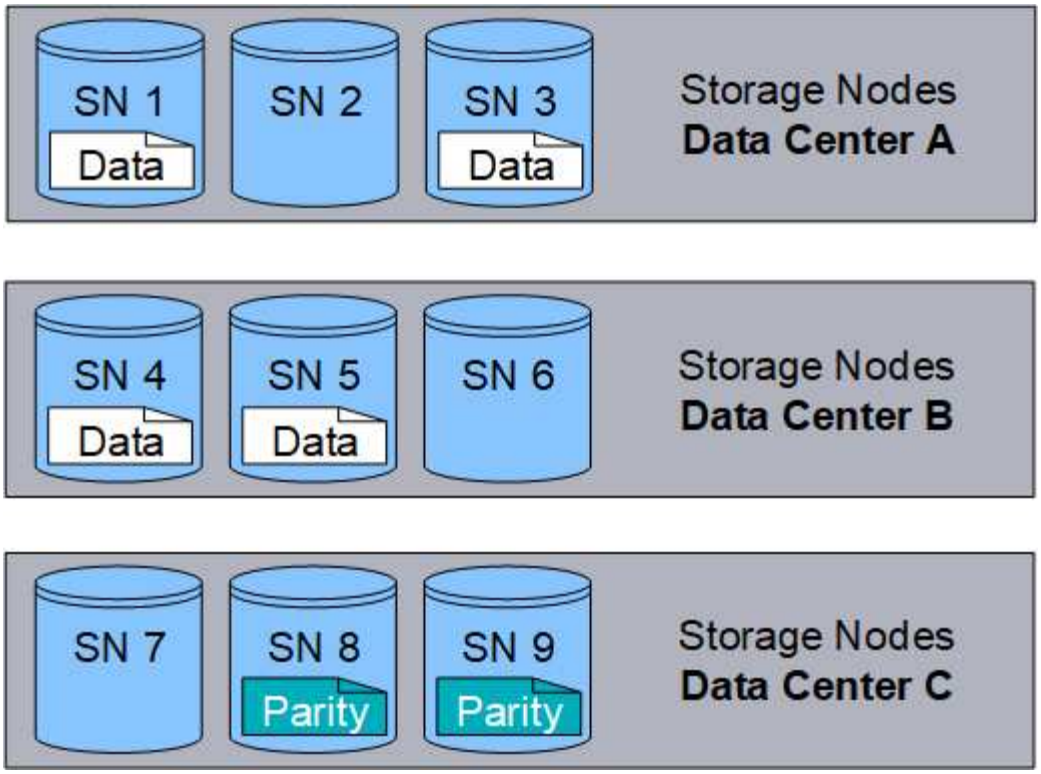
En el ejemplo siguiente, la regla make 2 copies especifica que se coloquen dos copias replicadas de cada objeto en un pool de almacenamiento que contenga tres nodos de almacenamiento.



Codificación de borrado

Cuando StorageGRID enlaza objetos con una regla de ILM que se configura para crear copias con código de borrado, corta los datos de objetos en fragmentos de datos, calcula fragmentos de paridad adicionales y almacena cada fragmento en un nodo de almacenamiento diferente. Cuando se accede a un objeto, se vuelve a ensamblar utilizando los fragmentos almacenados. Si un dato o un fragmento de paridad se corrompen o se pierden, el algoritmo de codificación de borrado puede recrear ese fragmento con un subconjunto de los datos restantes y fragmentos de paridad. Las reglas de ILM y los perfiles de codificación de borrado determinan el esquema de codificación de borrado utilizado.

En el siguiente ejemplo, se muestra el uso de códigos de borrado en los datos de un objeto. En este ejemplo, la regla ILM utiliza un esquema de codificación de borrado 4+2. Cada objeto se divide en cuatro fragmentos de datos iguales y dos fragmentos de paridad se calculan a partir de los datos del objeto. Cada uno de los seis fragmentos se almacena en un nodo de almacenamiento diferente en tres centros de datos para proporcionar protección de datos ante fallos de nodos o pérdidas de sitios.



Información relacionada

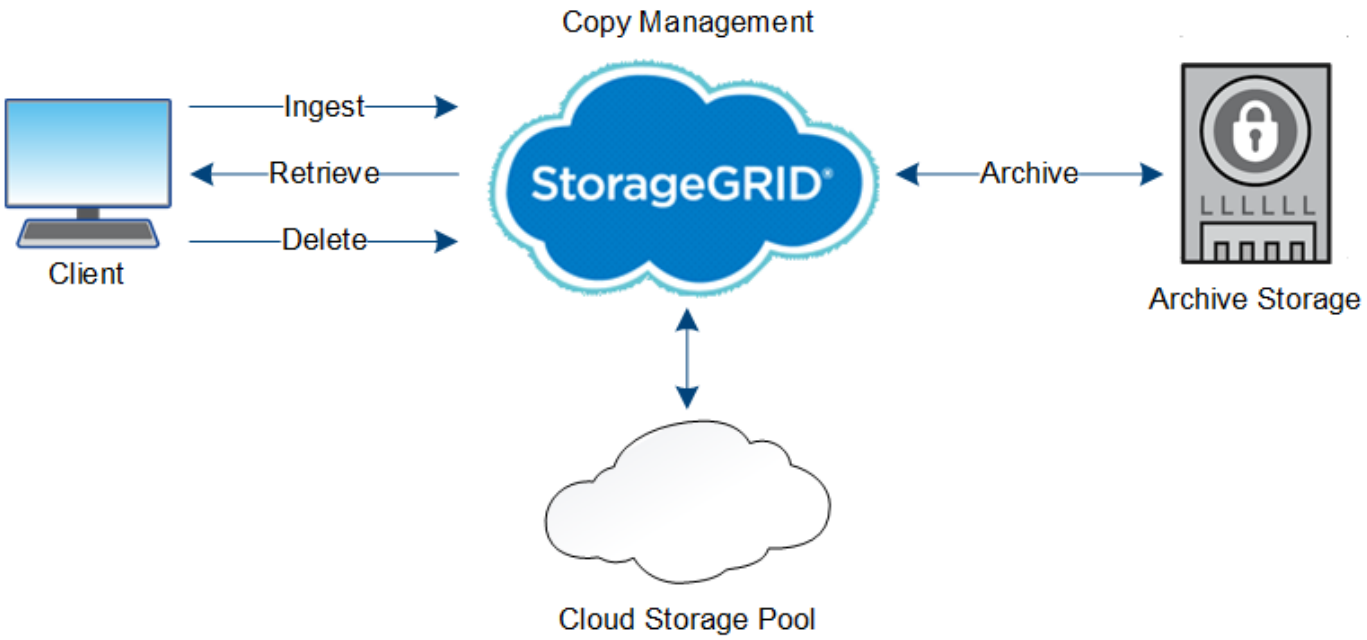
- "Gestión de objetos con ILM"
- "Utilizar la gestión del ciclo de vida de la información"

La vida de un objeto

La vida de un objeto consta de varias etapas. Cada etapa representa las operaciones que ocurren con el objeto.

La vida útil de un objeto incluye las operaciones de procesamiento, gestión de copias, recuperación y eliminación.

- **Procesamiento**: Proceso de una aplicación cliente S3 o Swift que guarda un objeto a través de HTTP en el sistema StorageGRID. En este momento, el sistema StorageGRID comienza a gestionar el objeto.
- **Gestión de copias**: El proceso de administración de copias replicadas y con código de borrado en StorageGRID, como se describe en las reglas de ILM en las políticas de ILM activas. Durante la fase de gestión de copias, StorageGRID protege los datos de objetos frente a la pérdida mediante la creación y el mantenimiento del número y el tipo especificados de copias de objetos en los nodos de almacenamiento, en un pool de almacenamiento en cloud o en el nodo de archivado.
- **Recuperar**: Proceso de una aplicación cliente que accede a un objeto almacenado por el sistema StorageGRID. El cliente lee el objeto, que se recupera de un nodo de almacenamiento, un pool de almacenamiento de cloud o un nodo de archivado.
- **Eliminar**: El proceso de eliminar todas las copias de objetos de la cuadrícula. Los objetos se pueden eliminar como resultado de que la aplicación cliente envíe una solicitud de eliminación al sistema StorageGRID o como resultado de un proceso automático que StorageGRID realiza cuando finaliza la vida útil del objeto.



Información relacionada

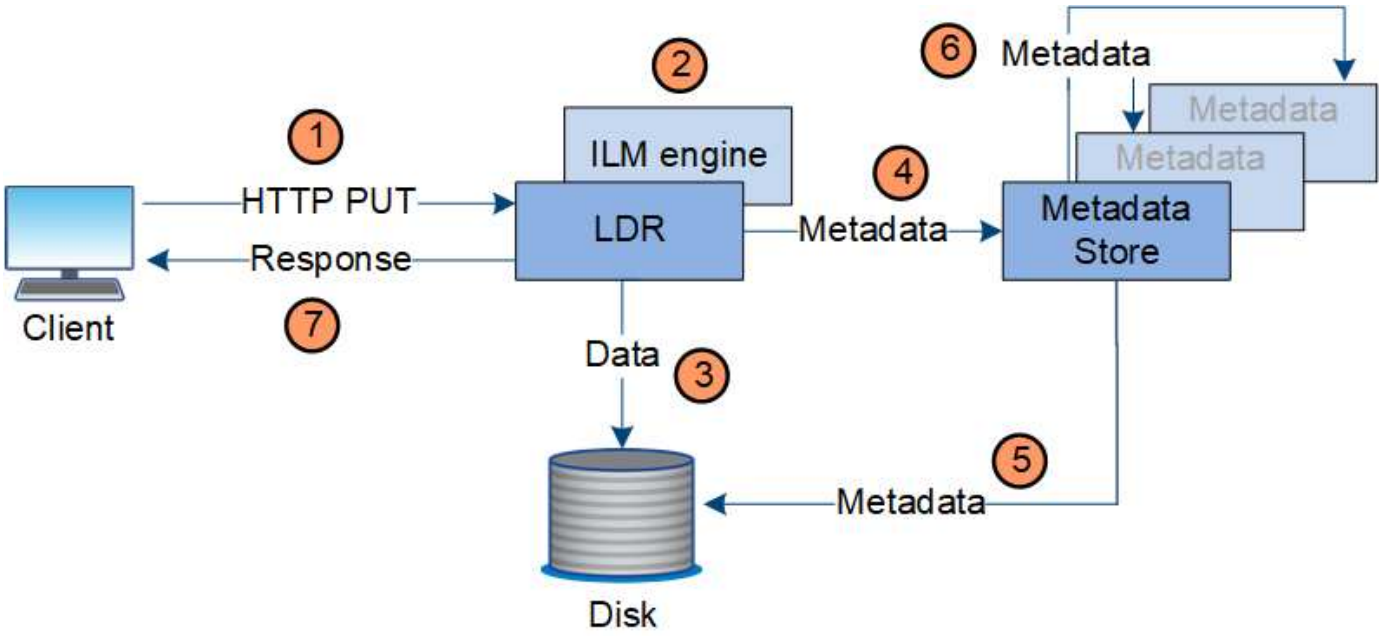
- "Gestión de objetos con ILM"
- "Utilizar la gestión del ciclo de vida de la información"

Flujo de datos de ingesta

Una operación de ingesta, o guardado, consta de un flujo de datos definido entre el cliente y el sistema StorageGRID.

Flujo de datos

Cuando un cliente procesa un objeto al sistema StorageGRID, el servicio LDR en los nodos de almacenamiento procesa la solicitud y almacena los metadatos y los datos en el disco.



1. La aplicación cliente crea el objeto y lo envía al sistema StorageGRID mediante una solicitud PUT HTTP.
2. El objeto se evalúa según la política de ILM del sistema.
3. El servicio LDR guarda los datos de los objetos como una copia replicada o como una copia con código de borrado. (El diagrama muestra una versión simplificada del almacenamiento de una copia replicada en el disco).
4. El servicio LDR envía los metadatos del objeto al almacén de metadatos.
5. El almacén de metadatos guarda los metadatos del objeto en el disco.
6. El almacén de metadatos propaga copias de metadatos de objetos a otros nodos de almacenamiento. Estas copias también se guardan en el disco.
7. El servicio LDR devuelve una respuesta HTTP 200 OK al cliente para reconocer que el objeto se ha ingerido.

Gestión de copias

Los datos de objetos se gestionan mediante las políticas de ILM activas y las reglas de ILM asociadas. Las reglas de ILM hacen copias replicadas o con código de borrado para proteger los datos de objetos de la pérdida.

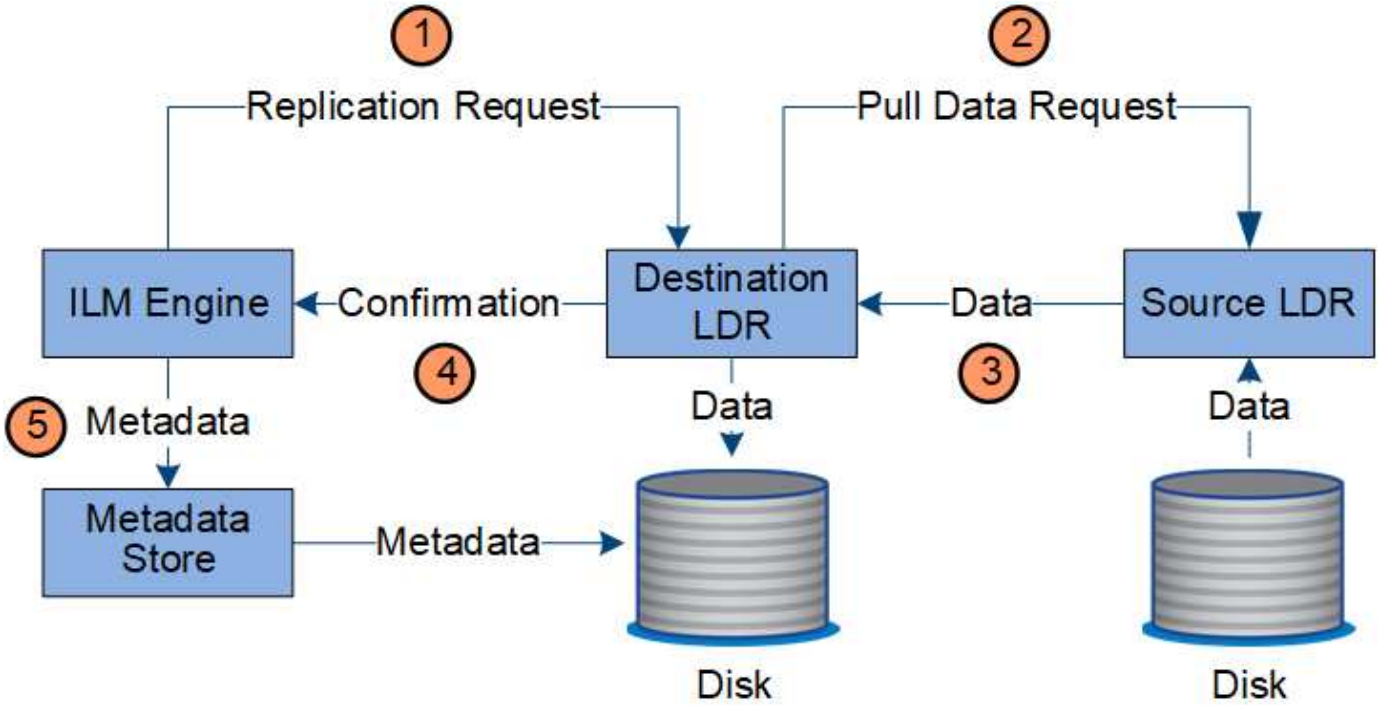
Es posible que sean necesarios diferentes tipos o ubicaciones de copias de objetos en distintos momentos de la vida del objeto. Las reglas de ILM se evalúan periódicamente para asegurarse de que los objetos estén ubicados según sea necesario.

El servicio LDR gestiona los datos de objetos.

Protección de contenido: Replicación

Si las instrucciones de colocación del contenido de una regla de ILM requieren copias replicadas de datos de objetos, los nodos de almacenamiento que componen el pool de almacenamiento configurado y las almacenan en disco.

El motor de gestión del ciclo de vida de la información del servicio LDR controla la replicación y garantiza que se almacene el número correcto de copias en las ubicaciones correctas y la cantidad de tiempo correcta.

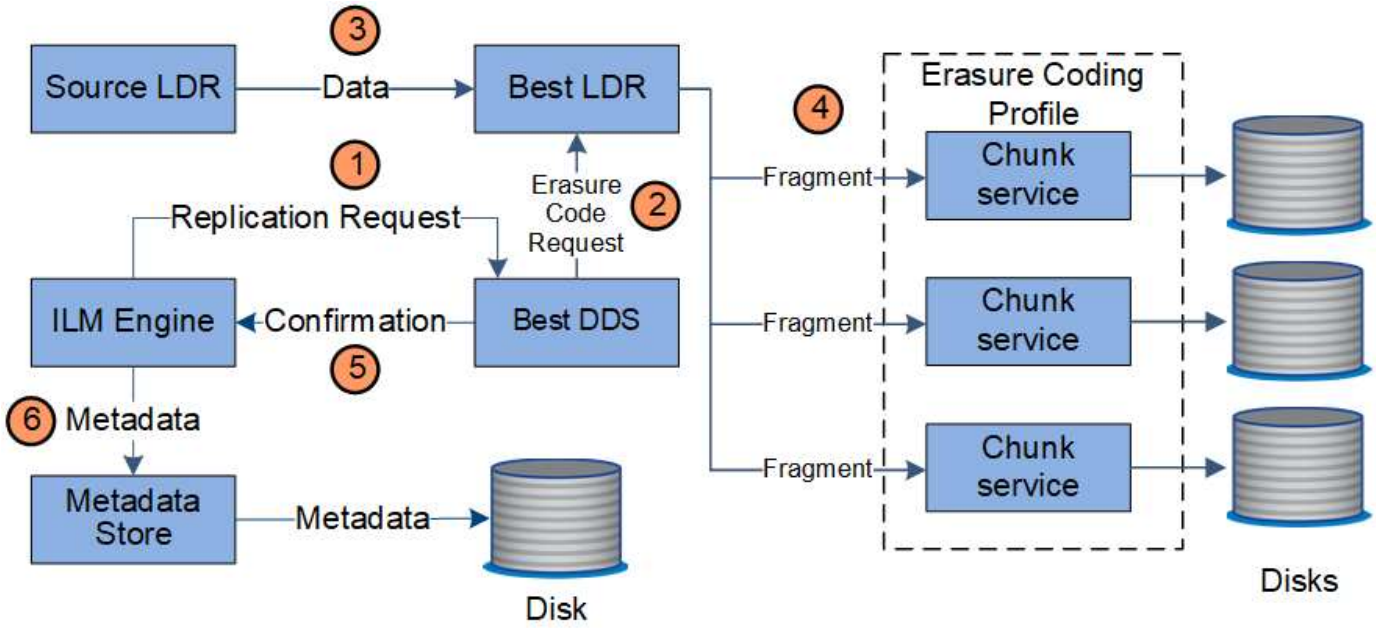


1. El motor de ILM consulta al servicio ADC para determinar el mejor servicio LDR de destino dentro del pool de almacenamiento especificado por la regla de ILM. A continuación, envía ese servicio LDR un comando para iniciar la replicación.
2. El servicio LDR de destino consulta al servicio ADC para obtener la mejor ubicación de origen. A continuación, envía una solicitud de replicación al servicio LDR de origen.
3. El servicio LDR de origen envía una copia al servicio LDR de destino.
4. El servicio LDR de destino notifica al motor de ILM que los datos del objeto se han almacenado.
5. El motor de ILM actualiza el almacén de metadatos con los metadatos de la ubicación de objetos.

Protección de contenido: Codificación de borrado

Si una regla de ILM incluye instrucciones para hacer copias con código de borrado de los datos de objetos, el esquema de código de borrado correspondiente divide los datos de los objetos en datos y fragmentos de paridad, y los distribuye por los nodos de almacenamiento que se configuran en el perfil de código de borrado.

El motor de ILM, que es un componente del servicio LDR, controla el código de borrado y garantiza que el perfil de código de borrado se aplique a los datos de los objetos.

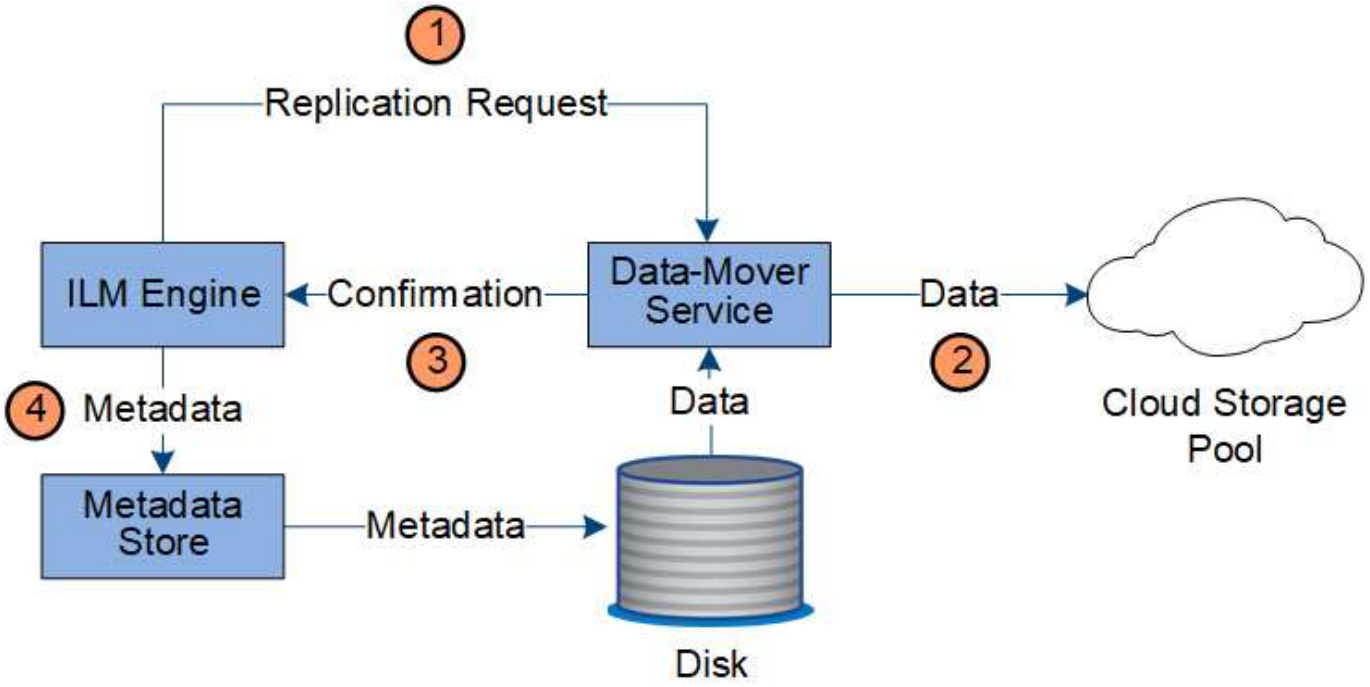


1. El motor ILM consulta al servicio ADC para determinar qué servicio DDS puede realizar mejor la operación de codificación de borrado. Cuando se determina, el motor de ILM envía una solicitud de inicio a ese servicio.
2. El servicio DDS indica a un LDR que borre los datos del objeto.
3. El servicio LDR de origen envía una copia al servicio LDR seleccionado para codificación de borrado.
4. Después de crear el número adecuado de fragmentos de datos y paridad, el servicio LDR distribuye estos fragmentos por los nodos de almacenamiento (servicios Chunk) que forman el pool de almacenamiento del perfil de codificación de borrado.
5. El servicio LDR notifica al motor de ILM y confirma que los datos del objeto se han distribuido correctamente.
6. El motor de ILM actualiza el almacén de metadatos con los metadatos de la ubicación de objetos.

Protección de contenido: Pool de almacenamiento en cloud

Si las instrucciones de colocación de contenido de una regla de ILM requieren que se almacene una copia replicada de los datos de objetos en un Cloud Storage Pool, los datos de objetos se duplican en el bloque de S3 externo o en el contenedor de almacenamiento de Azure Blob que se especificó para el Cloud Storage Pool.

El motor de ILM, que es un componente del servicio LDR, y el servicio Data mover controla el movimiento de objetos a Cloud Storage Pool.



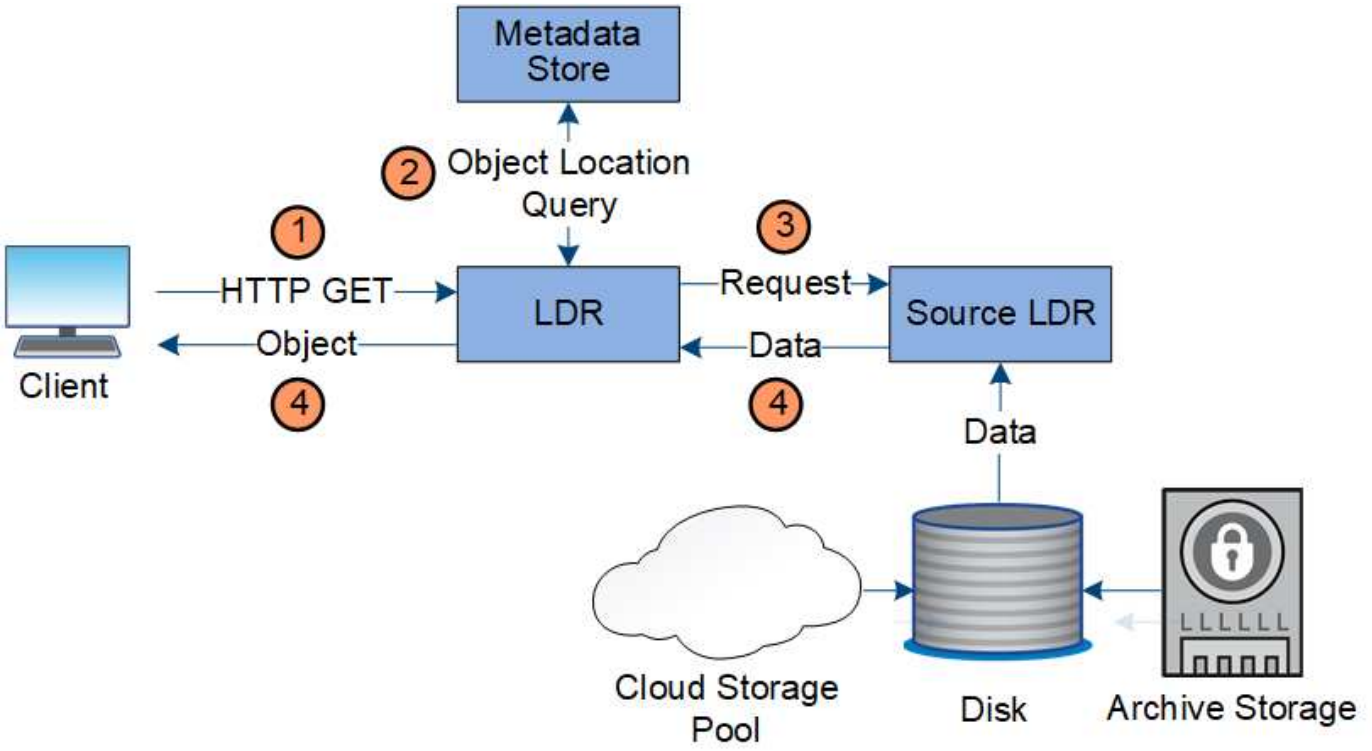
1. El motor de ILM selecciona un servicio Data mover para replicar en el Cloud Storage Pool.
2. El servicio Data mover envía los datos del objeto al Pool de almacenamiento en la nube.
3. El servicio Data mover notifica al motor ILM que los datos del objeto se han almacenado.
4. El motor de ILM actualiza el almacén de metadatos con los metadatos de la ubicación de objetos.

Recuperar el flujo de datos

Una operación de recuperación consta de un flujo de datos definido entre el sistema StorageGRID y el cliente. El sistema utiliza atributos para realizar el seguimiento de la recuperación del objeto desde un nodo de almacenamiento o, si fuera necesario, un pool de almacenamiento en cloud o un nodo de archivado.

El servicio LDR del nodo de almacenamiento consulta el almacén de metadatos para localizar los datos del objeto y los recupera del servicio LDR de origen. Preferentemente, la recuperación se realiza desde un nodo de almacenamiento. Si el objeto no está disponible en un nodo de almacenamiento, la solicitud de recuperación se dirige a un pool de almacenamiento de cloud o a un nodo de archivado.

Si la única copia de objeto se encuentra en el almacenamiento de AWS Glacier o en el nivel de Azure Archive, la aplicación cliente debe emitir una solicitud S3 RestoreObject para restaurar una copia recuperable en el Cloud Storage Pool.



1. El servicio LDR recibe una solicitud de recuperación de la aplicación cliente.
2. El servicio LDR consulta al almacén de metadatos de la ubicación y los metadatos de los datos de objetos.
3. El servicio LDR reenvía la solicitud de recuperación al servicio LDR de origen.
4. El servicio LDR de origen devuelve los datos de objeto del servicio LDR consultado y el sistema devuelve el objeto a la aplicación cliente.

Eliminar flujo de datos

Todas las copias de objetos se eliminan del sistema StorageGRID cuando un cliente realiza una operación de eliminación o cuando finaliza la vida útil del objeto, lo que activa su eliminación automática. Hay un flujo de datos definido para la eliminación de objetos.

Suprimir jerarquía

StorageGRID proporciona varios métodos para controlar cuándo se retienen o se eliminan objetos. Los objetos se pueden eliminar por solicitud del cliente o de forma automática. StorageGRID siempre prioriza la configuración de cualquier bloqueo de objetos S3 sobre las solicitudes de eliminación del cliente, cuya prioridad superan las instrucciones de colocación de ILM y el ciclo de vida de los bloques S3.

- **S3 Object Lock**: Si la configuración global de S3 Object Lock está habilitada para la cuadrícula, los clientes S3 pueden crear cubos con S3 Object Lock habilitado y, a continuación, utilizar la API REST de S3 para especificar la configuración de retención legal y hasta la fecha para cada versión de objeto añadida a ese bloque.
  - Una versión de objeto que está bajo una conservación legal no se puede eliminar con ningún método.
  - Antes de que se alcance la fecha de retención hasta la versión de un objeto, esa versión no se puede eliminar con ningún método.
  - ILM conserva los objetos de los bloques con S3 Object Lock habilitado «para siempre». Sin embargo, una vez alcanzada la fecha de retención hasta la fecha, una solicitud de cliente puede eliminar una

versión de objeto o la expiración del ciclo de vida de la cuchara.

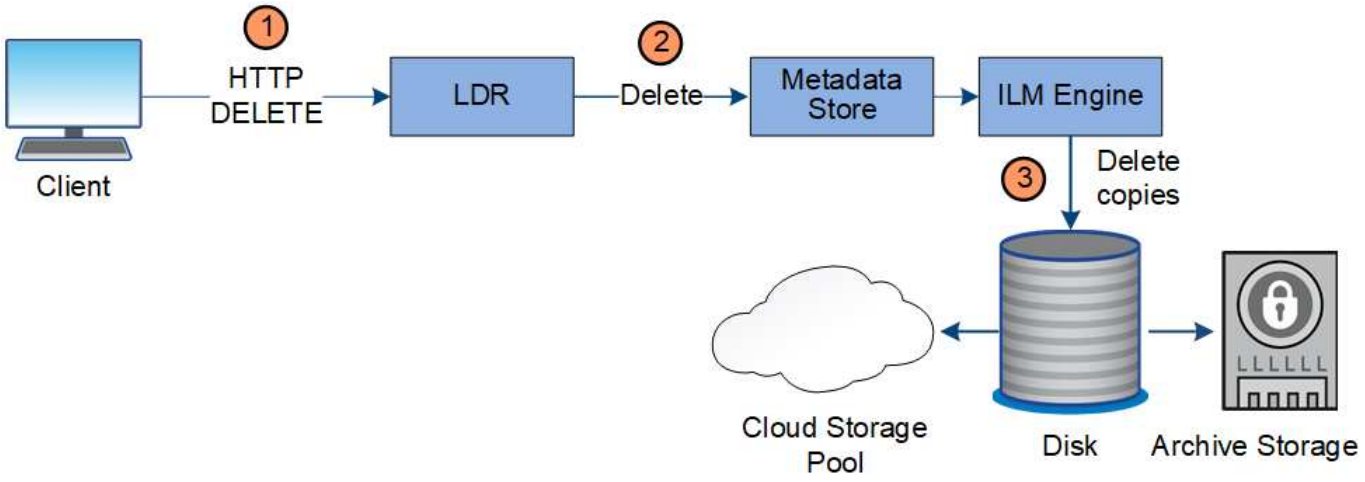
  - Si los clientes S3 aplican una fecha de retención hasta el depósito por defecto, no es necesario especificar una fecha de retención hasta cada objeto.

- **Solicitud de eliminación de cliente**: Un cliente S3 o Swift puede emitir una solicitud de eliminación de objeto. Cuando un cliente elimina un objeto, todas las copias del objeto se quitan del sistema StorageGRID.
- **Eliminar objetos en el cubo**: Los usuarios del administrador de inquilinos pueden usar esta opción para eliminar permanentemente todas las copias de los objetos y versiones de objetos en cubos seleccionados del sistema StorageGRID.
- **Ciclo de vida de bloque S3**: Los clientes S3 pueden agregar una configuración de ciclo de vida a sus bloques que especifica una acción de caducidad. Si existe un ciclo de vida de un bloque, StorageGRID elimina automáticamente todas las copias de un objeto cuando se cumple la fecha o el número de días especificados en la acción Expiración, a menos que el cliente elimine primero el objeto.
- **Instrucciones de colocación de ILM**: Suponiendo que el bloque no tiene habilitado el bloqueo de objetos S3 y que no hay un ciclo de vida de bloque, StorageGRID elimina automáticamente un objeto cuando finaliza el último período de tiempo de la regla ILM y no se especifican más colocaciones para el objeto.

> Cuando se configura el ciclo de vida de un bloque de S3, las acciones de caducidad del ciclo de vida anulan la política de ILM de los objetos que coinciden con el filtro de ciclo de vida. Como resultado, es posible que un objeto se conserve en la cuadrícula aunque hayan caducado las instrucciones de gestión del ciclo de vida de la información relativas a la ubicación del objeto.

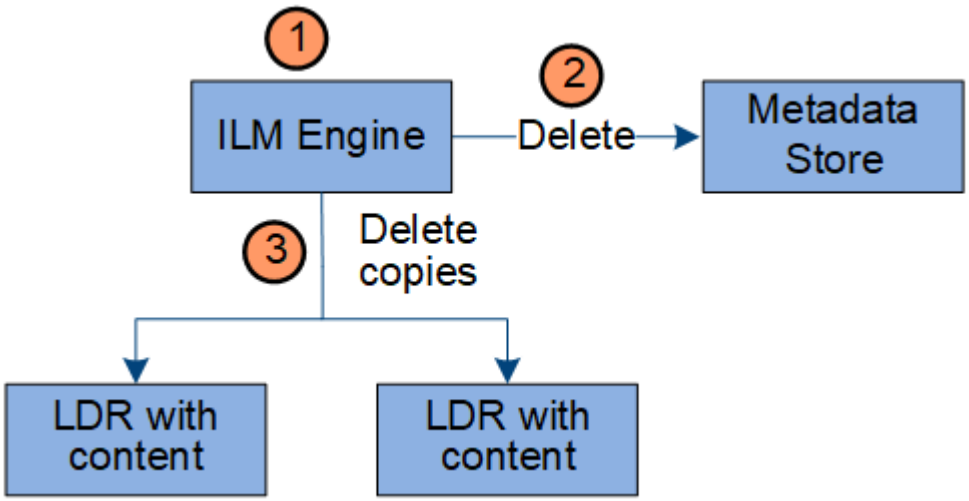
Consulte "Cómo se eliminan los objetos" si quiere más información.

Flujo de datos para eliminaciones de clientes



1. El servicio LDR recibe una solicitud de eliminación de la aplicación cliente.
2. El servicio LDR actualiza el almacén de metadatos para que el objeto se parezca eliminado a las solicitudes del cliente e indica al motor de ILM que elimine todas las copias de los datos de los objetos.
3. El objeto se elimina del sistema. El almacén de metadatos se actualiza para eliminar los metadatos del objeto.

El flujo de datos para eliminaciones de ILM



1. El motor de ILM determina que el objeto debe eliminarse.
2. El motor de ILM notifica al almacén de metadatos. El almacén de metadatos actualiza los metadatos del objeto para que el objeto se vea eliminado a las solicitudes del cliente.
3. El motor de ILM elimina todas las copias del objeto. El almacén de metadatos se actualiza para eliminar los metadatos del objeto.

Utilizar la gestión del ciclo de vida de la información

La gestión de la vida útil de la información (ILM) se utiliza para controlar la ubicación, la duración y el comportamiento de ingesta de todos los objetos del sistema StorageGRID. Las reglas de ILM determinan la manera en que StorageGRID almacena los objetos a lo largo del tiempo. Puede configurar una o varias reglas de ILM y luego añadirlas a una política de ILM.

Una cuadrícula sólo tiene una política activa a la vez. Una política puede contener varias reglas.

Las reglas de ILM definen:

- Qué objetos se deben almacenar. Una regla se puede aplicar a todos los objetos o puede especificar filtros para identificar a qué objetos se aplica una regla. Por ejemplo, una regla puede aplicarse solo a los objetos asociados con determinadas cuentas de inquilino, bloques S3 específicos o contenedores Swift, o valores de metadatos específicos.
- El tipo de almacenamiento y la ubicación. Los objetos se pueden almacenar en nodos de almacenamiento, en pools de almacenamiento en cloud o en nodos de archivado.
- El tipo de copias de objeto realizadas. Las copias pueden replicarse o codificarse con código de borrado.
- Para las copias replicadas, el número de copias realizadas.
- Para las copias con código de borrado, se utiliza el esquema de código de borrado.
- Los cambios a lo largo del tiempo en la ubicación de almacenamiento de un objeto y el tipo de copias.
- Cómo se protegen los datos de objetos cuando se ingieren los objetos en el grid (ubicación síncrona o doble registro).

Tenga en cuenta que los metadatos de objetos no están gestionados por las reglas de ILM. En su lugar, los metadatos de objetos se almacenan en una base de datos de Cassandra en lo que se conoce como almacén

de metadatos. Se mantienen automáticamente tres copias de los metadatos de objetos en cada sitio para proteger los datos frente a pérdidas.

Regla de ILM de ejemplo

Por ejemplo, una regla de ILM podría especificar lo siguiente:

- Aplicar solo a los objetos que pertenecen al inquilino A..
- Realice dos copias replicadas de dichos objetos y almacene cada copia en un sitio diferente.
- Conservar las dos copias «para siempre», lo que significa que StorageGRID no las eliminará automáticamente. En su lugar, StorageGRID conservará estos objetos hasta que se eliminen mediante una solicitud de eliminación del cliente o cuando finalice el ciclo de vida de un bloque.
- Use la opción Equilibrada para el comportamiento de ingesta: La instrucción de ubicación de dos sitios se aplica en cuanto el inquilino A guarda un objeto en StorageGRID, a menos que no sea posible hacer inmediatamente las dos copias requeridas.

  Por ejemplo, si el sitio 2 no se puede acceder cuando el inquilino A guarda un objeto, StorageGRID realizará dos copias provisionales en los nodos de almacenamiento del sitio 1. En cuanto el sitio 2 esté disponible, StorageGRID realizará la copia necesaria en ese sitio.

Cómo evalúa una política de ILM los objetos

Las políticas de ILM activas para el sistema de StorageGRID controlan la ubicación, la duración y el comportamiento de procesamiento de todos los objetos.

Cuando los clientes guardan objetos en StorageGRID, los objetos se evalúan según el conjunto ordenado de reglas de ILM en la política activa, de la siguiente manera:

1. Si los filtros de la primera regla de la política coinciden con un objeto, el objeto se procesa según el comportamiento de procesamiento de esa regla y se almacena según las instrucciones de ubicación de esa regla.
2. Si los filtros de la primera regla no coinciden con el objeto, el objeto se evalúa con cada regla subsiguiente de la política hasta que se realiza una coincidencia.
3. Si ninguna regla coincide con un objeto, se aplican las instrucciones de comportamiento de procesamiento y colocación de la regla predeterminada de la directiva. La regla predeterminada es la última regla de una política y no puede utilizar ningún filtro. Debe aplicarse a todos los inquilinos, todos los grupos y todas las versiones del objeto.

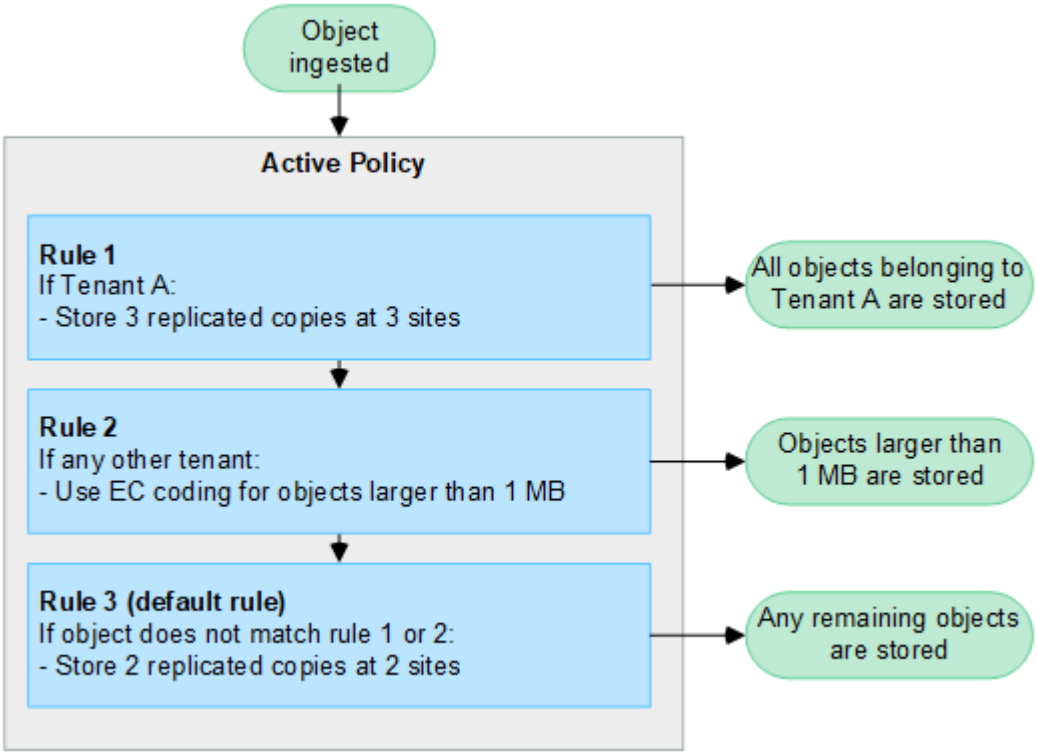
Ejemplo de política de ILM

Por ejemplo, una política de ILM podría contener tres reglas de ILM que especifiquen lo siguiente:

- **Regla 1: Copias replicadas para el Inquilino A**
  - Haga coincidir todos los objetos que pertenecen al inquilino A..
  - Almacene estos objetos como tres copias replicadas en tres sitios.
  - Los objetos que pertenecen a otros arrendatarios no coinciden con la Regla 1, por lo que se evalúan según la Regla 2.
- **Regla 2: Codificación de borrado para objetos mayores de 1 MB**
  - Hacer coincidir todos los objetos de otros inquilinos, pero solo si son mayores de 1 MB. Estos objetos de mayor tamaño se almacenan mediante codificación de borrado 6+3 en tres instalaciones.

- No coincide con los objetos de 1 MB o menos, por lo que estos objetos se evalúan con la Regla 3.

- **Regla 3: 2 copias 2 data centers** (predeterminado)
  - Es la última regla y la predeterminada de la política. No utiliza filtros.
  - Realice dos copias replicadas de todos los objetos que no coincidan con la Regla 1 o la Regla 2 (objetos que no pertenezcan al arrendatario A que tengan 1 MB o menos).



Información relacionada

- "Gestión de objetos con ILM"

Explora StorageGRID

Explore Grid Manager

Grid Manager es una interfaz gráfica basada en navegador que permite configurar, administrar y supervisar el sistema StorageGRID.

> 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.

Cuando inicia sesión en Grid Manager, se conecta a un nodo de administración. Cada sistema StorageGRID incluye un nodo de administrador primario y cualquier número de nodos de administrador que no son primarios. Puede conectarse a cualquier nodo de administrador y cada nodo de administrador muestra una vista similar del sistema StorageGRID.

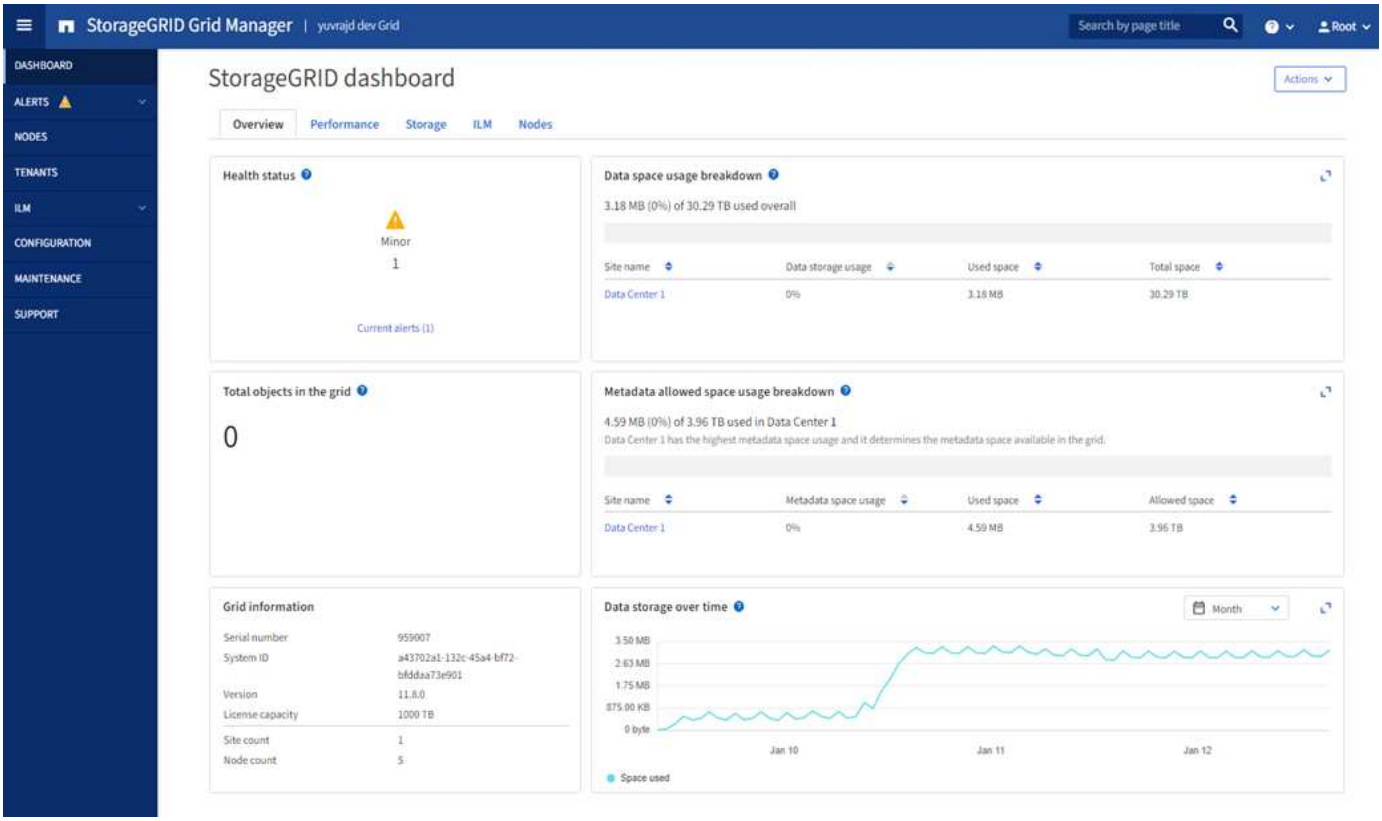
Puede acceder a Grid Manager mediante una "navegador web compatible".

Consola de Grid Manager

Cuando inicie sesión por primera vez en Grid Manager, puede utilizar el panel de control para "supervise las

actividades del sistema" análisis general.

La consola contiene información sobre el estado y el rendimiento del sistema, el uso del almacenamiento, procesos de ILM, operaciones de S3 y Swift, y los nodos del grid. Puede hacerlo "configure el panel de control" al seleccionar de una colección de tarjetas que contienen la información que necesita para controlar eficazmente su sistema.



Para obtener una explicación de la información que se muestra en cada tarjeta, seleccione el icono de ayuda para esa tarjeta.

Campo de búsqueda

El campo **Buscar** de la barra de encabezado permite navegar rápidamente a una página específica dentro de Grid Manager. Por ejemplo, puede introducir **KM** para acceder a la página Servidor de administración de claves (KMS). Puede utilizar **Buscar** para buscar entradas en la barra lateral del Gestor de cuadrícula y en los menús Configuración, Mantenimiento y Soporte.

Menú de ayuda

El menú de ayuda proporciona acceso a:

- La "FabricPool" y.. "Configuración de S3" asistente
- El centro de documentación de StorageGRID para la versión actual
- "Documentación de API"
- Información sobre la versión de StorageGRID instalada actualmente

Menú Alertas

El menú Alertas proporciona una interfaz fácil de usar para detectar, evaluar y resolver problemas que pueden

producirse durante el funcionamiento de StorageGRID.

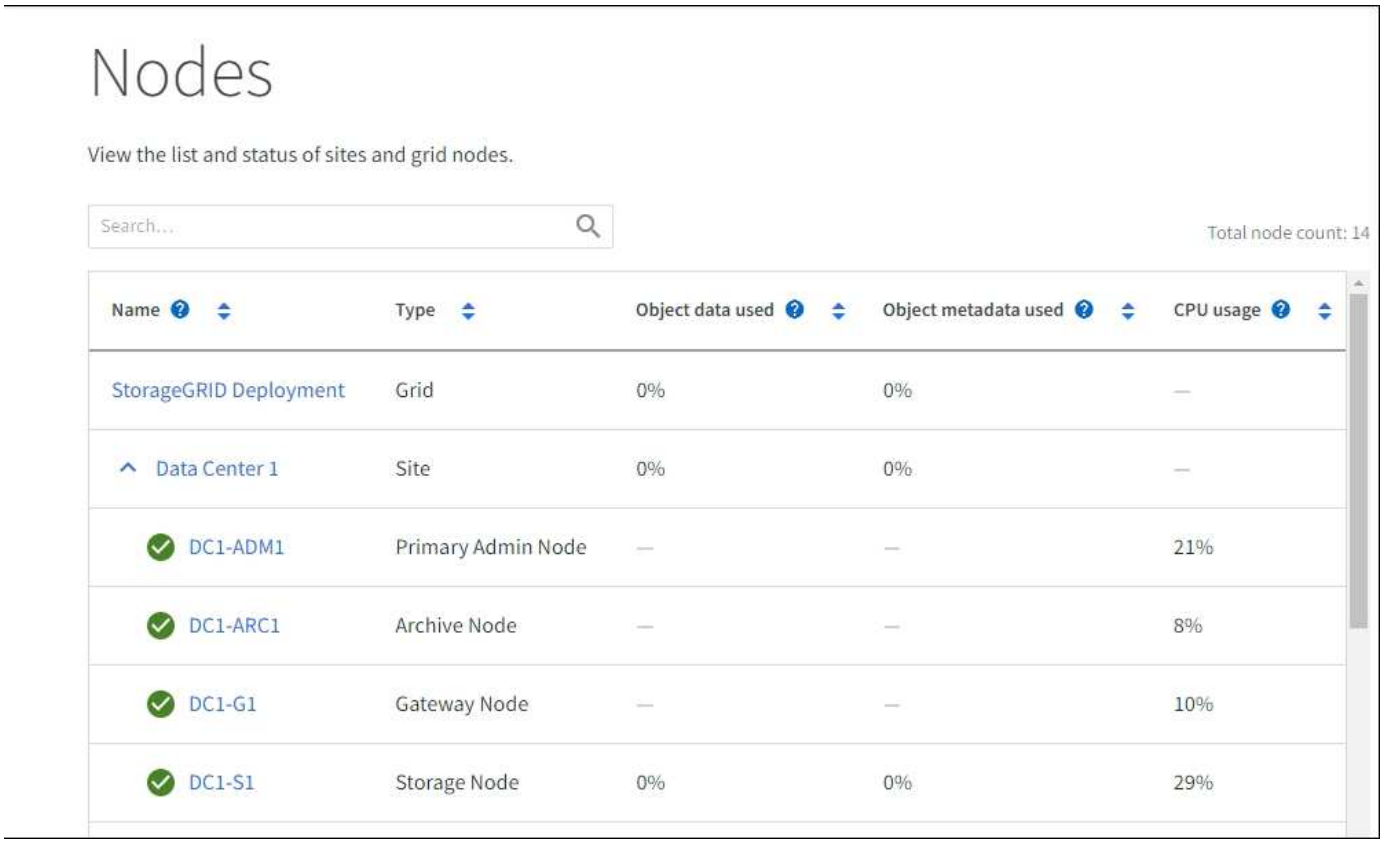
En el menú Alertas, puede realizar lo siguiente a. "gestionar alertas":

- Revisar las alertas actuales
- Revisar las alertas resueltas
- Configure silencios para suprimir notificaciones de alerta
- Defina reglas de alerta para condiciones que activen alertas
- Configure el servidor de correo electrónico para las notificaciones de alertas

Nodos

La "Nodos" muestra información sobre toda la cuadrícula, cada sitio de la cuadrícula y cada nodo de un sitio.

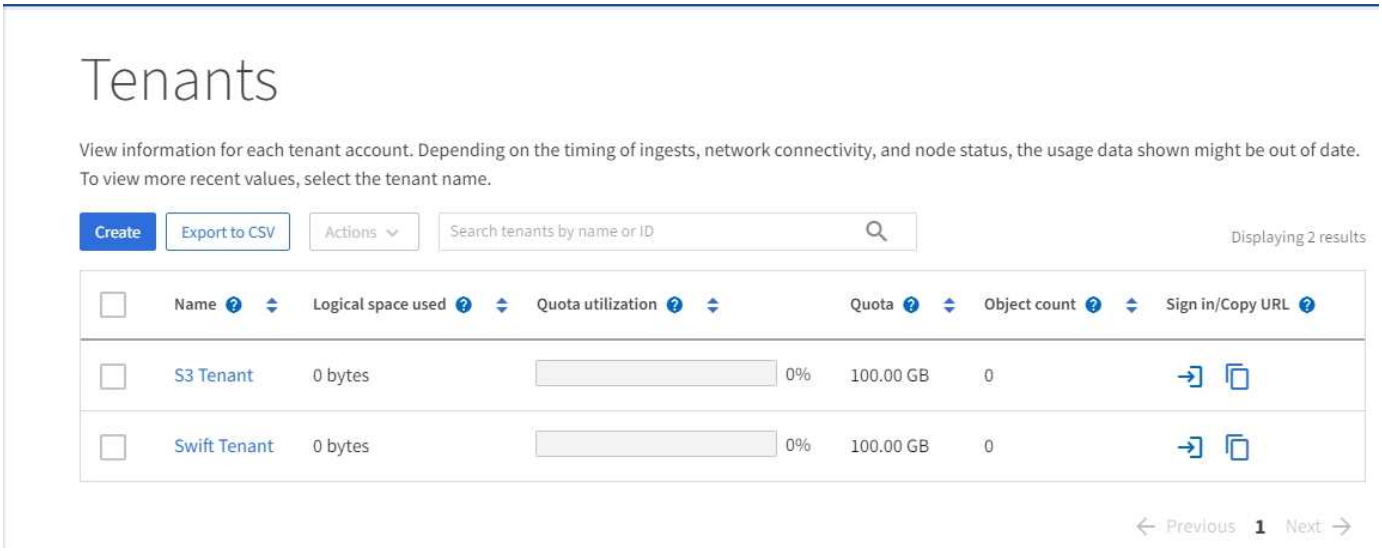
La página de inicio de los nodos muestra métricas combinadas para toda la cuadrícula. Para ver la información de un sitio o nodo en particular, seleccione el sitio o el nodo.



Inquilinos

La "Clientes" le permite hacerlo "cree y supervise las cuentas de inquilino de almacenamiento" Para su sistema StorageGRID. Debe crear al menos una cuenta de inquilino para especificar quién puede almacenar y recuperar objetos y qué funcionalidad está disponible para ellos.

La página Tenants también proporciona detalles de uso para cada cliente, incluyendo la cantidad de almacenamiento usado y el número de objetos. Si establece una cuota cuando creó el arrendatario, puede ver la cantidad de esa cuota que se ha utilizado.



Menú ILM

La "Menú ILM" le permite "Configurar las reglas y las políticas de gestión de la vida útil de la información (ILM)" que rigen la durabilidad y la disponibilidad de los datos. También puede introducir un identificador de objeto para ver los metadatos de ese objeto.

En el menú de ILM, puede ver y gestionar ILM:

- Bases de datos
- Normativas
- Etiquetas de políticas
- Pools de almacenamiento
- Codificación de borrado
- Grados de almacenamiento
- Regiones
- Búsqueda de metadatos de objetos

Menú de configuración

El menú Configuración le permite especificar los ajustes de red, la configuración de seguridad, la configuración del sistema, las opciones de supervisión y las opciones de control de acceso.

Tareas de red

Entre las tareas de red se incluyen:

- "Gestionar grupos de alta disponibilidad"
- "Gestión de puntos finales del equilibrador de carga"
- "Configuración de nombres de dominio de punto final S3"
- "Gestión de directivas de clasificación de tráfico"
- "Configurando interfaces VLAN"

Tareas de seguridad

Las tareas de seguridad incluyen:

- "Gestión de certificados de seguridad"
- "Gestión de los controles internos del firewall"
- "Configuración de servidores de gestión de claves"
- Configuración de los ajustes de seguridad, incluido el "Política de TLS y SSH", "opciones de seguridad de objetos y redes", y. "configuración de seguridad de la interfaz".
- Configuración de los ajustes de un "proxy de almacenamiento" o una "proxy de administración"

Tareas del sistema

Las tareas del sistema incluyen:

- Uso "federación de grid" Para clonar información de cuenta de inquilino y replicar datos de objetos entre dos sistemas StorageGRID.
- Opcionalmente, active el "Comprimir objetos almacenados" opción.
- "Gestión del bloqueo de objetos S3"
- Comprender las opciones de almacenamiento como "segmentación de objetos" y.. "marcas de agua de volumen de almacenamiento".

Tareas de supervisión

Las tareas de supervisión incluyen:

- "Configuración de los mensajes de auditoría y los destinos de registro"
- "Uso de la supervisión de SNMP"

Tareas de control de acceso

Las tareas de control de acceso incluyen:

- "Gestión de los grupos de administración"
- "Gestión de usuarios administradores"
- Cambiar el "aprovisionamiento de la clave de acceso" o. "contraseñas de la consola del nodo"
- "Mediante la federación de identidades"
- "Configuración de SSO"

Menú de mantenimiento

El menú Mantenimiento le permite realizar tareas de mantenimiento, mantenimiento del sistema y mantenimiento de la red.

Tareas

Las tareas de mantenimiento incluyen:

- "Operaciones de decomisionar" para eliminar los nodos y sitios de cuadrícula no utilizados

- "Operaciones de expansión" para agregar nuevos nodos y sitios de cuadrícula
- "Procedimientos de recuperación de nodos de grid" para sustituir un nodo con fallos y restaurar los datos
- "Cambiar el nombre de los procedimientos" para cambiar los nombres mostrados de la cuadrícula, los sitios y los nodos
- "Operaciones de comprobación de existencia de objetos" para verificar la existencia (aunque no la corrección) de los datos de objeto
- Ejecución de un "reinicio gradual" para reiniciar varios nodos de cuadrícula
- "Operaciones de restauración de volúmenes"

Sistema

Algunas de las tareas de mantenimiento del sistema que se pueden realizar son:

- "Ver información de licencias de StorageGRID" o. "actualizando la información de licencia"
- Generar y descargar el "Paquete de recuperación"
- Realizar actualizaciones de software StorageGRID, incluidas actualizaciones de software, correcciones urgentes y actualizaciones para el software de sistema operativo SANtricity en los dispositivos seleccionados
  - "Procedimiento de actualización"
  - "Procedimiento de revisión"
  - "Actualice el sistema operativo SANtricity en las controladoras de almacenamiento SG6000 mediante Grid Manager"
  - "Actualice el sistema operativo SANtricity en las controladoras de almacenamiento SG5700 mediante Grid Manager"

Red

Algunas de las tareas de mantenimiento de red que puede realizar son:

- "Configurando servidores DNS"
- "Actualizando subredes de red de grid"
- "Gestionar servidores NTP"

Menú de soporte

El menú Soporte ofrece opciones que ayudan al soporte técnico a analizar y solucionar problemas del sistema. Hay tres partes en el menú Soporte: Herramientas, Alarmas (heredadas) y otras.

Herramientas

En la sección Herramientas del menú Soporte, puede:

- "Configure AutoSupport"
- "Ejecutar diagnóstico" en el estado actual de la cuadrícula
- "Acceda al árbol de topología de cuadrícula" para ver información detallada sobre los nodos de cuadrícula, los servicios y los atributos
- "Recopilar archivos de registro y datos del sistema"

- "Revisar las métricas de soporte"

> Las herramientas disponibles en la opción * Metrics* están diseñadas para su uso por el soporte técnico. Algunas funciones y elementos de menú de estas herramientas no son intencionalmente funcionales.

Alarmas (heredadas)

Desde la "Alarmas (heredadas)" Del menú Soporte, puede:

- Revise las alarmas actuales, históricas y globales
- Configurar eventos personalizados
- Configuración "notificaciones por correo electrónico para alarmas heredadas"

> Aunque el sistema de alarma heredado sigue siendo compatible, el sistema de alerta ofrece importantes ventajas y es más fácil de usar.

Otros

Desde la otra sección del menú Soporte, puede:

- Gestione "coste de enlace"
- Ver "Sistema de gestión de redes (NMS)" entradas
- Gestione "marcas de agua de almacenamiento"

Explore el responsable de inquilinos

La "Administrador de inquilinos" es la interfaz gráfica basada en navegador a la que los usuarios inquilinos acceden para configurar, gestionar y supervisar sus cuentas de almacenamiento.

> El gestor de inquilinos se actualiza con cada versión y es posible que no coincida con las capturas de pantalla de ejemplo de esta página.

Cuando los usuarios de inquilinos inician sesión en el Administrador de inquilinos, se conectan a un nodo de administración.

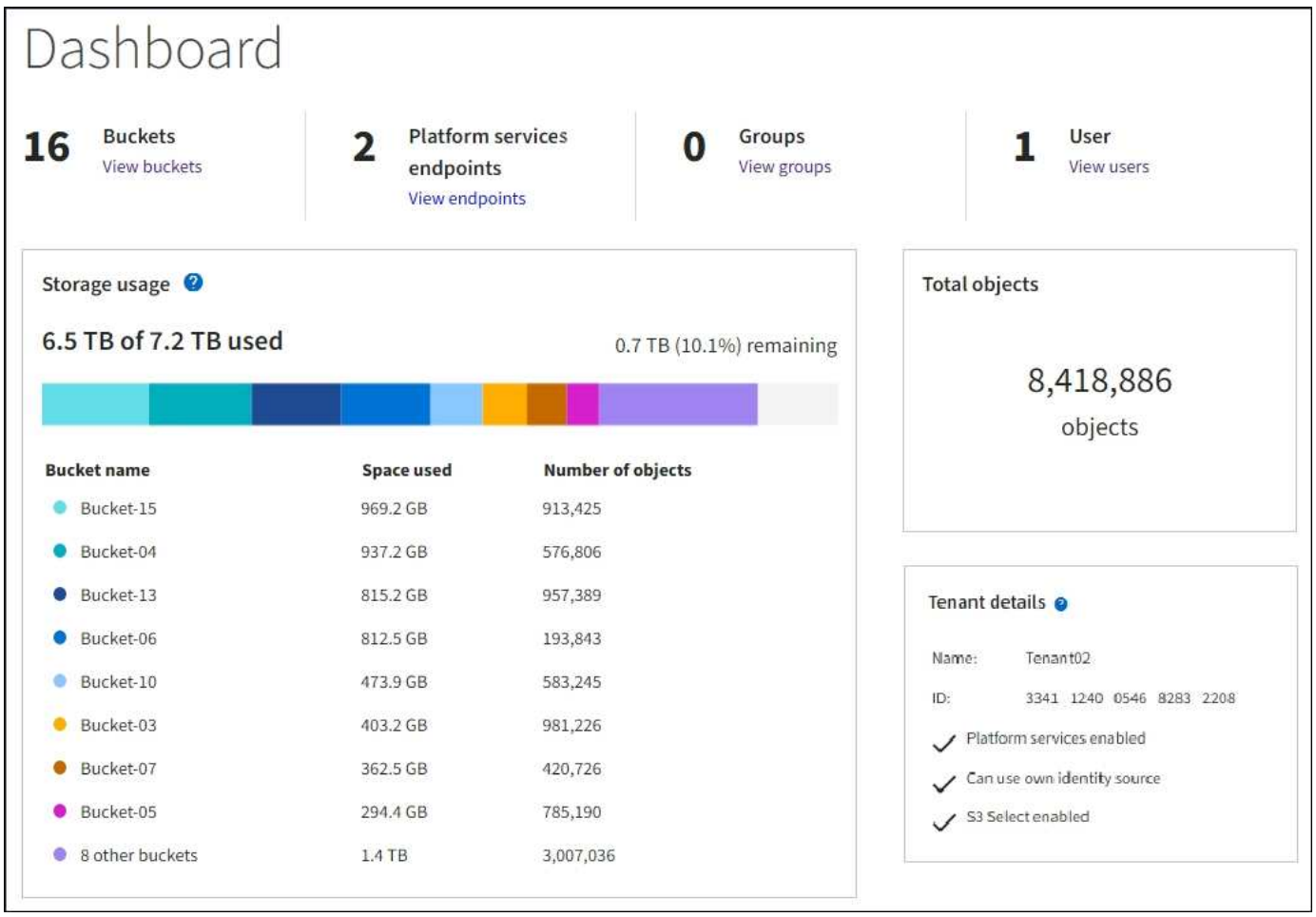
Consola del administrador de inquilinos

Una vez que un administrador de grid crea una cuenta de inquilino mediante Grid Manager o la API de gestión de grid, los usuarios de inquilinos pueden iniciar sesión en el Administrador de inquilinos.

La consola de tenant Manager permite que los usuarios inquilinos supervisen el uso del almacenamiento de un vistazo. El panel Storage Usage contiene una lista de los bloques más grandes (S3) o contenedores (Swift) para el inquilino. El valor espacio utilizado es la cantidad total de datos de objeto del bloque o contenedor. El gráfico de barras representa los tamaños relativos de estos cubos o contenedores.

El valor mostrado encima del gráfico de barras es una suma del espacio utilizado para todos los cubos o contenedores del arrendatario. Si se especificó el número máximo de gigabytes, terabytes o petabytes disponibles para el inquilino cuando se creó la cuenta, también se muestra la cantidad de cuota utilizada y

restante.



Menú Almacenamiento (S3)

El menú Storage se proporciona únicamente para cuentas de inquilinos de S3. Este menú permite a los usuarios de S3 administrar claves de acceso; crear, gestionar y suprimir buckets; administrar puntos finales de servicios de plataforma; y ver cualquier conexión de federación de grid que se les permita utilizar.

Mis claves de acceso

Los usuarios de inquilinos S3 pueden gestionar las claves de acceso de la siguiente manera:

- Los usuarios que tienen el permiso Administrar sus propias credenciales de S3 pueden crear o eliminar sus propias claves de acceso de S3.
- Los usuarios que tienen el permiso de acceso root pueden administrar las claves de acceso para la cuenta root de S3, su propia cuenta y todos los demás usuarios. Las claves de acceso raíz también proporcionan acceso completo a los bloques y objetos del inquilino, a menos que una política de bloque lo deshabilite explícitamente.

> La gestión de las claves de acceso de otros usuarios se realiza desde el menú Access Management.

Cucharones

Los usuarios inquilinos de S3 con los permisos correspondientes pueden realizar las siguientes tareas para sus bloques:

- Crear cubos
- Habilite el bloqueo de objetos de S3 para un bloque nuevo (asume que la función de bloqueo de objetos de S3 está habilitada para el sistema StorageGRID)
- Actualice los valores de coherencia
- Activar y desactivar las actualizaciones de hora del último acceso
- Activar o suspender el control de versiones de objetos
- Actualizar S3 Retención predeterminada de bloqueo de objetos
- Configurar el uso compartido de recursos de origen cruzado (CORS)
- Eliminar todos los objetos de un depósito
- Eliminar cubos vacíos
- Utilice la "S3 Consola" para gestionar objetos de cubo

Si un administrador de grid habilitó el uso de servicios de plataforma para la cuenta de inquilino, un usuario inquilino de S3 con los permisos correspondientes también puede realizar estas tareas:

- Configure las notificaciones de eventos S3, que se pueden enviar a un servicio de destino que admita Amazon Simple Notification Service.
- Configure la replicación de CloudMirror, que permite que el inquilino replique automáticamente objetos en un bloque de S3 externo.
- Configurar la integración de búsqueda, que envía metadatos de objetos a un índice de búsqueda de destino siempre que se crea, se elimina o actualiza un objeto o sus metadatos o etiquetas.

Extremos de servicios de plataforma

Si un administrador de grid ha habilitado el uso de servicios de plataforma para la cuenta de inquilino, un usuario de inquilino de S3 con el permiso Manage Endpoints puede configurar un punto final de destino para cada servicio de plataforma.

Conexiones de federación de grid

Si un administrador de grid ha habilitado el uso de una conexión de federación de grid para la cuenta de inquilino, un usuario de S3 que tiene permiso de acceso raíz puede ver el nombre de la conexión, acceder a la página de detalles de bloque de cada bloque que tiene habilitada la replicación entre grid, y ver el error más reciente que se produce cuando los datos del depósito se están replicando en la otra cuadrícula de la conexión. Consulte "Ver conexiones de federación de grid".

Menú Access Management

El menú Access Management permite a los inquilinos StorageGRID importar grupos de usuarios desde un origen de identidades federado y asignar permisos de gestión. Los inquilinos también pueden gestionar los usuarios y los grupos de inquilinos locales, a menos que el inicio de sesión único (SSO) esté vigente para todo el sistema StorageGRID.

Directrices sobre redes

Directrices de redes: Descripción general

Use estas directrices para obtener más información sobre la arquitectura de StorageGRID y las topologías de red, así como para conocer los requisitos de configuración y aprovisionamiento de la red.

Acerca de estas instrucciones

Estas directrices ofrecen información que se puede usar para crear la infraestructura de red de StorageGRID antes de implementar y configurar nodos de StorageGRID. Utilice estas directrices para asegurarse de que la comunicación puede producirse entre todos los nodos de la cuadrícula y entre la cuadrícula y los clientes y servicios externos.

Los clientes externos y los servicios externos necesitan conectarse a redes StorageGRID para realizar funciones como las siguientes:

- Almacenar y recuperar datos de objetos
- Recibir notificaciones por correo electrónico
- Acceder a la interfaz de gestión de StorageGRID (el administrador de grid y el administrador de inquilinos)
- Acceder al recurso compartido de auditoría (opcional)
- Proporcionar servicios como:
  - Protocolo de hora de red (NTP)
  - Sistema de nombres de dominio (DNS)
  - Servidor de gestión de claves (KMS)

Las redes de StorageGRID deben configurarse de manera adecuada para manejar el tráfico de estas funciones y más.

Antes de empezar

Para configurar las redes de un sistema StorageGRID es necesario contar con un alto nivel de experiencia en conmutación Ethernet, redes TCP/IP, subredes, enrutamiento de red y servidores de seguridad.

Antes de configurar la red, familiarícese con la arquitectura de StorageGRID tal como se describe en "Más información sobre StorageGRID".

Después de determinar qué redes StorageGRID desea usar y cómo se configurarán esas redes, puede instalar y configurar los nodos StorageGRID siguiendo las instrucciones correspondientes.

Instale los nodos del dispositivo

- "Instale el hardware del dispositivo"

Instale nodos basados en software

- "Instalar StorageGRID en Red Hat Enterprise Linux"
- "Instalar StorageGRID en Ubuntu o Debian"
- "Instale StorageGRID en VMware"

Configure y administre el software de StorageGRID

- "Administre StorageGRID"
- "Notas de la versión"

Tipos de red StorageGRID

Los nodos de grid en un proceso del sistema de StorageGRID *grid traffic*, *admin traffic* y *client*. Debe configurar la red de forma adecuada para administrar estos tres tipos de tráfico y proporcionar control y seguridad.

Tipos de tráfico

Tipo de tráfico	Descripción	Tipo de red
Tráfico de red	El tráfico interno de StorageGRID que viaja entre todos los nodos de la cuadrícula. Todos los nodos de grid deben poder comunicarse con el resto de los nodos de grid en esta red.	Red de grid (obligatoria)
Tráfico de administración	El tráfico utilizado para la administración y el mantenimiento del sistema.	Red de administración (opcional) Red VLAN (opcional)
Tráfico del cliente	El tráfico que se desplaza entre aplicaciones cliente externas y la cuadrícula, incluidas todas las solicitudes de almacenamiento de objetos de los clientes S3 y Swift.	Red de cliente (opcional) Red VLAN (opcional)

Puede configurar las redes de las siguientes maneras:

- Sólo red de red de red
- Redes Grid y Admin
- Redes de clientes y grid
- Grid, Admin y redes de clientes

La red de red es obligatoria y puede administrar todo el tráfico de red. Las redes de administración y cliente se pueden incluir en el momento de la instalación o agregar más tarde para adaptarse a los cambios en los requisitos. Aunque la red de administración y la red de cliente son opcionales, cuando se utilizan estas redes para gestionar el tráfico administrativo y de cliente, la red de cuadrícula se puede aislar y proteger.

Sólo se puede acceder a los puertos internos a través de la red de cuadrícula. Se puede acceder a los puertos externos desde todos los tipos de red. Esta flexibilidad proporciona varias opciones para diseñar una implementación de StorageGRID y configurar filtros de puertos e IP externos en switches y firewalls. Consulte "comunicaciones internas de los nodos de grid" y.. "comunicaciones externas".

Interfaces de red

Los nodos StorageGRID están conectados a cada red de acuerdo con las siguientes interfaces específicas:

Red	Nombre de la interfaz
Red de grid (obligatoria)	eth0
Red administrativa (opcional)	eth1
Red de cliente (opcional)	eth2

Para obtener detalles sobre la asignación de puertos virtuales o físicos a interfaces de red de los nodos, consulte las instrucciones de instalación:

Nodos basados en software

- "Instalar StorageGRID en Red Hat Enterprise Linux"
- "Instalar StorageGRID en Ubuntu o Debian"
- "Instale StorageGRID en VMware"

Nodos del dispositivo

- "Dispositivo de almacenamiento SGF6112"
- "Dispositivo de almacenamiento SG6000"
- "Dispositivo de almacenamiento SG5700"
- "Servicios de aplicaciones SG100 y SG1000"

Información de red para cada nodo

Tiene que configurar lo siguiente para cada red que habilite en un nodo:

- Dirección IP
- Máscara de subred
- Dirección IP de la pasarela

Solo puede configurar una combinación de dirección IP, máscara y puerta de enlace para cada una de las tres redes de cada nodo de grid. Si no desea configurar una puerta de enlace para una red, debe usar la dirección IP como dirección de puerta de enlace.

Grupos de alta disponibilidad

Los grupos de alta disponibilidad ofrecen la posibilidad de agregar direcciones IP virtuales (VIP) a la interfaz de red de cliente o de grid. Para obtener más información, consulte "Gestión de grupos de alta disponibilidad".

Red Grid

Se requiere la red de red. Se utiliza para todo el tráfico interno de StorageGRID. Grid Network proporciona conectividad entre todos los nodos de la cuadrícula, en todos los sitios y subredes. Todos los nodos de la red de cuadrícula deben poder comunicarse con los demás nodos. La red de cuadrícula puede estar compuesta de varias subredes. Las redes que contienen servicios de grid críticos, como NTP, también se pueden agregar como subredes de grid.

StorageGRID no admite la traducción de direcciones de red (NAT) entre los nodos.

La red de cuadrícula se puede utilizar para todo el tráfico de administración y todo el tráfico de cliente, incluso si la red de administración y la red de cliente están configuradas. La puerta de enlace de red de cuadrícula es la puerta de enlace predeterminada del nodo a menos que el nodo tenga configurada la red de cliente.

> Al configurar la red de cuadrícula, debe asegurarse de que la red está protegida de clientes que no son de confianza, como los que se encuentran en Internet abierto.

Tenga en cuenta los siguientes requisitos y detalles para el gateway de red de Grid:

- La pasarela de red de cuadrícula debe configurarse si hay varias subredes de la cuadrícula.
- Grid Network Gateway es la puerta de enlace predeterminada del nodo hasta que se completa la configuración de la cuadrícula.
- Se generan automáticamente rutas estáticas para todos los nodos a todas las subredes configuradas en la lista global de subredes de red de cuadrícula.
- Si se agrega una red de cliente, la puerta de enlace predeterminada cambia de la puerta de enlace de red de cuadrícula a la puerta de enlace de red de cliente cuando finaliza la configuración de la cuadrícula.

Red de administración

La red administrativa es opcional. Una vez configurada, se puede utilizar para el tráfico de administración y mantenimiento del sistema. La red administrativa suele ser una red privada y no es necesario que se pueda enrutar entre nodos.

Puede elegir qué nodos de grid deben tener habilitada la red de administrador.

Cuando utiliza la red administrativa, el tráfico administrativo y de mantenimiento no necesita desplazarse por la red de red. Entre los usos típicos de la red administrativa se incluyen los siguientes:

- Acceso a las interfaces de usuario de Grid Manager y de arrendatario Manager.
- Acceso a servicios esenciales como servidores NTP, servidores DNS, servidores de gestión de claves (KMS) externos y servidores de protocolo ligero de acceso a directorios (LDAP).
- Acceso a registros de auditoría en nodos de administrador.
- Acceso de protocolo de shell seguro (SSH) para mantenimiento y soporte.

La red de administración nunca se utiliza para el tráfico de grid interno. Se proporciona una puerta de enlace de red de administración y permite que la red de administración se comunique con varias subredes externas. Sin embargo, la puerta de enlace de red del administrador nunca se usa como la puerta de enlace predeterminada del nodo.

Tenga en cuenta los siguientes requisitos y detalles para la puerta de enlace de red de administración:

- La pasarela de red de administración es necesaria si las conexiones se realizarán desde fuera de la subred de la red de administración o si se configuran varias subredes de la red de administración.
- Se crean rutas estáticas para cada subred configurada en la lista de subredes de red de administración del nodo.

Red cliente

La red cliente es opcional. Cuando se la configura, se utiliza para proporcionar acceso a los servicios grid para aplicaciones cliente como S3 y Swift. Si piensa hacer que los datos de StorageGRID sean accesibles para un recurso externo (por ejemplo, un pool de almacenamiento en cloud o el servicio de replicación de CloudMirror

de StorageGRID), el recurso externo también puede usar la red de clientes. Los nodos de grid pueden comunicarse con cualquier subred accesible a través de la puerta de enlace de red del cliente.

Puede elegir qué nodos de grid deben tener activada la red de cliente. Todos los nodos no tienen que estar en la misma red cliente, y los nodos nunca se comunicarán entre sí a través de la red cliente. La red de cliente no se pone en funcionamiento hasta que se completa la instalación de la red.

Para mayor seguridad, puede especificar que la interfaz de red de cliente de un nodo no sea de confianza, de modo que la red de cliente sea más restrictiva de la que se permitan las conexiones. Si la interfaz de red de cliente de un nodo no es de confianza, la interfaz acepta conexiones salientes como las que utiliza la replicación de CloudMirror, pero solo acepta conexiones entrantes en puertos que se han configurado explícitamente como extremos de equilibrador de carga. Consulte "Gestionar los controles del firewall" y.. "Configurar puntos finales del equilibrador de carga".

Cuando utiliza una red cliente, no es necesario que el tráfico de cliente se desplace por la red de red de red. El tráfico de red de cuadrícula puede separarse en una red segura que no se puede enrutar. Los siguientes tipos de nodo se configuran con frecuencia con una red de cliente:

- Nodos de puerta de enlace, debido a que estos nodos proporcionan acceso al servicio de equilibrado de carga de StorageGRID y acceso de clientes S3 y Swift a la grid.
- Nodos de almacenamiento, ya que estos nodos proporcionan acceso a los protocolos S3 y Swift, así como a los pools de almacenamiento en cloud y al servicio de replicación de CloudMirror.
- Los nodos de administración, para garantizar que los usuarios inquilinos se puedan conectar al Administrador de inquilinos sin tener que utilizar la red de administración.

Tenga en cuenta lo siguiente para la puerta de enlace de red de cliente:

- La puerta de enlace de red de cliente es necesaria si la red de cliente está configurada.
- La puerta de enlace de red de cliente se convierte en la ruta predeterminada para el nodo de la cuadrícula cuando finaliza la configuración de la cuadrícula.

Redes VLAN opcionales

Según sea necesario, de forma opcional, puede utilizar redes de LAN virtual (VLAN) para el tráfico de clientes y para algunos tipos de tráfico de administración. Sin embargo, el tráfico de red no puede utilizar una interfaz VLAN. El tráfico interno de StorageGRID entre nodos siempre debe utilizar la red de cuadrícula en eth0.

Para admitir las VLAN, debe configurar una o varias interfaces en un nodo como interfaces troncales en el switch. Puede configurar la interfaz de red de grid (eth0) o la interfaz de red de cliente (eth2) para que sea una línea troncal, o puede agregar interfaces troncales al nodo.

Si eth0 está configurado como troncal, el tráfico de red de cuadrícula fluye a través de la interfaz nativa del tronco, como se ha configurado en el switch. De forma similar, si eth2 está configurado como una conexión troncal y la red cliente también está configurada en el mismo nodo, la red cliente utiliza la VLAN nativa del puerto troncal como configurada en el switch.

Solo se admite en redes VLAN el tráfico de administración entrante, como se usa para el tráfico SSH, Grid Manager o Tenant Manager. El tráfico saliente, como se usa para NTP, DNS, LDAP, KMS y los pools de almacenamiento en cloud, no se admite a través de redes VLAN.

> Las interfaces de VLAN solo se pueden añadir a los nodos de administración y a los nodos de puerta de enlace. No se puede usar una interfaz de VLAN para el acceso de cliente o de administrador a los nodos de almacenamiento o los nodos de archivado.

Consulte "Configure las interfaces VLAN" si desea obtener instrucciones y directrices.

Las interfaces VLAN solo se usan en grupos de alta disponibilidad y se asignan direcciones VIP en el nodo activo. Consulte "Gestión de grupos de alta disponibilidad" si desea obtener instrucciones y directrices.

Ejemplos de topología de red

Topología de red de cuadrícula

La topología de red más sencilla se crea configurando la red de cuadrícula únicamente.

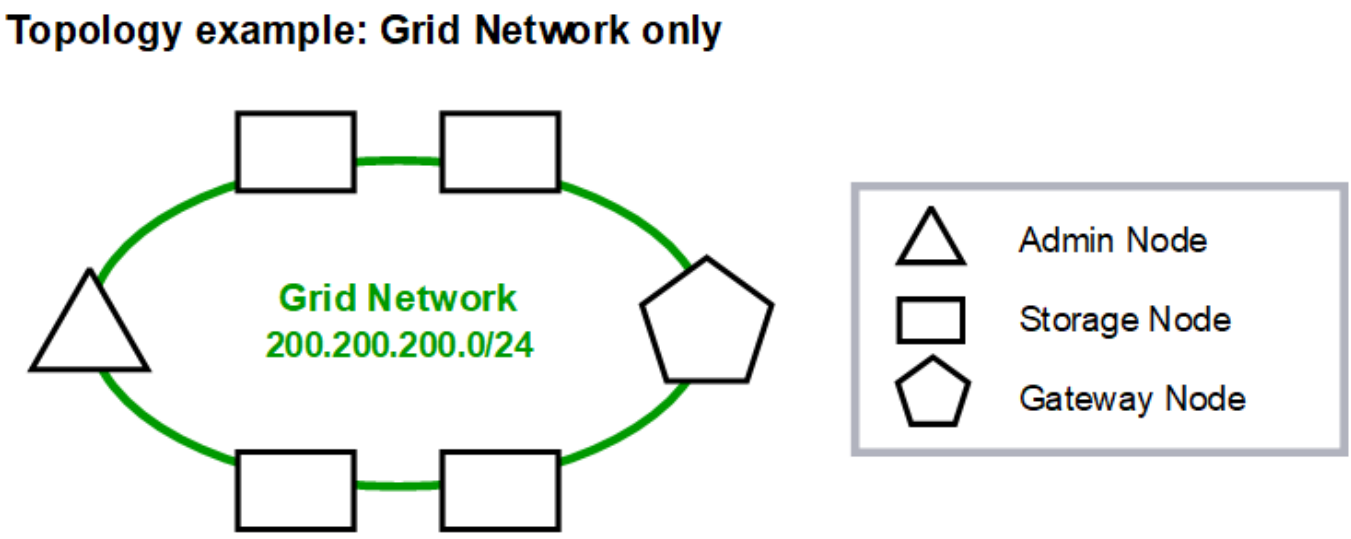
Al configurar Grid Network, se establecen la dirección IP del host, la máscara de subred y la dirección IP de la puerta de enlace para la interfaz eth0 de cada nodo de la cuadrícula.

Durante la configuración, debe agregar todas las subredes de red de cuadrícula a la Lista de subredes de red de cuadrícula (GNSL). Esta lista incluye todas las subredes de todos los sitios y podría incluir también subredes externas que proporcionan acceso a servicios críticos como NTP, DNS o LDAP.

En la instalación, la interfaz de red de cuadrícula aplica rutas estáticas para todas las subredes de la GNSL y establece la ruta predeterminada del nodo a la puerta de enlace de red de cuadrícula si se ha configurado alguna. GNSL no es necesario si no hay ninguna red de cliente y la puerta de enlace de red de cuadrícula es la ruta predeterminada del nodo. También se generan rutas de host a todos los demás nodos de la cuadrícula.

En este ejemplo, todo el tráfico comparte la misma red, incluido el tráfico relacionado con las solicitudes de clientes S3 y Swift, y las funciones de administración y mantenimiento.

> ⓘ Esta topología es adecuada para implementaciones de un único sitio que no están disponibles externamente, implementaciones de prueba de concepto o de prueba, o cuando un equilibrador de carga de terceros actúa como límite de acceso del cliente. Cuando sea posible, la red de red debe utilizarse exclusivamente para el tráfico interno. Tanto la red de administración como la red de cliente tienen restricciones de firewall adicionales que bloquean el tráfico externo a los servicios internos. Se admite el uso de Grid Network para el tráfico de clientes externos, pero este uso ofrece menos capas de protección.



Provisioned

GNSL → 200.200.200.0/24		
	Grid Network	
Nodes	**IP/mask**	**Gateway**
Admin	200.200.200.32/24	200.200.200.1
Storage	200.200.200.33/24	200.200.200.1
Storage	200.200.200.34/24	200.200.200.1
Storage	200.200.200.35/24	200.200.200.1
Storage	200.200.200.36/24	200.200.200.1
Gateway	200.200.200.37/24	200.200.200.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	200.200.200.1	Default	Grid Network gateway
	200.200.200.0/24	→	eth0	Link	Interface IP/mask

Topología de red de administrador

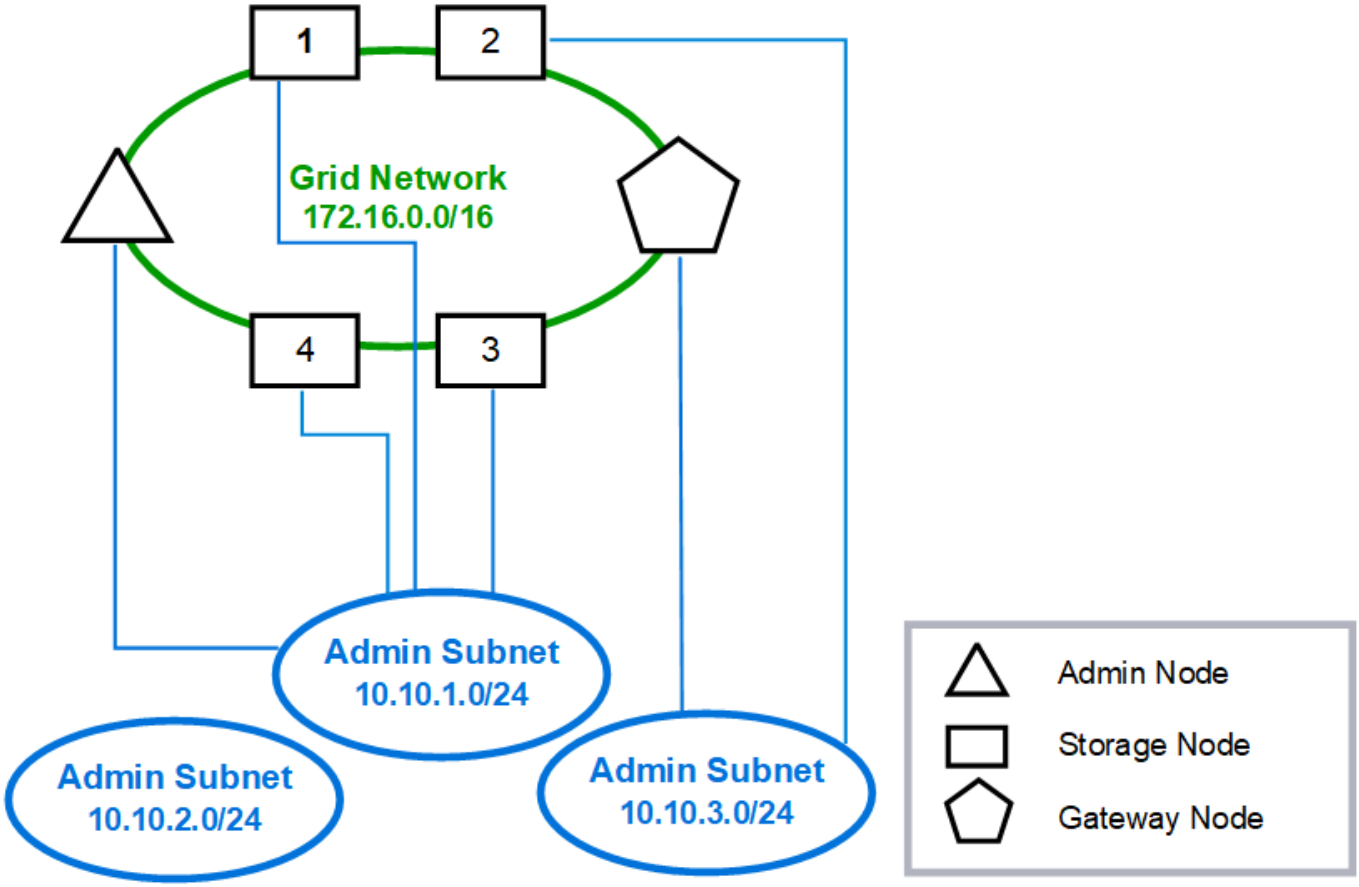
Tener una red Admin es opcional. Una forma de utilizar una red administrativa y una red de grid es configurar una red Grid enrutable y una red de administración limitada para cada nodo.

Cuando se configura la red de administración, se establece la dirección IP del host, la máscara de subred y la dirección IP de puerta de enlace para la interfaz eth1 de cada nodo de cuadrícula.

La red de administrador puede ser única para cada nodo y puede estar compuesta de varias subredes. Cada nodo se puede configurar con una lista de subredes externas de administración (AESL). ESL enumera las subredes a las que se puede acceder a través de la red de administración para cada nodo. ESL también debe incluir las subredes de cualquier servicio al que la cuadrícula acceda a través de la Red de administración, como NTP, DNS, KMS y LDAP. Las rutas estáticas se aplican para cada subred en el ESL.

En este ejemplo, la red de grid se utiliza para el tráfico relacionado con las solicitudes de cliente S3 y Swift y la gestión de objetos. Mientras que la red de administración se utiliza para funciones administrativas.

Topology example: Grid and Admin Networks



Provisioned

GNSL → 172.16.0.0/16
AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

	Grid Network		Admin Network	
Nodes	**IP/mask**	**Gateway**	**IP/mask**	**Gateway**
Admin	172.16.200.32/24	172.16.200.1	10.10.1.10/24	10.10.1.1
Storage 1	172.16.200.33/24	172.16.200.1	10.10.1.11/24	10.10.1.1
Storage 2	172.16.200.34/24	172.16.200.1	10.10.3.65/24	10.10.3.1
Storage 3	172.16.200.35/24	172.16.200.1	10.10.1.12/24	10.10.1.1
Storage 4	172.16.200.36/24	172.16.200.1	10.10.1.13/24	10.10.1.1
Gateway	172.16.200.37/24	172.16.200.1	10.10.3.66/24	10.10.3.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	172.16.200.1	Default	Grid Network gateway
Admin, Storage 1, 3, and 4	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	eth1	Link	Interface IP/mask
	10.10.2.0/24	→	10.10.1.1	Static	AESL
	10.10.3.0/24	→	10.10.1.1	Static	AESL
Storage 2, Gateway	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	10.10.3.1	Static	AESL
	10.10.2.0/24	→	10.10.3.1	Static	AESL
	10.10.3.0/24	→	eth1	Link	Interface IP/mask

Topología de la red de cliente

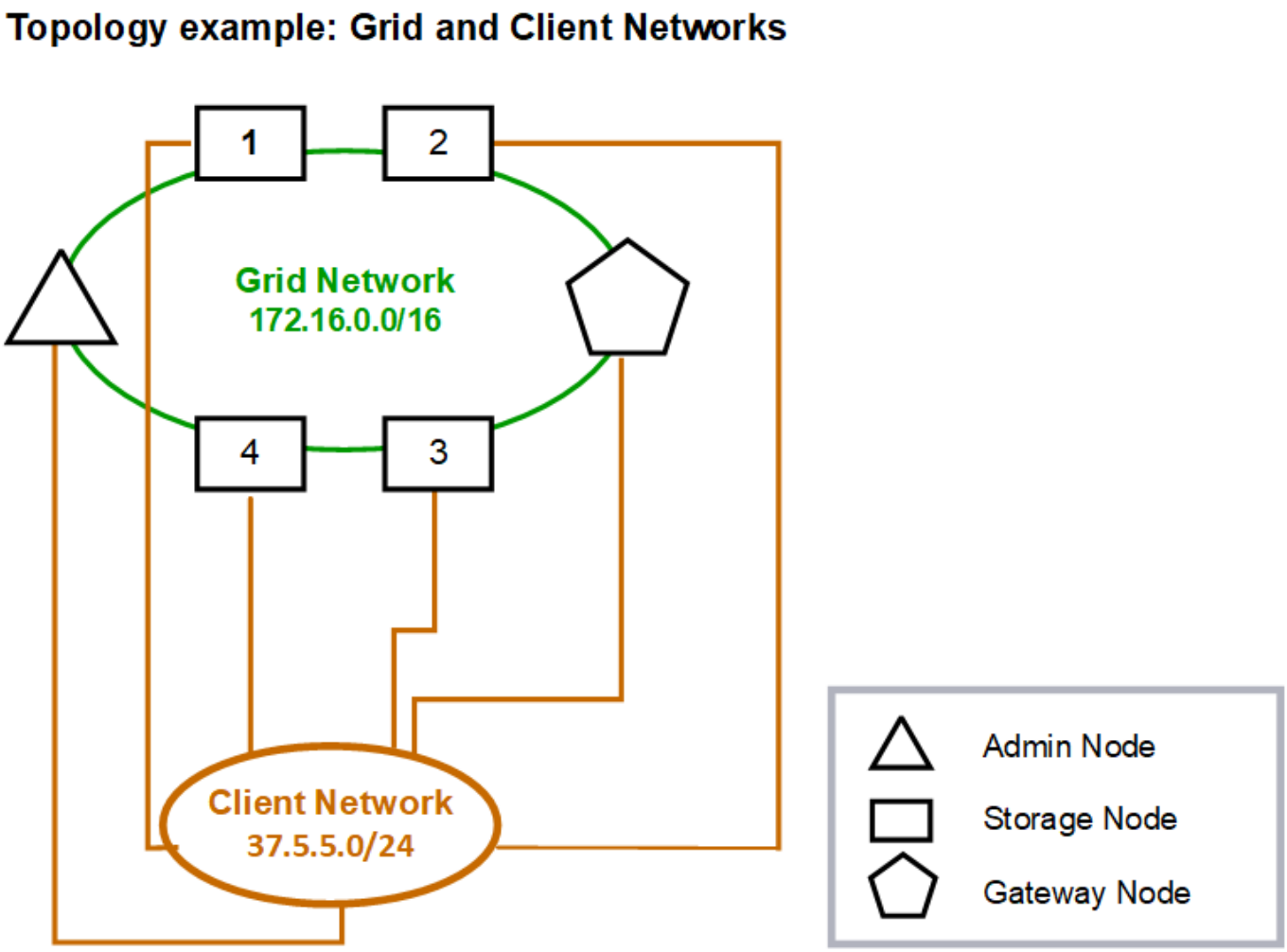
Tener una red cliente es opcional. Al usar una red de cliente, el tráfico de red de cliente (por ejemplo, S3 y Swift) se puede separar del tráfico interno de la cuadrícula, lo que permite que las redes de grid estén más seguras. El tráfico administrativo puede ser gestionado por el cliente o la red de cuadrícula cuando la red de administración no está configurada.

Cuando configura la red de cliente, establece la dirección IP del host, la máscara de subred y la dirección IP de puerta de enlace para la interfaz eth2 del nodo configurado. La red de cliente de cada nodo puede ser independiente de la red de cliente en cualquier otro nodo.

Si configura una red de cliente para un nodo durante la instalación, la puerta de enlace predeterminada del nodo cambia de la puerta de enlace de red de cuadrícula a la puerta de enlace de red de cliente cuando se completa la instalación. Si se añade más tarde una red de cliente, la puerta de enlace predeterminada del nodo se cambia de la misma manera.

En este ejemplo, la red de cliente se utiliza para solicitudes de clientes S3 y Swift y para funciones

administrativas, mientras que la red de grid se dedica a operaciones de gestión de objetos internos.



Provisioned

GNSL → 172.16.0.0/16			
	Grid Network	Client Network	
Nodes	IP/mask	IP/mask	Gateway
Admin	172.16.200.32/24	37.5.5.10/24	37.5.5.1
Storage	172.16.200.33/24	37.5.5.11/24	37.5.5.1
Storage	172.16.200.34/24	37.5.5.12/24	37.5.5.1
Storage	172.16.200.35/24	37.5.5.13/24	37.5.5.1
Storage	172.16.200.36/24	37.5.5.14/24	37.5.5.1
Gateway	172.16.200.37/24	37.5.5.15/24	37.5.5.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	37.5.5.1	Default	Client Network gateway
	172.16.0.0/16	→	eth0	Link	Interface IP/mask
	37.5.5.0/24	→	eth2	Link	Interface IP/mask

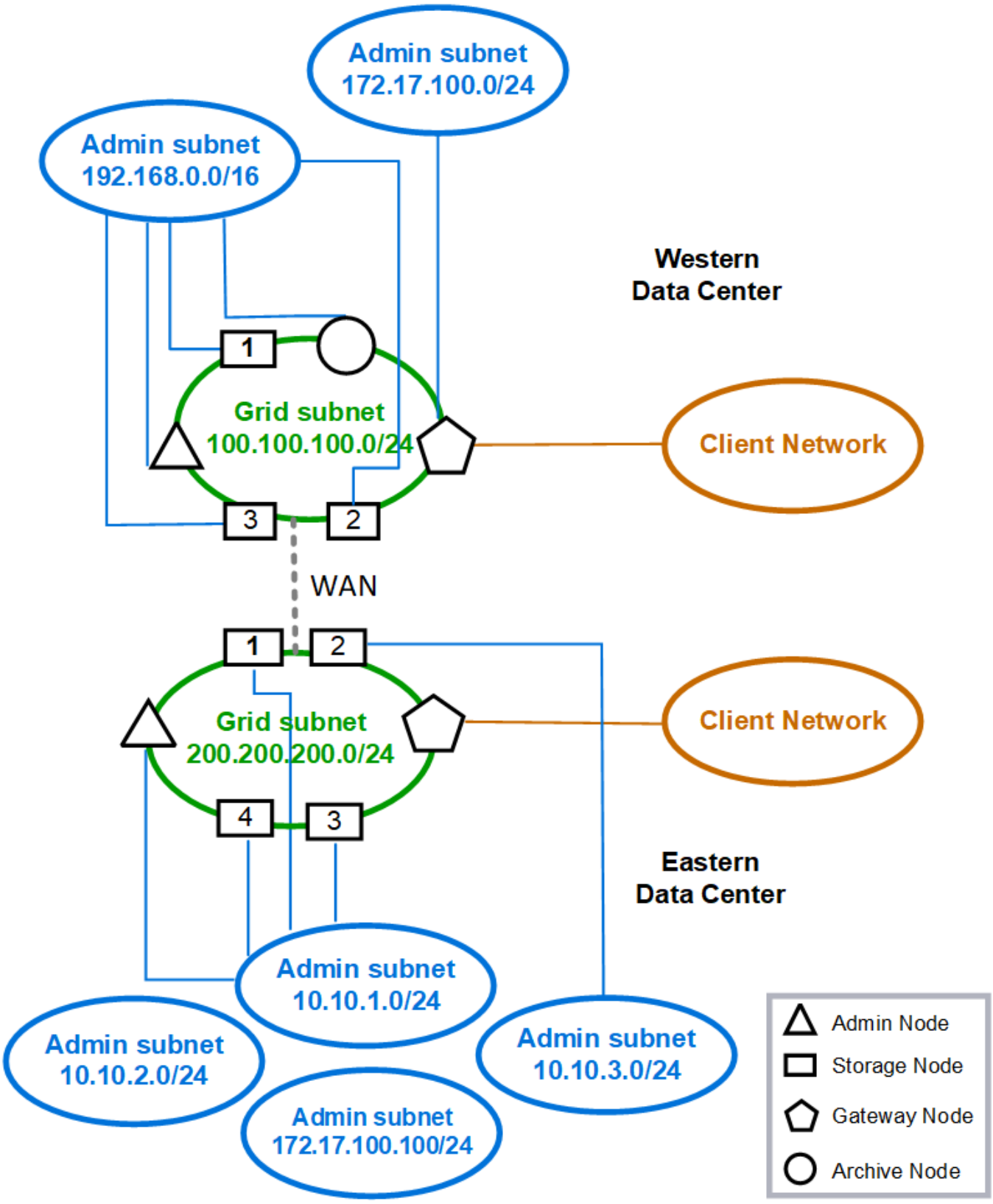
Topología para las tres redes

Puede configurar las tres redes en una topología de red que consiste en una red de red privada, redes de administración específicas de un sitio limitado y redes de cliente abiertas. El uso de puntos finales de equilibrador de carga y redes de cliente que no sean de confianza puede proporcionar seguridad adicional si es necesario.

En este ejemplo:

- La red de cuadrícula se utiliza para el tráfico de red relacionado con las operaciones de gestión de objetos internos.
- La red de administración se utiliza para el tráfico relacionado con funciones administrativas.
- La red de cliente se utiliza para el tráfico relacionado con las solicitudes de clientes S3 y Swift.

Topology example: Grid, Admin, and Client Networks



Requisitos de red

Debe verificar que la infraestructura y la configuración de redes actuales pueden admitir el diseño de red StorageGRID planificado.

Requisitos generales de red

Todas las puestas en marcha de StorageGRID deben admitir las siguientes conexiones.

Estas conexiones se pueden realizar a través de las redes Grid, Admin o Client o las combinaciones de estas redes, como se ilustra en los ejemplos de topología de red.

- **Conexiones de administración**: Conexiones de entrada de un administrador al nodo, normalmente a través de SSH. Acceso del navegador web a Grid Manager, al responsable de inquilinos y al instalador de dispositivos de StorageGRID.
- **Conexiones de servidor NTP**: Conexión UDP saliente que recibe una respuesta UDP entrante.

  El nodo de administración primario debe tener acceso al menos un servidor NTP.

- **Conexiones de servidor DNS**: Conexión UDP saliente que recibe una respuesta UDP entrante.
- **Conexiones del servidor LDAP/Active Directory**: Conexión TCP saliente desde el servicio Identity en nodos de almacenamiento.
- **AutoSupport**: Conexión TCP de salida de los nodos Admin a cualquiera de los dos `support.netapp.com` o un proxy configurado por el cliente.
- **Servidor de administración de claves externo**: Conexión TCP de salida desde cada nodo de dispositivo con cifrado de nodos activado.
- Conexiones TCP de entrada desde clientes S3 y Swift.
- Solicitudes salientes de servicios de plataforma de StorageGRID como la replicación de CloudMirror o de los pools de almacenamiento en cloud.

Si StorageGRID no puede contactar con ninguno de los servidores NTP o DNS aprovisionados mediante las reglas de enrutamiento predeterminadas, intentará el contacto automáticamente en todas las redes (Grid, Admin y Client) siempre y cuando se especifiquen las direcciones IP de los servidores DNS y NTP. Si se puede acceder a los servidores NTP o DNS en cualquier red, StorageGRID creará automáticamente reglas de enrutamiento adicionales para garantizar que la red se utilice para todos los futuros intentos de conexión con ella.

Aunque puede utilizar estas rutas de host detectadas automáticamente, en general debe configurar manualmente las rutas DNS y NTP para garantizar la conectividad en caso de que se produzca un error en la detección automática.

Si no está listo para configurar las redes de administración y cliente opcionales durante la implementación, puede configurar estas redes cuando apruebe los nodos de cuadrícula durante los pasos de configuración. Además, puede configurar estas redes después de la instalación mediante la herramienta Cambiar IP (consulte "Configurar las direcciones IP").

Solo se admiten las conexiones de clientes S3 y Swift, así como las conexiones de administración SSH, Grid Manager y inquilino Manager. Conexiones salientes, como los servidores NTP, DNS, LDAP, AutoSupport y KMS, Debe pasar directamente por las interfaces de cliente, administrador o red de grid. Si la interfaz se configura como una conexión troncal para admitir interfaces VLAN, este tráfico fluirá por la VLAN nativa de la interfaz, tal como se configuró en el switch.

Redes de área extensa (WAN) para varios sitios

Al configurar un sistema StorageGRID con varios sitios, la conexión WAN entre sitios debe tener un ancho de banda mínimo de 25 Mbit/segundo en cada dirección antes de tener en cuenta el tráfico de clientes. La replicación de datos o el código de borrado entre sitios, la expansión de nodos o sitios, la recuperación de nodos y otras operaciones o configuraciones requerirán un ancho de banda adicional.

Los requisitos mínimos reales de ancho de banda WAN dependen de la actividad del cliente y del esquema de protección de ILM. Para obtener ayuda para calcular los requisitos mínimos de ancho de banda WAN, póngase en contacto con su asesor de los servicios profesionales de NetApp.

Conexiones para nodos de administrador y nodos de puerta de enlace

Los nodos de administración siempre deben estar protegidos de clientes que no son de confianza, como los que están en la Internet abierta. Debe asegurarse de que ningún cliente que no sea de confianza puede acceder a un nodo de administración en la red de grid, la red de administración o la red de cliente.

Los nodos de administración y los nodos de puerta de enlace que planea añadir a grupos de alta disponibilidad se deben configurar con una dirección IP estática. Para obtener más información, consulte "Gestión de grupos de alta disponibilidad".

Uso de la traducción de direcciones de red (NAT)

No utilice la traducción de direcciones de red (NAT) en la red de grid entre nodos de grid o entre sitios de StorageGRID. Cuando utilice direcciones IPv4 privadas para la red de cuadrícula, esas direcciones deben poder enrudarse directamente desde cada nodo de cuadrícula de cada sitio. Sin embargo, según sea necesario, puede utilizar NAT entre clientes externos y nodos de cuadrícula, como para proporcionar una dirección IP pública para un nodo de puerta de enlace. El uso de NAT para tender un segmento de red pública sólo se admite cuando se emplea una aplicación de túnel que es transparente para todos los nodos de la cuadrícula, lo que significa que los nodos de la cuadrícula no necesitan conocimientos de direcciones IP públicas.

Requisitos específicos de la red

Siga los requisitos para cada tipo de red StorageGRID.

Routers y puertas de enlace de red

- Si se establece, la puerta de enlace para una red determinada debe estar dentro de la subred de la red específica.
- Si configura una interfaz con direcciones estáticas, debe especificar una dirección de puerta de enlace distinta de 0.0.0.0.
- Si no tiene una puerta de enlace, lo mejor es establecer la dirección de la puerta de enlace para que sea la dirección IP de la interfaz de red.

Subredes

> Cada red debe estar conectada a su propia subred que no se superponga con ninguna otra red del nodo.

Grid Manager aplica las siguientes restricciones durante la implementación. Se proporcionan aquí para ayudar en la planificación de la red previa al despliegue.

- La máscara de subred para cualquier dirección IP de red no puede ser 255.255.255.254 o 255.255.255.255 (/31 o /32 en notación CIDR).
- La subred definida por una dirección IP de interfaz de red y una máscara de subred (CIDR) no puede superponer la subred de ninguna otra interfaz configurada en el mismo nodo.
- La subred de red de cuadrícula para cada nodo debe estar incluida en el GNSL.
- La subred de la red de administración no puede superponerse con la subred de la red de red de red, la subred de la red de cliente o cualquier subred de la GNSL.
- Las subredes de la AESL no pueden superponerse con ninguna subred de la GNSL.
- La subred de la red cliente no puede superponerse con la subred de la red de red de red, la subred de la red de administración, ninguna subred de la GNSL ni ninguna subred de la AESL.

Red Grid

- En el momento de la implementación, cada nodo de grid se debe conectar a la red de grid y debe ser capaz de comunicarse con el nodo administrador principal mediante la configuración de red especificada al implementar el nodo.
- Durante las operaciones normales de grid, cada nodo de grid debe poder comunicarse con los demás nodos de grid a través de la red de cuadrícula.

> Grid Network debe poder enrutar directamente entre cada nodo. No se admite la traducción de direcciones de red (NAT) entre nodos.

- Si la red de cuadrícula consta de varias subredes, agréguelas a la Lista de subredes de red de cuadrícula (GNSL). Las rutas estáticas se crean en todos los nodos de cada subred en el GNSL.
- Si la interfaz de red de cuadrícula está configurada como una conexión troncal para admitir interfaces VLAN, la VLAN nativa de la conexión debe ser la VLAN utilizada para el tráfico de red de red de red de red de red de red de red. Debe accederse a todos los nodos de grid a través de la VLAN nativa del tronco.

Red de administración

La red administrativa es opcional. Si planea configurar una red de administración, siga estos requisitos y directrices.

Los usos típicos de la red de administración incluyen conexiones de administración, AutoSupport, KMS y conexiones a servidores críticos como NTP, DNS y LDAP si estas conexiones no se proporcionan a través de la red de grid o la red de cliente.

> La Red de administración y ESL pueden ser exclusivos de cada nodo, siempre que se pueda acceder a los servicios de red y clientes deseados.

> Debe definir al menos una subred en la red de administración para habilitar las conexiones entrantes desde subredes externas. Las rutas estáticas se generan automáticamente en cada nodo para cada subred de la ESL.

Red cliente

La red cliente es opcional. Si planea configurar una red de cliente, tenga en cuenta las siguientes consideraciones.

- La red de clientes está diseñada para admitir el tráfico de clientes S3 y Swift. Si se configura, la puerta de enlace de red de cliente se convierte en la puerta de enlace predeterminada del nodo.
- Si utiliza una red de cliente, puede ayudar a proteger StorageGRID de ataques hostiles aceptando tráfico de cliente entrante sólo en puntos finales de equilibrador de carga configurados explícitamente. Consulte "Configurar puntos finales del equilibrador de carga".
- Si la interfaz de red de cliente está configurada como troncal para admitir interfaces VLAN, considere si es necesario configurar la interfaz de red de cliente (eth2). Si se configura, el tráfico de red de cliente fluirá a través de la VLAN nativa del tronco, como se configuró en el switch.

Consideraciones sobre redes específicas de la implementación

Implementaciones de Linux

Para obtener eficiencia, fiabilidad y seguridad, el sistema StorageGRID se ejecuta en Linux como una colección de motores de contenedor. No se requiere una configuración de red relacionada con el motor del contenedor en un sistema StorageGRID.

Utilice un dispositivo que no sea de vínculo, como un par VLAN o Ethernet virtual (veth), para la interfaz de red del contenedor. Especifique este dispositivo como la interfaz de red en el archivo de configuración del nodo.

> No utilice dispositivos de enlace o puente directamente como interfaz de red de contenedor. Hacerlo podría evitar el arranque de nodos debido a un problema de kernel con el uso de macvlan con dispositivos de enlace y puente en el espacio de nombres de contenedores.

Consulte las instrucciones de instalación para "Red Hat Enterprise Linux" o. "Ubuntu o Debian" implementaciones.

Configuración de red host para puestas en marcha del motor de contenedores

Antes de iniciar la implementación de StorageGRID en una plataforma de motor de contenedores, determine qué redes (grid, administrador, cliente) utilizará cada nodo. Debe asegurarse de que la interfaz de red de cada nodo esté configurada en la interfaz de host virtual o física correcta y que cada red tenga el ancho de banda suficiente.

Hosts físicos

Si utiliza hosts físicos para dar soporte a los nodos de grid:

- Asegúrese de que todos los hosts utilicen la misma interfaz de host para cada interfaz de nodo. Esta estrategia simplifica la configuración del host y permite la migración de nodos futura.
- Obtenga una dirección IP para el propio host físico.

> El host puede usar una interfaz física del host en sí y uno o más nodos que se ejecutan en el host. Todas las direcciones IP asignadas al host o los nodos que utilizan esta interfaz deben ser únicas. El host y el nodo no pueden compartir direcciones IP.

- Abra los puertos requeridos en el host.
- Si piensa utilizar interfaces VLAN en StorageGRID, el host debe tener una o varias interfaces troncales en las que se pueda acceder a las VLAN deseadas. Estas interfaces se pueden pasar al contenedor de nodos como eth0, eth2 o como interfaces adicionales. Para añadir enlaces troncales o interfaces de acceso, consulte lo siguiente:

- **RHEL (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
- **Ubuntu o Debian (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
- **RHEL, Ubuntu o Debian (después de instalar el nodo)**: "Linux: Añada tronco o interfaces de acceso a un nodo"

Recomendaciones mínimas de ancho de banda

En la siguiente tabla, se presentan las recomendaciones mínimas de ancho de banda LAN para cada tipo de nodo StorageGRID y cada tipo de red. Debe aprovisionar cada host físico o virtual con suficiente ancho de banda de red para satisfacer los requisitos mínimos del agregado de ancho de banda para la cantidad total y el tipo de nodos StorageGRID que planea ejecutar en ese host.

Tipo de nodo	Tipo de red		
	Cuadrícula	Admin	Cliente
	• Ancho de banda LAN mínimo*	Admin	10 Gbps
1 Gbps	1 Gbps	Puerta de enlace	10 Gbps
1 Gbps	10 Gbps	Reducida	10 Gbps
1 Gbps	10 Gbps	Archivado	10 Gbps

> En esta tabla no se incluye el ancho de banda SAN, el cual es necesario para acceder al almacenamiento compartido. Si utiliza almacenamiento compartido al que se accede a través de Ethernet (iSCSI o FCoE), debe aprovisionar interfaces físicas independientes en cada host para proporcionar un ancho DE banda SAN suficiente. Para evitar presentar un cuello de botella, el ancho DE banda SAN de un host determinado debe igualar prácticamente el ancho de banda de red del nodo de almacenamiento agregado para todos los nodos de almacenamiento que se ejecuten en ese host.

Utilice la tabla para determinar el número mínimo de interfaces de red que se deben aprovisionar en cada host, según el número y el tipo de nodos StorageGRID que piensa ejecutar en ese host.

Por ejemplo, para ejecutar un nodo de administrador, un nodo de puerta de enlace y un nodo de almacenamiento en un solo host:

- Conectar las redes Grid y Admin en el nodo Admin (requiere 10 + 1 = 11 Gbps)
- Conecte las redes Grid y Client en el nodo Gateway (requiere 10 + 10 = 20 Gbps)
- Conectar la red de grid en el nodo de almacenamiento (requiere 10 Gbps)

En este escenario, debe proporcionar un mínimo de 11 + 20 + 10 = 41 Gbps de ancho de banda de red, Que podrían ser satisfechas por dos interfaces de 40 Gbps o cinco interfaces de 10 Gbps, potencialmente agregadas en enlaces y luego compartidas por las tres o más VLAN que llevan las subredes Grid, Admin y Client locales al centro de datos físico que contiene el host.

Para obtener algunas maneras recomendadas de configurar los recursos físicos y de red en los hosts del clúster de StorageGRID con el fin de prepararse para la implementación de StorageGRID, consulte lo

siguiente:

- "Configurar la red host (Red Hat Enterprise Linux)"
- "Configurar la red host (Ubuntu o Debian)"

Conexión a redes y puertos para los servicios de plataforma y los pools de almacenamiento en cloud

Si piensa utilizar los servicios de plataforma StorageGRID o los pools de almacenamiento en cloud, debe configurar la red de grid y los firewalls para garantizar que se pueda acceder a los extremos de destino.

Conexión en red para servicios de plataforma

Como se describe en "Gestione servicios de plataforma para clientes" y.. "Gestione los servicios de la plataforma", Los servicios de plataforma incluyen servicios externos que proporcionan integración de búsqueda, notificación de eventos y replicación CloudMirror.

Los servicios de plataforma requieren acceso desde los nodos de almacenamiento que alojan el servicio ADC de StorageGRID a los extremos de servicio externos. Algunos ejemplos para proporcionar acceso son:

- En los nodos de almacenamiento con servicios ADC, configure redes de administración únicas con entradas AESL que se enrutan a los extremos de destino.
- Confíe en la ruta predeterminada proporcionada por una red cliente. Si utiliza la ruta predeterminada, puede utilizar la "Función de red de cliente no confiable" para restringir las conexiones entrantes.

Redes para Cloud Storage Pools

Los pools de almacenamiento en cloud también requieren el acceso de los nodos de almacenamiento a los extremos que proporciona el servicio externo que se utiliza, como el almacenamiento de Amazon S3 Glacier o Microsoft Azure Blob. Para obtener más información, consulte "Qué es un pool de almacenamiento en la nube".

Puertos para los servicios de plataforma y Cloud Storage Pools

De forma predeterminada, los servicios de plataforma y las comunicaciones de Cloud Storage Pool utilizan los puertos siguientes:

- **80**: Para los URI de punto final que comienzan con `http`
- **443**: Para URI de punto final que comienzan con `https`

Se puede especificar un puerto diferente cuando se crea o edita el extremo. Consulte "Referencia de puerto de red".

Si utiliza un servidor proxy no transparente, también debe hacerlo "configure las opciones del proxy de almacenamiento" para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

VLAN y servicios de plataforma y Cloud Storage Pools

No puede utilizar redes VLAN para servicios de plataforma o pools de Cloud Storage. Los extremos de destino deben ser accesibles a través de Grid, Admin o Client Network.

Nodos del dispositivo

Puede configurar los puertos de red en dispositivos StorageGRID para utilizar los modos de enlace de puertos que cumplan con los requisitos de rendimiento, redundancia y conmutación al respaldo.

Los puertos 10/25-GbE de los dispositivos StorageGRID se pueden configurar en modo de enlace fijo o agregado para las conexiones a la red Grid y a la red de clientes.

Los puertos de red administrador de 1 GbE se pueden configurar en modo independiente o activo-Backup para las conexiones a la red administrativa.

Consulte la información sobre los modos de enlace de puertos para su dispositivo:

- "Modos de enlace de puertos (SGF6112)"
- "Modos de enlace de puertos (controladora SG6000-CN)"
- "Modos de enlace de puertos (controladora E5700SG)"
- "Modos de enlace de puertos (SG100 y SG1000)"

Instalación y aprovisionamiento de red

Debe comprender cómo se utilizan Grid Network y las redes de administración y cliente opcionales durante la implementación de nodos y la configuración de grid.

Puesta en marcha inicial de un nodo

Cuando implemente un nodo por primera vez, debe conectar el nodo a la red de grid y asegurarse de que tiene acceso al nodo de administración principal. Si la red de cuadrícula está aislada, puede configurar la red de administración en el nodo de administración principal para el acceso de configuración e instalación desde fuera de la red de cuadrícula.

Una red de cuadrícula con una puerta de enlace configurada se convierte en la puerta de enlace predeterminada para un nodo durante la implementación. La puerta de enlace predeterminada permite que los nodos de grid de las subredes independientes se comuniquen con el nodo de administración principal antes de que se haya configurado la cuadrícula.

Si es necesario, las subredes que contienen servidores NTP o que requieren acceso a Grid Manager o API también se pueden configurar como subredes de cuadrícula.

Registro automático de nodos con el nodo de administración principal

Una vez que los nodos se han implementado, se registran en el nodo de administrador principal mediante la red de grid. A continuación, puede utilizar el administrador de grid, el `configure-storagegrid.py` Python o la API de instalación para configurar la cuadrícula y aprobar los nodos registrados. Durante la configuración de la cuadrícula, puede configurar varias subredes. Las rutas estáticas a estas subredes a través de la puerta de enlace de red de cuadrícula se crearán en cada nodo cuando complete la configuración de la cuadrícula.

Desactivación de la red de administración o de la red de cliente

Si desea desactivar la red de administración o la red de cliente, puede eliminar la configuración de ellos durante el proceso de aprobación del nodo o puede utilizar la herramienta Cambiar IP una vez completada la instalación (consulte "Configurar las direcciones IP").

Directrices posteriores a la instalación

Después de completar la implementación y la configuración de un nodo de grid, siga estas directrices para el direccionamiento DHCP y los cambios de configuración de red.

- Si se utilizó DHCP para asignar direcciones IP, configure una reserva DHCP para cada dirección IP en las redes que se estén utilizando.

  DHCP solo puede configurarse durante la fase de implementación. No puede configurar DHCP durante la configuración.

  > Los nodos se reinician cuando cambian sus direcciones IP, lo que puede provocar interrupciones de servicio si un cambio de dirección DHCP afecta a varios nodos al mismo tiempo.

- Debe usar los procedimientos de cambio IP si desea cambiar direcciones IP, máscaras de subred y puertas de enlace predeterminadas para un nodo de grid. Consulte "Configurar las direcciones IP".
- Si realiza cambios de configuración de redes, incluidos los cambios de enrutamiento y puerta de enlace, es posible que se pierda la conectividad de cliente al nodo de administración principal y a otros nodos de grid. En función de los cambios de red aplicados, es posible que deba restablecer estas conexiones.

Referencia de puerto de red

Debe asegurarse de que la infraestructura de red pueda proporcionar comunicación interna y externa entre los nodos de la cuadrícula y a clientes y servicios externos. Es posible que necesite acceso a través de firewalls internos y externos, sistemas de conmutación y sistemas de enrutamiento.

Utilice los detalles proporcionados para "Comunicaciones internas de los nodos de grid" y.. "Comunicaciones externas" para determinar cómo configurar cada puerto necesario.

Comunicaciones internas de los nodos de grid

El firewall interno de StorageGRID permite conexiones entrantes a puertos específicos de la red de grid. Las conexiones también se aceptan en los puertos definidos por puntos finales del equilibrador de carga.

> NetApp recomienda habilitar el tráfico del protocolo de mensajes de control de Internet (ICMP) entre los nodos de grid. Habilitar el tráfico ICMP puede mejorar el rendimiento de conmutación al respaldo cuando no se puede alcanzar un nodo de grid.

Además de ICMP y los puertos enumerados en la tabla, StorageGRID utiliza el Protocolo de redundancia del enrutador virtual (VRRP). VRRP es un protocolo de Internet que utiliza el número de protocolo IP 112. StorageGRID utiliza VRRP sólo en modo unidifusión. VRRP sólo es necesario si "grupos de alta disponibilidad" están configurados.

Directrices para nodos basados en Linux

Si las políticas de redes empresariales restringen el acceso a cualquiera de estos puertos, puede reasignar puertos en el momento de la implementación mediante un parámetro de configuración de implementación. Para obtener más información acerca de la reasignación de puertos y los parámetros de configuración de

implementación, consulte:

- "Instalar StorageGRID en Red Hat Enterprise Linux"
- "Instalar StorageGRID en Ubuntu o Debian"

Directrices para nodos basados en VMware

Configure los siguientes puertos únicamente si necesita definir restricciones de firewall externas a la red de VMware.

Si las políticas de redes empresariales restringen el acceso a cualquiera de estos puertos, puede reasignar los puertos al implementar nodos mediante VMware vSphere Web Client o mediante un valor de archivo de configuración al automatizar la puesta en marcha de nodos de grid. Para obtener más información acerca de la reasignación de puertos y los parámetros de configuración de implementación, consulte "Instale StorageGRID en VMware".

Directrices para nodos de dispositivos

Si las directivas de redes empresariales restringen el acceso a cualquiera de estos puertos, puede reasignar puertos mediante el instalador de dispositivos de StorageGRID. Consulte "Opcional: Reasignar puertos de red para el dispositivo".

Puertos internos StorageGRID

Puerto	TCP o UDP	De	Para	Detalles
22	TCP	Nodo de administrador principal	Todos los nodos	Para realizar procedimientos de mantenimiento, el nodo administrador principal debe poder comunicarse con los demás nodos mediante SSH en el puerto 22. Permitir el tráfico SSH desde otros nodos es opcional.
80	TCP	Dispositivos	Nodo de administrador principal	Lo usan los dispositivos StorageGRID para comunicarse con el nodo administrador principal para iniciar la instalación.
123	UDP	Todos los nodos	Todos los nodos	Servicio de protocolo de hora de red. Cada nodo sincroniza su hora con todos los demás nodos mediante NTP.
443	TCP	Todos los nodos	Nodo de administrador principal	Se utiliza para comunicar el estado al nodo de administración principal durante la instalación y otros procedimientos de mantenimiento.
1055	TCP	Todos los nodos	Nodo de administrador principal	Tráfico interno para instalación, expansión, recuperación y otros procedimientos de mantenimiento.
1139	TCP	Nodos de almacenamiento	Nodos de almacenamiento	Tráfico interno entre los nodos de almacenamiento.

Puerto	TCP o UDP	De	Para	Detalles
1501	TCP	Todos los nodos	Nodos de almacenamiento con ADC	Generación de informes, auditoría y tráfico interno de configuración.
1502	TCP	Todos los nodos	Nodos de almacenamiento	Tráfico interno relacionado con S3 y Swift.
1504	TCP	Todos los nodos	Nodos de administración	Informes del servicio NMS y tráfico interno de configuración.
1505	TCP	Todos los nodos	Nodos de administración	Tráfico interno de servicio AMS.
1506	TCP	Todos los nodos	Todos los nodos	Tráfico interno de estado del servidor.
1507	TCP	Todos los nodos	Nodos de puerta de enlace	Tráfico interno del equilibrador de carga.
1508	TCP	Todos los nodos	Nodo de administrador principal	Tráfico interno de gestión de la configuración.
1509	TCP	Todos los nodos	Nodos de archivado	Tráfico interno del nodo de archivado.
1511	TCP	Todos los nodos	Nodos de almacenamiento	Tráfico interno de metadatos.
7001	TCP	Nodos de almacenamiento	Nodos de almacenamiento	Comunicación del clúster entre nodos TLS de Cassandra.
7443	TCP	Todos los nodos	Nodo de administrador principal	Tráfico interno para instalación, expansión, recuperación, otros procedimientos de mantenimiento e informes de errores.
8011	TCP	Todos los nodos	Nodo de administrador principal	Tráfico interno para instalación, expansión, recuperación y otros procedimientos de mantenimiento.

Puerto	TCP o UDP	De	Para	Detalles
8443	TCP	Nodo de administrador principal	Nodos del dispositivo	Tráfico interno relacionado con el procedimiento de modo de mantenimiento.
9042	TCP	Nodos de almacenamiento	Nodos de almacenamiento	Puerto de cliente Cassandra.
9999	TCP	Todos los nodos	Todos los nodos	Tráfico interno para múltiples servicios. Incluye procedimientos de mantenimiento, mediciones y actualizaciones de redes.
10226	TCP	Nodos de almacenamiento	Nodo de administrador principal	Los dispositivos StorageGRID lo utilizan para reenviar paquetes AutoSupport desde E-Series SANtricity System Manager al nodo de administración principal.
10342	TCP	Todos los nodos	Nodo de administrador principal	Tráfico interno para instalación, expansión, recuperación y otros procedimientos de mantenimiento.
11139	TCP	Nodos de almacenamiento/archivado	Nodos de almacenamiento/archivado	Tráfico interno entre los nodos de almacenamiento y los nodos de archivado.
18000	TCP	Nodos de almacenamiento/administrador	Nodos de almacenamiento con ADC	Tráfico interno del servicio de cuentas.
18001	TCP	Nodos de almacenamiento/administrador	Nodos de almacenamiento con ADC	Tráfico interno de Federación de identidades.
18002	TCP	Nodos de almacenamiento/administrador	Nodos de almacenamiento	Tráfico de API interno relacionado con los protocolos de objetos.
18003	TCP	Nodos de almacenamiento/administrador	Nodos de almacenamiento con ADC	Servicios de plataforma tráfico interno.

Puerto	TCP o UDP	De	Para	Detalles
18017	TCP	Nodos de almacenamiento/administrador	Nodos de almacenamiento	Tráfico interno del servicio Data mover para Cloud Storage Pools.
18019	TCP	Nodos de almacenamiento	Nodos de almacenamiento	Tráfico interno del servicio de fragmentos para la codificación de borrado.
18082	TCP	Nodos de almacenamiento/administrador	Nodos de almacenamiento	Tráfico interno relacionado con S3.
18083	TCP	Todos los nodos	Nodos de almacenamiento	Tráfico interno relacionado con Swift.
18086	TCP	Todos los nodos de cuadrícula	Todos los nodos de almacenamiento	Tráfico interno relacionado con el servicio LDR.
18200	TCP	Nodos de almacenamiento/administrador	Nodos de almacenamiento	Estadísticas adicionales acerca de las solicitudes de cliente.
19000	TCP	Nodos de almacenamiento/administrador	Nodos de almacenamiento con ADC	Tráfico interno del servicio Keystone.

Información relacionada

"Comunicaciones externas"

Comunicaciones externas

Los clientes necesitan comunicarse con los nodos de grid para procesar y recuperar contenido. Los puertos utilizados dependen de los protocolos de almacenamiento de objetos seleccionados. Estos puertos deben ser accesibles para el cliente.

Acceso restringido a los puertos

Si las políticas de red de la empresa restringen el acceso a cualquiera de los puertos, puede utilizar "puntos finales del equilibrador de carga" para permitir el acceso a puertos definidos por el usuario.

Reasignación de puertos

Para utilizar sistemas y protocolos como SMTP, DNS, SSH o DHCP, debe reasignar puertos al implementar nodos. Sin embargo, no debe reasignar los puntos finales del equilibrador de carga. Para obtener información sobre la reasignación de puertos, consulte las instrucciones de instalación:

- "Instalar StorageGRID en Red Hat Enterprise Linux"
- "Instalar StorageGRID en Ubuntu o Debian"
- "Instale StorageGRID en VMware"
- "Opcional: Reasignar puertos de red para el dispositivo"

Puertos que se utilizan para comunicaciones externas

En la siguiente tabla se muestran los puertos que se utilizan para el tráfico hacia los nodos.

> En esta lista no se incluyen los puertos que se pueden configurar como "puntos finales del equilibrador de carga".

Puerto	TCP o UDP	Protocolo	De	Para	Detalles
22	TCP	SSH	Portátil de servicio	Todos los nodos	Se requiere acceso SSH o consola para procedimientos con pasos de la consola. Opcionalmente, puede utilizar el puerto 2022 en lugar de 22.
25	TCP	SMTP	Nodos de administración	Servidor de correo electrónico	Se usa para alertas y AutoSupport basado en correo electrónico. Puede anular el valor predeterminado de puerto 25 mediante la página servidores de correo electrónico.
53	TCP/UDP	DNS	Todos los nodos	Servidores DNS	Se utiliza para DNS.
67	UDP	DHCP	Todos los nodos	Servicio DHCP	Si se utiliza de manera opcional para admitir la configuración de red basada en DHCP. El servicio dhclient no se ejecuta para cuadrículas configuradas estáticamente.
68	UDP	DHCP	Servicio DHCP	Todos los nodos	Si se utiliza de manera opcional para admitir la configuración de red basada en DHCP. El servicio dhclient no se ejecuta para redes que utilizan direcciones IP estáticas.
80	TCP	HTTP	Navegador	Nodos de administración	El puerto 80 redirige al puerto 443 para la interfaz de usuario del nodo de administración.
80	TCP	HTTP	Navegador	Dispositivos	El puerto 80 redirige al puerto 8443 para el instalador del dispositivo StorageGRID.

Puerto	TCP o UDP	Protocolo	De	Para	Detalles
80	TCP	HTTP	Nodos de almacenamiento con ADC	AWS	Se utiliza para mensajes de servicios de plataforma enviados a AWS u otros servicios externos que utilizan HTTP. Los inquilinos pueden anular el valor de puerto HTTP predeterminado de 80 al crear un extremo.
80	TCP	HTTP	Nodos de almacenamiento	AWS	Solicitudes de Cloud Storage Pools enviadas a destinos de AWS que utilizan HTTP. Los administradores de grid pueden anular el valor de puerto HTTP predeterminado de 80 al configurar un pool de almacenamiento en el cloud.
111	TCP/UDP	Rpcind	Cliente NFS	Nodos de administración	Utilizado por la exportación de auditoría basada en NFS (portmap). **Nota:** este puerto sólo es necesario si está activada la exportación de auditoría basada en NFS. **Nota:** El soporte para NFS ha sido obsoleto y se eliminará en una versión futura.
123	UDP	NTP	Nodos NTP primarios	NTP externo	Servicio de protocolo de hora de red. Los nodos seleccionados como orígenes NTP primarios también sincronizan las horas del reloj con los orígenes de hora NTP externos.
137	UDP	NetBIOS	Cliente de SMB	Nodos de administración	Lo utiliza la exportación de auditoría basada en SMB para clientes que requieren compatibilidad con NetBIOS. **Nota:** Este puerto solo es necesario si la exportación de auditoría basada en SMB está habilitada.
138	UDP	NetBIOS	Cliente de SMB	Nodos de administración	Lo utiliza la exportación de auditoría basada en SMB para clientes que requieren compatibilidad con NetBIOS. **Nota:** Este puerto solo es necesario si la exportación de auditoría basada en SMB está habilitada.

Puerto	TCP o UDP	Protocolo	De	Para	Detalles
139	TCP	SMB	Cliente de SMB	Nodos de administración	Lo utiliza la exportación de auditoría basada en SMB para clientes que requieren compatibilidad con NetBIOS. **Nota:** Este puerto solo es necesario si la exportación de auditoría basada en SMB está habilitada.
161	TCP/UDP	SNMP	Cliente SNMP	Todos los nodos	Se utiliza para realizar sondeos de SNMP. Todos los nodos proporcionan información básica, mientras que los nodos de administrador también proporcionan datos de alertas y alarmas. El puerto UDP 161 se establece de forma predeterminada cuando está configurado. **Nota:** este puerto sólo es necesario y sólo se abre en el firewall del nodo si SNMP está configurado. Si planea utilizar SNMP, puede configurar puertos alternativos. **Nota:** para obtener más información sobre el uso de SNMP con StorageGRID, póngase en contacto con su representante de cuentas de NetApp.
162	TCP/UDP	Notificaciones SNMP	Todos los nodos	Destinos de notificaciones	Las notificaciones y capturas de SNMP salientes se muestran de forma predeterminada en el puerto UDP 162. **Nota:** este puerto sólo es necesario si SNMP está activado y los destinos de notificación están configurados. Si planea utilizar SNMP, puede configurar puertos alternativos. **Nota:** para obtener más información sobre el uso de SNMP con StorageGRID, póngase en contacto con su representante de cuentas de NetApp.
389	TCP/UDP	LDAP	Nodos de almacenamiento con ADC	Active Directory/LDAP	Se utiliza para conectarse a un servidor Active Directory o LDAP para la Federación de identidades.

Puerto	TCP o UDP	Protocolo	De	Para	Detalles
443	TCP	HTTPS	Navegador	Nodos de administración	Lo utilizan los exploradores web y los clientes de API de administración para acceder a Grid Manager y a arrendatario Manager. **Nota**: Si cierra los puertos 443 o 8443 de Grid Manager, cualquier usuario conectado actualmente a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones con privilegios. Consulte "Configurar los controles del firewall" Para configurar direcciones IP con privilegios.
443	TCP	HTTPS	Nodos de administración	Active Directory	Lo utilizan los nodos de administrador que se conectan a Active Directory si el inicio de sesión único (SSO) está habilitado.
443	TCP	HTTPS	Nodos de archivado	Amazon S3	Se usa para acceder a Amazon S3 desde nodos de archivado.
443	TCP	HTTPS	Nodos de almacenamiento con ADC	AWS	Se utiliza para los mensajes de servicios de la plataforma enviados a AWS u otros servicios externos que utilizan HTTPS. Los inquilinos pueden sustituir el valor de puerto HTTP predeterminado de 443 al crear un punto final.
443	TCP	HTTPS	Nodos de almacenamiento	AWS	Solicitudes de pools de almacenamiento en la nube enviadas a destinos de AWS que usan HTTPS. Los administradores de grid pueden anular el valor predeterminado del puerto HTTPS de 443 al configurar un pool de almacenamiento en el cloud.
445	TCP	SMB	Cliente de SMB	Nodos de administración	Utilizado por la exportación de auditoría basada en SMB. **Nota:** Este puerto solo es necesario si la exportación de auditoría basada en SMB está habilitada.

Puerto	TCP o UDP	Protocolo	De	Para	Detalles
903	TCP	NFS	Cliente NFS	Nodos de administración	Utilizada por la exportación de auditorías basadas en NFS (`rpc.mountd`). **Nota:** este puerto sólo es necesario si está activada la exportación de auditoría basada en NFS. **Nota:** El soporte para NFS ha sido obsoleto y se eliminará en una versión futura.
2022	TCP	SSH	Portátil de servicio	Todos los nodos	Se requiere acceso SSH o consola para procedimientos con pasos de la consola. De manera opcional, puede utilizar el puerto 22 en lugar de 2022.
2049	TCP	NFS	Cliente NFS	Nodos de administración	Utilizada por la exportación de auditoría basada en NFS (nfs). **Nota:** este puerto sólo es necesario si está activada la exportación de auditoría basada en NFS. **Nota:** El soporte para NFS ha sido obsoleto y se eliminará en una versión futura.
5353	UDP	MDNS	Todos los nodos	Todos los nodos	Proporciona el servicio DNS de multidifusión (mDNS) que se utiliza para los cambios de IP de red completa y para la detección de nodos de administración principales durante la instalación, la expansión y la recuperación.
5696	TCP	KMIP	Dispositivo	KMS	Protocolo de interoperabilidad de gestión de claves (KMIP) tráfico externo de los dispositivos configurados para el cifrado de nodos en el servidor de gestión de claves (KMS), a menos que se especifique un puerto diferente en la página de configuración de KMS del instalador de dispositivos de StorageGRID.
8022	TCP	SSH	Portátil de servicio	Todos los nodos	SSH en el puerto 8022 otorga acceso al sistema operativo base en las plataformas de dispositivos y nodos virtuales para que admitan y solucionar problemas. Este puerto no se usa para los nodos basados en Linux (configuración básica) y no es necesario acceder a ellos entre los nodos de grid ni durante las operaciones normales.

Puerto	TCP o UDP	Protocolo	De	Para	Detalles
8443	TCP	HTTPS	Navegador	Nodos de administración	Opcional. Lo utilizan los exploradores web y los clientes API de administración para acceder a Grid Manager. Se puede utilizar para separar las comunicaciones de Grid Manager y de arrendatario Manager. **Nota**: Si cierra los puertos 443 o 8443 de Grid Manager, cualquier usuario conectado actualmente a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones con privilegios. Consulte "Configurar los controles del firewall" Para configurar direcciones IP con privilegios.
9022	TCP	SSH	Portátil de servicio	Dispositivos	Concede acceso a los dispositivos StorageGRID en modo de preconfiguración para soporte y resolución de problemas. No es necesario que este puerto esté accesible entre los nodos de grid ni durante las operaciones normales.
9091	TCP	HTTPS	Servicio Grafana externo	Nodos de administración	Utilizados por servicios de Grafana externos para un acceso seguro al servicio Prometheus de StorageGRID. **Nota:** este puerto sólo es necesario si está habilitado el acceso a Prometheus basado en certificados.
9092	TCP	Kafka	Nodos de almacenamiento con ADC	Clúster de Kafka	Se utiliza para mensajes de servicios de plataforma enviados a un clúster de Kafka. Los inquilinos pueden anular la configuración de puerto Kafka predeterminada de 9092 al crear un punto final.
9443	TCP	HTTPS	Navegador	Nodos de administración	Opcional. Lo utilizan exploradores web y clientes de API de gestión para acceder al administrador de inquilinos. Se puede utilizar para separar las comunicaciones de Grid Manager y de arrendatario Manager.
18082	TCP	HTTPS	Clientes S3	Nodos de almacenamiento	Tráfico del cliente de S3 directamente a los nodos de almacenamiento (HTTPS).

Puerto	TCP o UDP	Protocolo	De	Para	Detalles
18083	TCP	HTTPS	Clientes Swift	Nodos de almacenamiento	El tráfico del cliente de Swift directamente a los nodos de almacenamiento (HTTPS).
18084	TCP	HTTP	Clientes S3	Nodos de almacenamiento	Tráfico de cliente de S3 directamente a los nodos de almacenamiento (HTTP).
18085	TCP	HTTP	Clientes Swift	Nodos de almacenamiento	Tráfico de clientes de Swift directamente a los nodos de almacenamiento (HTTP).
23000-23999	TCP	HTTPS	Todos los nodos en la cuadrícula de origen para la replicación entre grid	Nodos de administración y nodos de puerta de enlace en el grid de destino para la replicación entre grid	Este rango de puertos está reservado para conexiones de federación de grid. Ambas cuadrículas de una conexión determinada utilizan el mismo puerto.

Inicio rápido para StorageGRID

Siga estos pasos generales para configurar y usar cualquier sistema StorageGRID.

1 Aprenda, planifique y recopile datos

Trabaje con su representante de cuenta de NetApp para conocer las opciones y planificar su nuevo sistema StorageGRID. Considere estos tipos de preguntas:

- ¿Cuántos datos de objetos espera almacenar al principio y con el tiempo?
- ¿Cuántos sitios necesita?
- ¿Cuántos y qué tipos de nodos necesita en cada sitio?
- ¿Qué redes StorageGRID utilizará?
- ¿Quién utilizará la cuadrícula para almacenar objetos? ¿Qué aplicaciones usarán?
- ¿Tiene algún requisito especial de seguridad o almacenamiento?
- ¿Necesita cumplir con algún requisito legal o regulatorio?

De manera opcional, colabore con su asesor de servicios profesionales de NetApp para acceder a la herramienta ConfigBuilder de NetApp para completar un libro de configuración para usarlo cuando instale e implemente su nuevo sistema. También puede utilizar esta herramienta para ayudar a automatizar la configuración de cualquier dispositivo StorageGRID. Consulte "Automatice la instalación y configuración de los

dispositivos".

Revisar "Más información sobre StorageGRID" y la "Directrices sobre redes".

2 Instale los nodos

Un sistema StorageGRID consta de nodos individuales basados en hardware y software. Primero se instala el hardware para cada nodo del dispositivo y se configura cada host Linux o VMware.

Para completar la instalación, debe instalar el software StorageGRID en cada dispositivo o host de software y conectar los nodos a un grid. Durante este paso, proporcionará los nombres de sitios y nodos, detalles de subred y direcciones IP para los servidores NTP y DNS.

Descubra cómo:

- "Instale el hardware del dispositivo"
- "Instalar StorageGRID en Red Hat Enterprise Linux"
- "Instalar StorageGRID en Ubuntu o Debian"
- "Instale StorageGRID en VMware"

3 Inicie sesión y compruebe el estado del sistema

En cuanto instale el nodo de administración principal, puede iniciar sesión en Grid Manager. A partir de ahí, puede revisar el estado general del nuevo sistema, habilitar correos electrónicos de alerta y AutoSupport y configurar nombres de dominio de punto final S3.

Descubra cómo:

- "Inicie sesión en Grid Manager"
- "Supervise el estado del sistema"
- "Configure AutoSupport"
- "Configure notificaciones por correo electrónico para las alertas"
- "Configure los nombres de dominio de punto final S3"

4 Configurar y gestionar

Las tareas de configuración necesarias para un nuevo sistema StorageGRID dependen de cómo se utilizará el grid. Como mínimo, debe configurar el acceso al sistema, utilizar los asistentes de FabricPool y S3 y gestionar varias configuraciones de seguridad y almacenamiento.

Descubra cómo:

- "Control del acceso a StorageGRID"
- "Utilice el asistente de configuración de S3"
- "Use el asistente de configuración de FabricPool"
- "Gestionar la seguridad"
- "Endurecimiento del sistema"

5 Configure ILM

Puede controlar la ubicación y la duración de cada objeto en el sistema StorageGRID mediante la configuración de una política de gestión de ciclo de vida de la información (ILM) que consta de una o más reglas de ILM. Las reglas de ILM indican a la StorageGRID cómo crear y distribuir copias de datos de objetos y cómo gestionar esas copias con el tiempo.

Descubra cómo: "Gestión de objetos con ILM"

6 Utilice StorageGRID

Una vez que se completa la configuración inicial, las cuentas de inquilino de StorageGRID pueden usar aplicaciones cliente S3 y Swift para procesar, recuperar y eliminar objetos.

Descubra cómo:

- "Usar una cuenta de inquilino"
- "Usar la API de REST DE S3"
- "Usar la API de REST de Swift"

7 Supervisión y solución de problemas

Cuando el sistema está en funcionamiento, debe supervisar sus actividades de forma regular y solucionar cualquier alerta. Es posible que también desee configurar un servidor de syslog externo, usar la supervisión SNMP o recoger datos adicionales.

Descubra cómo:

- "Supervisar StorageGRID"
- "Solucionar problemas de StorageGRID"

8 Expandir, mantener y recuperar

Puede añadir nodos o sitios para ampliar la capacidad o la funcionalidad del sistema. También puede realizar varios procedimientos de mantenimiento para recuperarse de fallos o mantener el sistema de StorageGRID actualizado y funcionando de forma eficiente.

Descubra cómo:

- "Expanda una cuadrícula"
- "Mantenga su grid"
- "Recuperar nodos"

Instala, actualiza y corrige StorageGRID

Dispositivos StorageGRID

Vaya a. "Documentación del dispositivo StorageGRID" Para saber cómo instalar, configurar y mantener dispositivos de almacenamiento y servicios de StorageGRID.

Instalar StorageGRID en Red Hat Enterprise Linux

Inicio rápido para instalar StorageGRID en Red Hat Enterprise Linux

Siga estos pasos generales para instalar un nodo StorageGRID de Red Hat Enterprise Linux (RHEL) Linux.

1 **Preparación**

- Descubra "Arquitectura de StorageGRID y topología de red".
- Conozca los aspectos específicos de "Redes StorageGRID".
- Reúna y prepare el "Información y materiales requeridos".
- Prepare lo necesario "CPU y RAM".
- Prevea "requisitos de rendimiento y almacenamiento".
- "Prepare los servidores Linux" Que alojará sus nodos de StorageGRID.

2 **Puesta en marcha**

Desplegar nodos de grid. Cuando se implementan nodos de grid, se crean como parte del sistema StorageGRID y se conectan a una o varias redes.

- Para implementar nodos de grid basados en software en los hosts que preparó en el paso 1, utilice la línea de comandos de Linux y. "archivos de configuración de nodos".
- Para poner en marcha los nodos de dispositivos StorageGRID, siga el "Inicio rápido para la instalación de hardware".

3 **Configuración**

Cuando se hayan desplegado todos los nodos, utilice Grid Manager a. "configure la cuadrícula y complete la instalación".

Automatizar la instalación

Para ahorrar tiempo y proporcionar coherencia, puede automatizar la instalación del servicio de host de StorageGRID y la configuración de nodos de grid.

- Use un marco de orquestación estándar como Ansible, Puppet o Chef para automatizar:

- Instalación de RHEL
- La configuración de redes y almacenamiento
- Instalación del motor de contenedor y del servicio de host StorageGRID
- Puesta en marcha de nodos de grid virtual

Consulte "Automatizar la instalación y configuración del servicio de host de StorageGRID".

- Después de implementar los nodos de grid, "Automatice la configuración del sistema StorageGRID" Usando el script de configuración de Python proporcionado en el archivo de instalación.
- "Automatice la instalación y la configuración de los nodos de grid de dispositivos"
- Si es un desarrollador avanzado de implementaciones de StorageGRID, automatice la instalación de los nodos de grid mediante el "Instalación de la API de REST".

Planificar y preparar la instalación en Red Hat

Información y materiales requeridos

Antes de instalar StorageGRID, recopile y prepare la información y los materiales necesarios.

Información obligatoria

Plan de red

Qué redes pretende conectar a cada nodo StorageGRID. StorageGRID admite múltiples redes para la separación del tráfico, la seguridad y la conveniencia administrativa.

Consulte StorageGRID "Directrices sobre redes".

Información de red

A menos que se utilice DHCP, las direcciones IP para asignar a cada nodo de grid y las direcciones IP de los servidores DNS y NTP.

Servidores para nodos de grid

Identificar un conjunto de servidores (físicos, virtuales o ambos) que, agregado, proporcione los recursos suficientes para respaldar el número y el tipo de nodos de StorageGRID que va a implementar.

> Si la instalación de StorageGRID no utilizará nodos de almacenamiento del dispositivo StorageGRID (hardware), debe usar almacenamiento RAID de hardware con caché de escritura respaldada por batería (BBWC). StorageGRID no admite el uso de redes de área de almacenamiento virtuales (VSAN), RAID de software ni ninguna protección RAID.

Migración de nodos (si es necesario)

Comprenda el "requisitos para la migración de nodos", si desea realizar el mantenimiento programado en hosts físicos sin ninguna interrupción del servicio.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Materiales requeridos

Licencia de StorageGRID de NetApp

Debe tener una licencia de NetApp válida y con firma digital.

> En el archivo de instalación de StorageGRID se incluye una licencia que no sea de producción, y que se puede utilizar para pruebas y entornos Grid de prueba de concepto.

Archivo de instalación de StorageGRID

"Descargue el archivo de instalación de StorageGRID y extraiga los archivos".

Portátil de servicio

El sistema StorageGRID se instala a través de un ordenador portátil de servicio.

El portátil de servicio debe tener:

- Puerto de red
- Cliente SSH (por ejemplo, PuTTY)
- "Navegador web compatible"

Documentación de StorageGRID

- "Notas de la versión"
- "Instrucciones para administrar StorageGRID"

Descargue y extraiga los archivos de instalación de StorageGRID

Debe descargar el archivo de instalación de StorageGRID y extraer los archivos necesarios.

Pasos

1. Vaya a la "Página de descargas de NetApp para StorageGRID".
2. Seleccione el botón para descargar la última versión, o seleccione otra versión en el menú desplegable y seleccione **Ir**.
3. Inicie sesión con el nombre de usuario y la contraseña de su cuenta de NetApp.
4. Si aparece una declaración Precaution/MustRead, léala y seleccione la casilla de verificación.

   > Debe aplicar cualquier revisión requerida después de instalar la versión de StorageGRID. Para obtener más información, consulte "procedimiento de revisión en las instrucciones de recuperación y mantenimiento".

5. Lea el Contrato de licencia de usuario final, seleccione la casilla de verificación y, a continuación, seleccione * Aceptar y continuar *.
6. En la columna **Install StorageGRID**, seleccione el archivo .tgz o .zip para Red Hat Enterprise Linux.

   > Seleccione la `.zip` Archivo si está ejecutando Windows en el portátil de servicio.

7. Guarde y extraiga el archivo de archivado.
8. Elija los archivos que necesite en la siguiente lista.

Los archivos que necesite dependen de la topología de cuadrícula planificada y de cómo implementar el sistema StorageGRID.

> Las rutas enumeradas en la tabla son relativas al directorio de nivel superior instalado por el archivo de instalación extraído

Ruta y nombre de archivo	Descripción
	Archivo de texto que describe todos los archivos contenidos en el archivo de descarga de StorageGRID.
	Una licencia gratuita que no proporciona ningún derecho de soporte para el producto.
	Paquete DE RPM para instalar las imágenes de los nodos StorageGRID en los hosts RHEL.
	Paquete DE RPM para instalar el servicio de host StorageGRID en los hosts de RHEL.
Herramienta de secuencia de comandos de la implementación	Descripción
	Script Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Una secuencia de comandos Python que se utiliza para automatizar la configuración de los dispositivos StorageGRID.
	Ejemplo de archivo de configuración para utilizar con `configure-storagegrid.py` guión.
	Ejemplo de secuencia de comandos Python que puede utilizar para iniciar sesión en la API de gestión de grid cuando está activado el inicio de sesión único. También puede utilizar este script para ping federate.
	Un archivo de configuración en blanco para usar con el `configure-storagegrid.py` guión.
	Ejemplo de rol y libro de estrategia de Ansible para configurar hosts de RHEL para la puesta en marcha del contenedor StorageGRID. Puede personalizar el rol o el libro de estrategia según sea necesario.

Ruta y nombre de archivo	Descripción
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de grid cuando se activa el inicio de sesión único (SSO) mediante Active Directory o ping federate.
	Un guion de ayuda llamado por el compañero `storagegrid-ssoauth-azure.py` Script de Python para realizar interacciones SSO con Azure.
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno StorageGRID que no sea de producción para probar la compatibilidad de la actualización.

Requisitos de software para Red Hat Enterprise Linux

Es posible usar una máquina virtual para alojar cualquier tipo de nodo StorageGRID. Se necesita una máquina virtual para cada nodo de grid.

Para instalar StorageGRID en Red Hat Enterprise Linux (RHEL), debe instalar algunos paquetes de software de terceros. Algunas distribuciones de Linux soportadas no contienen estos paquetes por defecto. Las versiones del paquete de software en las que se han probado las instalaciones de StorageGRID incluyen las que se indican en esta página.

> Si selecciona una opción de instalación en tiempo de ejecución de contenedor y distribución de Linux que requiera alguno de estos paquetes y la distribución de Linux no los instala automáticamente, instale una de las versiones que se enumeran aquí, si está disponible en su proveedor o en el proveedor de soporte para su distribución de Linux. De lo contrario, utilice las versiones de paquete predeterminadas disponibles en su proveedor.

> Todas las opciones de instalación requieren Podman o Docker. No instale ambos paquetes. Instale solo el paquete requerido por su opción de instalación.

Versiones de Python probadas

- 3,5.2-2
- 3,6.8-2
- 3,6.8-38
- 3,6.9-1
- 3,7.3-1
- 3,8.10-0

- 3,9.2-1
- 3,9.10-2
- 3,9.16-1
- 3.10.6-1
- 3.11.2-6

Versiones de Podman probadas

- 3,2.3-0
- 3,4.4+ds1
- 4,1.1-7
- 4,2.0-11
- 4,3.1+ds1-8+b1
- 4,4.1-8
- 4,4.1-12

Versiones de Docker probadas

> La compatibilidad de Docker está obsoleta y se eliminará en un lanzamiento futuro.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23,0.6-1
- Docker-CE 24,0.2-1
- Docker-CE 24,0.4-1
- Docker-CE 24,0.5-1
- Docker-CE 24,0.7-1
- 1.5-2

Requisitos de CPU y RAM

Antes de instalar el software StorageGRID, verifique y configure el hardware de manera que esté listo para admitir el sistema StorageGRID.

Cada nodo StorageGRID requiere los siguientes recursos mínimos:

- Núcleos de CPU: 8 por nodo
- RAM: Al menos 24 GB por nodo y de 2 a 16 GB menos que la RAM total del sistema, en función de la RAM total disponible y la cantidad de software que no sea StorageGRID que se ejecute en el sistema

Asegúrese de que el número de nodos StorageGRID que tiene previsto ejecutar en cada host físico o virtual no supere el número de núcleos de CPU o la RAM física disponible. Si los hosts no están dedicados a ejecutar StorageGRID (no se recomienda), asegúrese de tener en cuenta los requisitos de recursos de las otras aplicaciones.

Supervise el uso de la CPU y la memoria de forma regular para garantizar que estos recursos siguen teniendo la capacidad de adaptarse a su carga de trabajo. Por ejemplo, si se dobla la asignación de RAM y CPU de los nodos de almacenamiento virtual, se proporcionarán recursos similares a los que se proporcionan para los nodos de dispositivos StorageGRID. Además, si la cantidad de metadatos por nodo supera los 500 GB, puede aumentar la memoria RAM por nodo a 48 GB o más. Para obtener información sobre la gestión del almacenamiento de metadatos de objetos, el aumento del valor de Espacio Reservado de Metadatos y la supervisión del uso de CPU y memoria, consulte las instrucciones para "administración", "Supervisión", y. "actualizar" StorageGRID

Si la tecnología de subprocesos múltiples está habilitada en los hosts físicos subyacentes, puede proporcionar 8 núcleos virtuales (4 núcleos físicos) por nodo. Si el subprocesamiento no está habilitado en los hosts físicos subyacentes, debe proporcionar 8 núcleos físicos por nodo.

Si utiliza máquinas virtuales como hosts y tiene control del tamaño y el número de máquinas virtuales, debe utilizar una única máquina virtual para cada nodo StorageGRID y ajustar el tamaño de la máquina virtual según corresponda.

Para implementaciones de producción, no debe ejecutar varios nodos de almacenamiento en el mismo hardware de almacenamiento físico o host virtual. Cada nodo de almacenamiento de una única puesta en marcha de StorageGRID debe tener su propio dominio de fallos aislado. Puede maximizar la durabilidad y disponibilidad de los datos de objetos si se asegura de que un único error de hardware solo pueda afectar a un único nodo de almacenamiento.

Consulte también "Los requisitos de almacenamiento y rendimiento".

Los requisitos de almacenamiento y rendimiento

Debe comprender los requisitos de almacenamiento de los nodos de StorageGRID, de tal modo que pueda proporcionar espacio suficiente para admitir la configuración inicial y la ampliación de almacenamiento futura.

Los nodos de StorageGRID requieren tres categorías lógicas de almacenamiento:

- * Container pool* — almacenamiento de nivel de rendimiento (10K SAS o SSD) para los contenedores de nodos, que se asignará al controlador de almacenamiento del motor del contenedor cuando instale y configure el motor del contenedor en los hosts que soportarán sus nodos StorageGRID.
- **Datos del sistema** — almacenamiento de nivel de rendimiento (10K SAS o SSD) para almacenamiento persistente por nodo de datos del sistema y registros de transacciones, que los servicios host StorageGRID consumirán y asignarán a nodos individuales.
- **Almacenamiento masivo de datos de objetos**: Almacenamiento en niveles de rendimiento (10K SAS o SSD) y capacidad (NL-SAS/SATA) para el almacenamiento persistente de datos de objetos y metadatos de objetos.

Se deben utilizar dispositivos de bloques respaldados por RAID para todas las categorías de almacenamiento. No se admiten discos, SSD o JBOD no redundantes. Puede usar almacenamiento RAID compartido o local para cualquiera de las categorías de almacenamiento; sin embargo, si desea usar la funcionalidad de migración de nodos en StorageGRID, debe almacenar tanto los datos del sistema como los datos de objetos en almacenamiento compartido. Para obtener más información, consulte "Requisitos de migración de contenedores de nodos".

Requisitos de rendimiento

El rendimiento de los volúmenes utilizados para el pool de contenedores, los datos del sistema y los metadatos de objetos afecta significativamente el rendimiento general del sistema. Debe usar almacenamiento de nivel de rendimiento (10 000 SAS o SSD) para estos volúmenes a fin de garantizar que el rendimiento de disco sea adecuado en términos de latencia, operaciones de entrada/salida por segundo (IOPS) y rendimiento. Puede usar almacenamiento en niveles de capacidad (NL-SAS/SATA) para el almacenamiento persistente de datos de objetos.

Los volúmenes utilizados para el pool de contenedores, los datos del sistema y los datos de objetos deben tener el almacenamiento en caché de devolución de escritura habilitado. La caché debe estar en un medio protegido o persistente.

Requisitos para hosts que usan almacenamiento de NetApp ONTAP

Si el nodo StorageGRID utiliza almacenamiento asignado de un sistema NetApp ONTAP, confirme que el volumen no tiene una política de organización en niveles de FabricPool habilitada. Al deshabilitar el almacenamiento en niveles de FabricPool para los volúmenes que se usan con los nodos StorageGRID, se simplifica la solución de problemas y las operaciones de almacenamiento.

> No utilice nunca FabricPool para colocar en niveles datos relacionados con StorageGRID en el propio StorageGRID. La organización en niveles de los datos de StorageGRID en StorageGRID aumenta la solución de problemas y la complejidad operativa.

Número de hosts requeridos

Cada sitio StorageGRID requiere como mínimo tres nodos de almacenamiento.

> En una puesta en marcha de producción, no ejecute más de un nodo de almacenamiento en un solo host físico o virtual. El uso de un host dedicado para cada nodo de almacenamiento proporciona un dominio de fallo aislado.

Pueden ponerse en marcha otros tipos de nodos, como los nodos de administrador o los nodos de pasarela, en los mismos hosts o bien en sus propios hosts dedicados, según sea necesario.

Número de volúmenes de almacenamiento para cada host

En la siguiente tabla se muestra el número de volúmenes de almacenamiento (LUN) necesarios para cada host y el tamaño mínimo requerido para cada LUN, en función del cual se pondrán en marcha los nodos en ese host.

El tamaño máximo de LUN probado es 39 TB.

> Estos números son para cada host, no para toda la cuadrícula.

Propósito de LUN	Categoría de almacenamiento	Número de LUN	Tamaño mínimo/LUN
Bloque de almacenamiento del motor del contenedor	Pool de contenedores	1	Número total de nodos × 100 GB

Propósito de LUN	Categoría de almacenamiento	Número de LUN	Tamaño mínimo/LUN
`/var/local` volumen	Datos del sistema	1 para cada nodo de este host	90 GB
Nodo de almacenamiento	Datos de objetos	3 para cada nodo de almacenamiento de este host **Nota:** un nodo de almacenamiento basado en software puede tener de 1 a 16 volúmenes de almacenamiento; se recomiendan al menos 3 volúmenes de almacenamiento.	12 TB (4 TB/LUN) CONSULTE Requisitos de almacenamiento para nodos de almacenamiento si quiere más información.
Nodo de almacenamiento (solo metadatos)	Metadatos de objetos	1	4 TB consulte Requisitos de almacenamiento para nodos de almacenamiento si quiere más información. **Nota**: Solo se requiere un rangedb para los nodos de almacenamiento solo de metadatos.
Registros de auditoría del nodo de administrador	Datos del sistema	1 para cada nodo de administrador de este host	200 GB
Tablas Admin Node	Datos del sistema	1 para cada nodo de administrador de este host	200 GB

En función del nivel de auditoría configurado, el tamaño de las entradas de usuario, como el nombre de clave de objeto S3, Y cuántos datos de registro de auditoría debe conservar, es posible que necesite aumentar el tamaño del LUN del registro de auditoría en cada nodo de administración.Por lo general, un grid genera aproximadamente 1 KB de datos de auditoría por operación de S3. Lo que significaría que un LUN de 200 GB admitiría 70 millones de operaciones al día o 800 operaciones por segundo durante dos o tres días.

Espacio de almacenamiento mínimo para un host

En la siguiente tabla se muestra el espacio de almacenamiento mínimo necesario para cada tipo de nodo. Puede utilizar esta tabla para determinar la cantidad mínima de almacenamiento que debe proporcionar al host en cada categoría de almacenamiento, según la cual se pondrán en marcha los nodos en ese host.

Las instantáneas de disco no se pueden utilizar para restaurar los nodos de grid. En su lugar, consulte "recuperación de nodo de grid" procedimientos para cada tipo de nodo.

Tipo de nodo	Pool de contenedores	Datos del sistema	Datos de objetos
Nodo de almacenamiento	100 GB	90 GB	4.000 GB
Nodo de administración	100 GB	490 GB (3 LUN)	*no aplicable*
Nodo de puerta de enlace	100 GB	90 GB	*no aplicable*
Nodo de archivado	100 GB	90 GB	*no aplicable*

Ejemplo: Calcular los requisitos de almacenamiento para un host

Suponga que planea implementar tres nodos en el mismo host: Un nodo de almacenamiento, un nodo de administración y un nodo de puerta de enlace. Debe proporcionar un mínimo de nueve volúmenes de almacenamiento al host. Necesitará un mínimo de 300 GB de almacenamiento de nivel de rendimiento para los contenedores de nodos, 670 GB de almacenamiento de nivel de rendimiento para los datos del sistema y los registros de transacciones, y 12 TB de almacenamiento de nivel de capacidad para los datos de objetos.

Tipo de nodo	Propósito de LUN	Número de LUN	Tamaño de LUN
Nodo de almacenamiento	Bloque de almacenamiento del motor del contenedor	1	300 GB (100 GB/nodo)
Nodo de almacenamiento	`/var/local` volumen	1	90 GB
Nodo de almacenamiento	Datos de objetos	3	12 TB (4 TB/LUN)
Nodo de administración	`/var/local` volumen	1	90 GB
Nodo de administración	Registros de auditoría del nodo de administrador	1	200 GB
Nodo de administración	Tablas Admin Node	1	200 GB
Nodo de puerta de enlace	`/var/local` volumen	1	90 GB

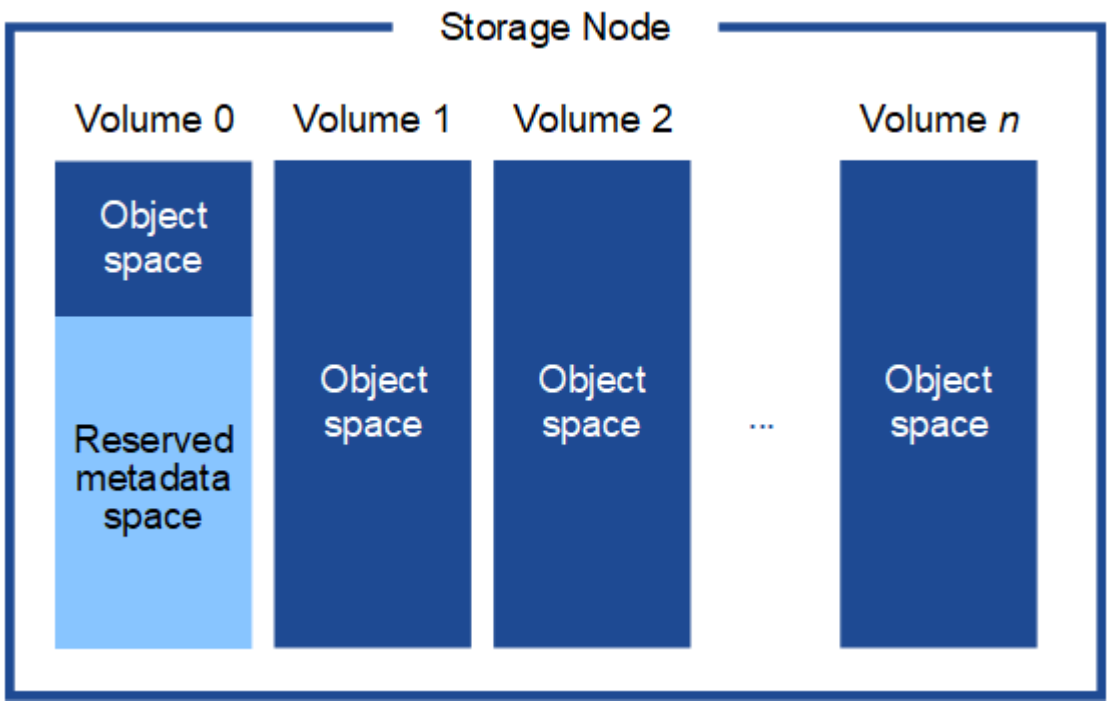
Tipo de nodo	Propósito de LUN	Número de LUN	Tamaño de LUN
Total		**9**	• Piscina de contenedores:* 300 GB **Datos del sistema:** 670 GB **Datos del objeto:** 12,000 GB

Requisitos de almacenamiento para nodos de almacenamiento

Un nodo de almacenamiento basado en software puede tener de 1 a 16 volúmenes de almacenamiento: Se recomiendan -3 o más volúmenes de almacenamiento. Cada volumen de almacenamiento debe ser 4 TB o mayor.

> Un nodo de almacenamiento de dispositivo puede tener hasta 48 volúmenes de almacenamiento.

Como se muestra en la figura, StorageGRID reserva espacio para los metadatos del objeto en el volumen de almacenamiento 0 de cada nodo de almacenamiento. Cualquier espacio restante en el volumen de almacenamiento 0 y cualquier otro volumen de almacenamiento en el nodo de almacenamiento se utilizan exclusivamente para los datos de objetos.



Para proporcionar redundancia y proteger los metadatos de objetos de la pérdida, StorageGRID almacena tres copias de los metadatos para todos los objetos del sistema en cada sitio. Las tres copias de metadatos de objetos se distribuyen uniformemente por todos los nodos de almacenamiento de cada sitio.

Cuando se instala un grid con nodos de almacenamiento solo de metadatos, el grid también debe contener un número mínimo de nodos para el almacenamiento de objetos. Consulte "Tipos de nodos de almacenamiento"

Para obtener más información sobre nodos de almacenamiento solo de metadatos.

- Para un grid de sitio único, hay al menos dos nodos de almacenamiento configurados para objetos y metadatos.
- Para un grid de varios sitios, al menos un nodo de almacenamiento por sitio está configurado para objetos y metadatos.

Cuando se asigna espacio al volumen 0 de un nuevo nodo de almacenamiento, se debe garantizar que haya espacio suficiente para la porción de ese nodo de todos los metadatos de objetos.

- Como mínimo, debe asignar al menos 4 TB al volumen 0.

> Si solo se utiliza un volumen de almacenamiento para un nodo de almacenamiento y se asignan 4 TB o menos al volumen, es posible que el nodo de almacenamiento introduzca el estado de solo lectura de almacenamiento al inicio y almacene solo metadatos de objetos.

> Si se asigna menos de 500 GB al volumen 0 (solo para uso no en producción), el 10 % de la capacidad del volumen de almacenamiento se reserva para metadatos.

- Si va a instalar un nuevo sistema (StorageGRID 11,6 o superior) y cada nodo de almacenamiento tiene 128 GB o más de RAM, asigne 8 TB o más al volumen 0. Al usar un valor mayor para el volumen 0, se puede aumentar el espacio permitido para los metadatos en cada nodo de almacenamiento.
- Al configurar nodos de almacenamiento diferentes para un sitio, utilice el mismo ajuste para el volumen 0 si es posible. Si un sitio contiene nodos de almacenamiento de distintos tamaños, el nodo de almacenamiento con el volumen más pequeño 0 determinará la capacidad de metadatos de ese sitio.

Para obtener más información, vaya a. "Gestione el almacenamiento de metadatos de objetos".

Requisitos de migración de contenedores de nodos

La función de migración de nodos permite mover manualmente un nodo de un host a otro. Normalmente, ambos hosts están en el mismo centro de datos físico.

La migración de nodos le permite realizar el mantenimiento de un host físico sin interrumpir las operaciones de grid. Se mueven todos los nodos de StorageGRID, uno por vez, a otro host antes de desconectar el host físico. La migración de nodos requiere solamente un corto tiempo de inactividad para cada nodo y no debe afectar al funcionamiento o a la disponibilidad de los servicios de grid.

Si desea utilizar la función de migración de nodos StorageGRID, la implementación debe satisfacer requisitos adicionales:

- Nombres de interfaces de red consistentes entre los hosts de un único centro de datos físico
- Almacenamiento compartido para metadatos de StorageGRID y volúmenes de repositorios de objetos al que todos los hosts pueden acceder en un único centro de datos físico. Por ejemplo, puede usar cabinas de almacenamiento E-Series de NetApp.

Si utiliza hosts virtuales y la capa de hipervisor subyacente admite la migración de máquinas virtuales, es posible que desee utilizar esta función en lugar de la función de migración de nodos de StorageGRID. En este caso, puede ignorar estos requisitos adicionales.

Antes de realizar una migración o mantenimiento del hipervisor, apague los nodos correctamente. Consulte las instrucciones para "apagar un nodo de grid".

No se admite la migración en vivo de VMware

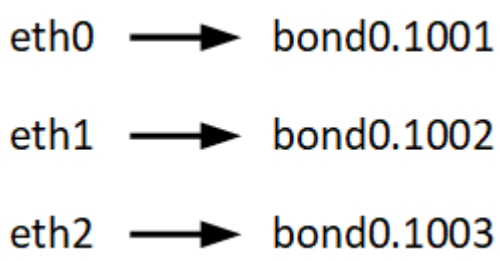
Al realizar una instalación completa en máquinas virtuales de VMware, OpenStack Live Migration y VMware LIVE vMotion provocan que la hora del reloj de la máquina virtual cambie y que los nodos de grid de ningún tipo no sean compatibles. Aunque es poco frecuente, las horas de reloj incorrectas pueden provocar la pérdida de datos o actualizaciones de configuración.

Es compatible con la migración de datos fríos. En la migración en frío, debe apagar los nodos de StorageGRID antes de migrarlos entre hosts. Consulte las instrucciones para "apagar un nodo de grid".

Nombres de interfaces de red consistentes

Para mover un nodo de un host a otro, el servicio de host StorageGRID debe tener cierta confianza en que la conectividad de red externa que tiene el nodo en su ubicación actual puede duplicarse en la nueva ubicación. Obtiene esta confianza mediante el uso de nombres de interfaz de red consistentes en los hosts.

Suponga, por ejemplo, que StorageGRID NodeA que se ejecuta en Host1 se ha configurado con las siguientes asignaciones de interfaz:



El lado izquierdo de las flechas corresponde a las interfaces tradicionales vistas desde un contenedor StorageGRID (es decir, las interfaces Grid, Admin y Client Network, respectivamente). El lado derecho de las flechas corresponde a las interfaces de host reales que proporcionan estas redes, que son tres interfaces VLAN subordinadas al mismo vínculo de interfaz física.

Ahora, supongamos que desea migrar NodeA a Host2. Si Host2 también tiene interfaces denominadas bond0.1001, bond0.1002, y bond0.1003, el sistema permitirá el movimiento, suponiendo que las interfaces con nombre similar proporcionarán la misma conectividad en Host2 que en Host1. Si Host2 no tiene interfaces con los mismos nombres, no se permitirá la transferencia.

Existen muchas formas de lograr una nomenclatura de interfaz de red coherente en varios hosts; consulte "Configurar la red host" para algunos ejemplos.

Almacenamiento compartido

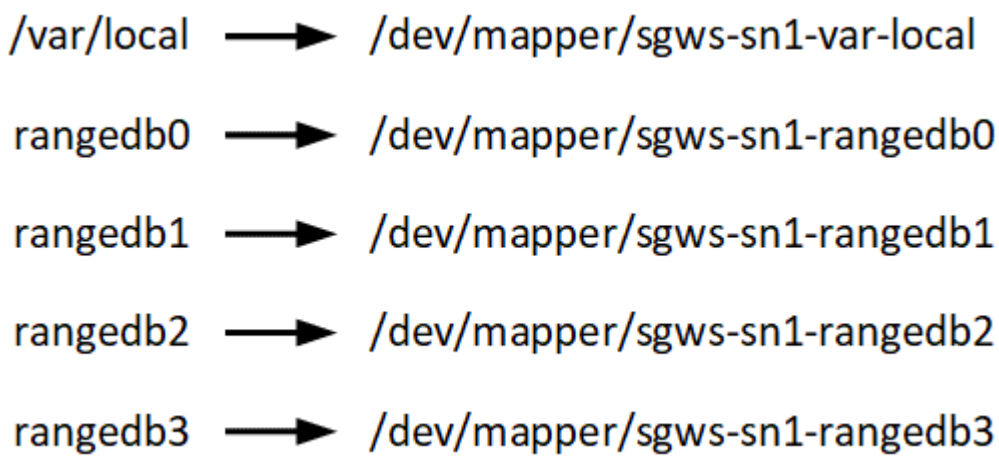
Para lograr migraciones de nodos rápidas y de baja sobrecarga, la función de migración de nodos de StorageGRID no mueve físicamente datos del nodo. En su lugar, la migración de nodos se realiza como par de operaciones de exportación e importación, de la siguiente manera:

1. Durante la operación de «exportación de nodo», se extrae una pequeña cantidad de datos de estado persistente del contenedor de nodos que se ejecuta en el HostA y se almacena en caché en el volumen de datos del sistema de ese nodo. A continuación, se instancia el contenedor de nodos en Hosta.
2. Durante la operación de importación de nodos, se instancian el contenedor de nodos en el host B que utiliza la misma interfaz de red y las asignaciones de almacenamiento en bloque que estaban vigentes en el host. A continuación, los datos de estado persistente en caché se insertan en la nueva instancia.

Dado este modo de funcionamiento, es necesario acceder a todos los volúmenes de almacenamiento de

objetos y datos del sistema del nodo desde Hosta y HostB para permitir la migración y funcionar. Además, deben haberse asignado al nodo utilizando nombres que se garanticen que hacen referencia a las mismas LUN en Hosta y HostB.

En el siguiente ejemplo se muestra una solución para la asignación de dispositivos de bloque para un nodo de almacenamiento de StorageGRID, donde se está utilizando el acceso múltiple de DM en los hosts y se ha utilizado el campo de alias en `/etc/multipath.conf` para proporcionar nombres de dispositivos de bloque coherentes y fáciles de usar disponibles en todos los hosts.



Preparar los hosts (Red Hat)

Cómo cambia la configuración de todo el host durante la instalación

En sistemas con configuración básica, StorageGRID realiza algunos cambios en todo el host `sysctl` configuración.

Se realizan los siguientes cambios:

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288
```

```
# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536
```

```
# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Instale Linux

Debe instalar StorageGRID en todos los hosts Grid de Red Hat Enterprise Linux. Para ver una lista de las versiones admitidas, use la herramienta de matriz de interoperabilidad de NetApp.

Asegúrese de que su sistema operativo esté actualizado al kernel 4,15 de Linux o superior.

Pasos

1. Instalar Linux en todos los hosts de grid físicos o virtuales de acuerdo con las instrucciones del mayorista o del procedimiento estándar.

   Si utiliza el instalador estándar de Linux, NetApp recomienda seleccionar la configuración de software para un nodo de computación, si está disponible o un entorno de base «mínima instalación». No instale ningún entorno de escritorio gráfico.

2. Asegúrese de que todos los hosts tengan acceso a repositorios de paquetes, incluido el canal Extras.

   Es posible que necesite estos paquetes adicionales más adelante en este procedimiento de instalación.

3. Si el intercambio está activado:

   a. Ejecute el siguiente comando: `$ sudo swapoff --all`

   b. Eliminar todas las entradas de intercambio de `/etc/fstab` para mantener los ajustes.

   Si no se deshabilita por completo el intercambio, el rendimiento se puede reducir considerablemente.

Configurar la red host (Red Hat Enterprise Linux)

Una vez finalizada la instalación de Linux en los hosts, puede que deba realizar alguna configuración adicional para preparar un conjunto de interfaces de red en cada host adecuado para la asignación a los nodos StorageGRID que se pondrá en marcha más adelante.

Antes de empezar

- Ha revisado el "Directrices para redes de StorageGRID".

- Ha revisado la información sobre "requisitos de migración de contenedores de nodos".
- Si utiliza hosts virtuales, ha leído el Consideraciones y recomendaciones para la clonación de direcciones MAC antes de configurar la red del host.

> Si utiliza equipos virtuales como hosts, debe seleccionar VMXNET 3 como adaptador de red virtual. El adaptador de red VMware E1000 ha provocado problemas de conectividad con contenedores StorageGRID puestos en marcha en ciertas distribuciones de Linux.

Acerca de esta tarea

Los nodos de grid deben poder acceder a la red de grid y, opcionalmente, a las redes de administrador y cliente. Para proporcionar este acceso, debe crear asignaciones que asocien la interfaz física del host con las interfaces virtuales para cada nodo de grid. Cuando se crean interfaces de host, se utilizan nombres descriptivos para facilitar la puesta en marcha en todos los hosts y para habilitar la migración.

La misma interfaz se puede compartir entre el host y uno o varios nodos. Por ejemplo, podría usar la misma interfaz para el acceso al host y el acceso a la red de administrador de nodo para facilitar el mantenimiento del host y del nodo. Aunque el host y los nodos individuales pueden compartir la misma interfaz, todos deben tener direcciones IP diferentes. Las direcciones IP no se pueden compartir entre nodos ni entre el host y cualquier nodo.

Puede utilizar la misma interfaz de red de host para proporcionar la interfaz de red de cuadrícula para todos los nodos StorageGRID del host; puede utilizar una interfaz de red de host diferente para cada nodo; o puede hacer algo entre ambos. Sin embargo, normalmente no debería proporcionar la misma interfaz de red host que las interfaces de red de Grid y Admin para un solo nodo, o bien como la interfaz de red de cuadrícula para un nodo y la interfaz de red de cliente para otro.

Puede completar esta tarea de muchas maneras. Por ejemplo, si los hosts son máquinas virtuales y va a implementar uno o dos nodos de StorageGRID para cada host, puede crear el número correcto de interfaces de red en el hipervisor y usar una asignación de 1 a 1. Si va a poner en marcha varios nodos en hosts con configuración básica para su uso en producción, puede aprovechar el soporte de la pila de red de Linux para VLAN y LACP para la tolerancia a fallos y el uso compartido de ancho de banda. En las siguientes secciones, se ofrecen enfoques detallados de estos dos ejemplos. No es necesario utilizar ninguno de estos ejemplos; puede utilizar cualquier enfoque que satisfaga sus necesidades.

> No utilice dispositivos de enlace o puente directamente como interfaz de red de contenedor. De esta manera, se podría evitar el inicio del nodo causado por un problema de kernel con el uso de MACVLAN con dispositivos de enlace y puente en el espacio de nombres del contenedor. En su lugar, utilice un dispositivo que no sea de vínculo, como un par VLAN o Ethernet virtual (veth). Especifique este dispositivo como la interfaz de red en el archivo de configuración del nodo.

Información relacionada

"Creando archivos de configuración del nodo"

Consideraciones y recomendaciones para la clonación de direcciones MAC

La clonación de direcciones MAC hace que el contenedor utilice la dirección MAC del host y el host utilice la dirección MAC de una dirección que especifique o una generada aleatoriamente. Debe utilizar la clonación de direcciones MAC para evitar el uso de configuraciones de red en modo promiscuo.

Activación de la clonado de MAC

En algunos entornos, la seguridad se puede mejorar mediante el clonado de direcciones MAC porque permite utilizar un NIC virtual dedicado para la red de administración, la red de cuadrícula y la red de cliente. Si el contenedor utiliza la dirección MAC de la NIC dedicada en el host, podrá evitar el uso de configuraciones de red en modo promiscuo.

> La clonación de direcciones MAC está pensada para utilizarse con instalaciones de servidores virtuales y puede que no funcione correctamente con todas las configuraciones de dispositivos físicos.

> Si no se puede iniciar un nodo debido a que una interfaz objetivo de clonado MAC está ocupada, es posible que deba establecer el enlace a "inactivo" antes de iniciar el nodo. Además, es posible que el entorno virtual pueda evitar la clonación de MAC en una interfaz de red mientras el enlace está activo. Si un nodo no puede configurar la dirección MAC e iniciar debido a una interfaz que está ocupada, configurar el enlace a "inactivo" antes de iniciar el nodo puede solucionar el problema.

La clonación de direcciones MAC está deshabilitada de forma predeterminada y debe establecerse mediante claves de configuración de nodos. Debe habilitarla cuando instala StorageGRID.

Hay una clave para cada red:

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

Si se establece la clave en "verdadero", el contenedor utilizará la dirección MAC de la NIC del host. Además, el host utilizará la dirección MAC de la red de contenedores especificada. De forma predeterminada, la dirección del contenedor es una dirección generada aleatoriamente, pero si ha definido una utilizando la `_NETWORK_MAC` la clave de configuración del nodo, en su lugar, se usa esa dirección. El host y el contenedor siempre tendrán direcciones MAC diferentes.

> Al habilitar la clonación MAC en un host virtual sin habilitar también el modo promiscuo en el hipervisor, es posible que la red de host Linux utilice la interfaz del host para dejar de funcionar.

Casos de uso de clonación DE MAC

Existen dos casos de uso a tener en cuenta con la clonación de MAC:

- Clonado DE MAC no activado: Cuando el `_CLONE_MAC` La clave del archivo de configuración del nodo no está establecida o se establece en "false", el host utilizará el NIC MAC host y el contenedor tendrá un MAC generado por StorageGRID, a menos que se especifique un MAC en el `_NETWORK_MAC` clave. Si se establece una dirección en la `_NETWORK_MAC` clave, el contenedor tendrá la dirección especificada en `_NETWORK_MAC` clave. Esta configuración de claves requiere el uso del modo promiscuo.
- Clonado DE MAC activado: Cuando la `_CLONE_MAC` La clave del archivo de configuración del nodo se establece en "true", el contenedor utiliza el NIC MAC del host y el host utiliza un MAC generado por StorageGRID, a menos que se especifique un MAC en el `_NETWORK_MAC` clave. Si se establece una dirección en la `_NETWORK_MAC` key, el host utiliza la dirección especificada en lugar de la generada. En esta configuración de claves, no debe utilizar el modo promiscuo.

Si no desea utilizar la clonación de direcciones MAC y prefiere permitir que todas las interfaces reciban y transmitan datos para direcciones MAC distintas de las asignadas por el hipervisor, Asegúrese de que las propiedades de seguridad en los niveles de conmutador virtual y grupo de puertos estén establecidas en **Aceptar** para el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas. Los valores establecidos en el conmutador virtual pueden ser anulados por los valores en el nivel de grupo de puertos, por lo que asegúrese de que la configuración sea la misma en ambos lugares.

Para habilitar la clonación de MAC, consulte "instrucciones para crear archivos de configuración de nodo".

Ejemplo de clonación EN MAC

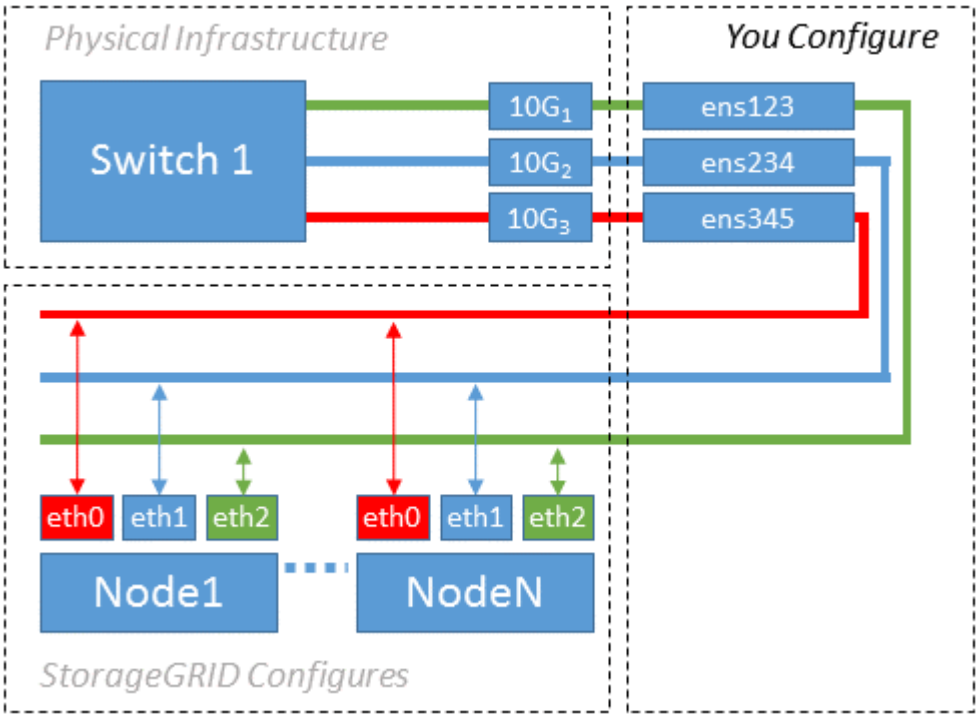
Ejemplo de clonación MAC habilitada con un host que tiene la dirección MAC 11:22:33:44:55:66 para la interfaz ens256 y las siguientes claves en el archivo de configuración del nodo:

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Resultado: El MAC de host para ens256 es b2:9c:02:c2:27:10 y el MAC de red de administración es 11:22:33:44:55:66

Ejemplo 1: Asignación de 1 a 1 a NIC físicas o virtuales

El ejemplo 1 describe una asignación sencilla de interfaz física que requiere poca o ninguna configuración en el lado del host.



El sistema operativo Linux crea el `ensXYZ` interfaces automáticamente durante la instalación o el arranque, o cuando las interfaces se añaden en caliente. No se necesita ninguna configuración que no sea asegurarse de que las interfaces estén configuradas para que se encuentren en funcionamiento automáticamente después

del arranque. Es necesario determinar cuál `ensXYZ` Corresponde a qué red StorageGRID (grid, administrador o cliente) para poder proporcionar las asignaciones correctas más adelante en el proceso de configuración.

Tenga en cuenta que en la figura se muestran varios nodos StorageGRID; sin embargo, normalmente usaría esta configuración para máquinas virtuales de un solo nodo.

Si el conmutador 1 es un conmutador físico, debe configurar los puertos conectados a las interfaces 10G1 a 10G3 para el modo de acceso y colocarlos en las VLAN adecuadas.

Ejemplo 2: Enlace LACP que transporta VLAN

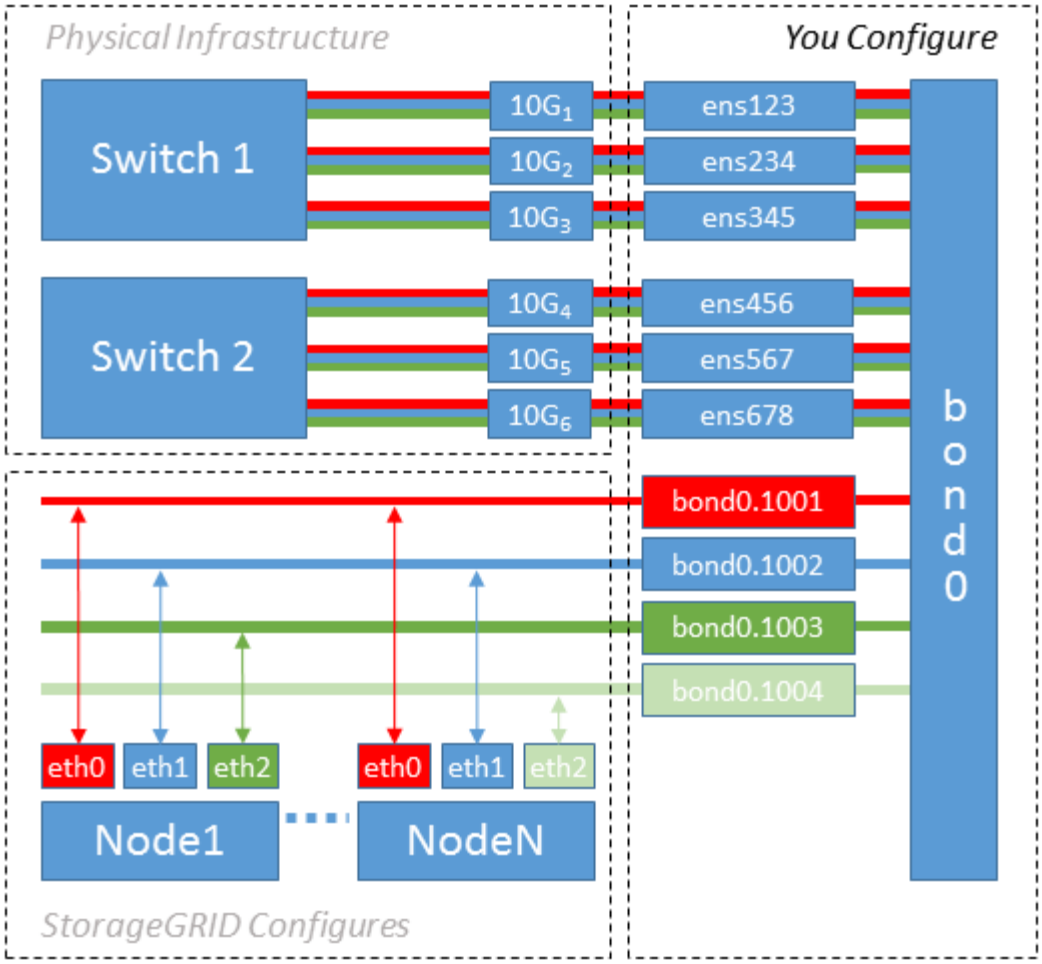
Acerca de esta tarea

En el ejemplo 2 se supone que está familiarizado con las interfaces de red de enlace y con la creación de interfaces VLAN en la distribución Linux que está utilizando.

El ejemplo 2 describe un esquema genérico, flexible y basado en VLAN que facilita el uso compartido de todo el ancho de banda de red disponible en todos los nodos de un único host. Este ejemplo se aplica especialmente a hosts con configuración básica.

Para entender este ejemplo, supongamos que tiene tres subredes distintas para las redes Grid, Admin y Client en cada centro de datos. Las subredes se encuentran en VLAN independientes (1001, 1002 y 1003) y se presentan al host en un puerto de tronco enlazado con LACP (bond0). Usted configuraría tres interfaces VLAN en el enlace: Bond0.1001, bond0.1002, y bond0.1003.

Si requiere VLAN y subredes independientes para redes de nodos en el mismo host, puede agregar interfaces VLAN en el vínculo y asignarlas al host (mostrado como bond0.1004 en la ilustración).



Pasos

1. Agregue todas las interfaces de red físicas que se utilizarán para la conectividad de red de StorageGRID en un único vínculo de LACP.

   Utilice el mismo nombre para el enlace en cada host. Por ejemplo: `bond0`.

2. Cree interfaces VLAN que utilicen este vínculo como su «dispositivo físico» asociado mediante la convención de nomenclatura de la interfaz VLAN estándar `physdev-name.VLAN ID`.

   Tenga en cuenta que los pasos 1 y 2 requieren una configuración adecuada en los conmutadores EDGE que terminan los otros extremos de los enlaces de red. Los puertos del switch perimetral también deben agregarse a un canal de puerto LACP, donde se debe configurar como tronco y donde se puede pasar todas las VLAN requeridas.

   Se proporcionan archivos de configuración de interfaz de muestra para este esquema de configuración de red por host.

Información relacionada

"Ejemplo de /etc/sysconfig/network-scripts"

Configurar el almacenamiento del host

Se deben asignar los volúmenes de almacenamiento en bloque a cada host.

Antes de empezar

Ha revisado los siguientes temas, que le proporcionan información necesaria para realizar esta tarea:

"Los requisitos de almacenamiento y rendimiento"

"Requisitos de migración de contenedores de nodos"

Acerca de esta tarea

Cuando asigne volúmenes de almacenamiento de bloques (LUN) a hosts, utilice las tablas en «Requisitos de almacenamiento» para determinar lo siguiente:

- Número de volúmenes necesarios para cada host (según la cantidad y los tipos de nodos que se pondrán en marcha en ese host)
- Categoría de almacenamiento para cada volumen (es decir, datos del sistema o datos de objetos)
- El tamaño de cada volumen

Utilizará esta información, así como el nombre persistente asignado por Linux a cada volumen físico cuando implemente nodos StorageGRID en el host.

No es necesario crear particiones, formatear o montar ninguno de estos volúmenes; solo debe asegurarse de que sean visibles para los hosts.

Solo se requiere un LUN de datos de objetos para los nodos de almacenamiento solo de metadatos.

Evite utilizar archivos especiales de dispositivos raw (`/dev/sdb`, por ejemplo) al redactar la lista de nombres de volumen. Estos archivos pueden cambiar entre reinicios del host, lo que impacta en el funcionamiento correcto del sistema. Si utiliza LUN iSCSI y rutas múltiples de asignación de dispositivos, considere el uso de alias multivía en la `/dev/mapper` directorio, especialmente si la topología SAN incluye rutas de red redundantes al almacenamiento compartido. De forma alternativa, puede utilizar los enlaces programables creados por el sistema en `/dev/disk/by-path/` para los nombres de dispositivos persistentes.

Por ejemplo:

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Los resultados serán distintos para cada instalación.

Asigne nombres descriptivos a cada uno de estos volúmenes de almacenamiento en bloques para simplificar la instalación inicial de StorageGRID y los procedimientos de mantenimiento futuros. Si se utiliza el controlador multivía del asignador de dispositivos para acceder de forma redundante a volúmenes de almacenamiento compartido, es posible utilizar el `alias` en su `/etc/multipath.conf` archivo.

Por ejemplo:

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

Esto hará que los alias aparezcan como dispositivos de bloque en el `/dev/mapper` directorio en el host, lo que permite especificar un nombre descriptivo y de fácil validación cada vez que una operación de configuración o mantenimiento requiere especificar un volumen de almacenamiento de bloques.

> Si está configurando almacenamiento compartido para admitir la migración de nodos de StorageGRID y el uso de rutas múltiples de asignación de dispositivos, puede crear e instalar un común `/etc/multipath.conf` en todos los hosts ubicados conjuntamente. Solo tiene que asegurarse de usar un volumen de almacenamiento de motor de contenedores diferente en cada host. El uso de alias e incluir el nombre de host de destino en el alias de cada LUN del volumen de almacenamiento del motor de contenedor hará que esto resulte fácil de recordar y se recomienda.

Información relacionada

"Configurar el volumen de almacenamiento del motor del contenedor"

Configurar el volumen de almacenamiento del motor del contenedor

Antes de instalar el motor de contenedor (Docker o Podman), es posible que deba formatear el volumen de almacenamiento y montarlo.

Acerca de esta tarea

Puede omitir estos pasos si tiene pensado utilizar almacenamiento local para el volumen de almacenamiento de Docker o Podman y tener suficiente espacio disponible en la partición de host que contiene `/var/lib/docker` Para Docker y. `/var/lib/containers` Para Podman.

Podman solo es compatible con Red Hat Enterprise Linux (RHEL).

Pasos

1. Cree un sistema de archivos en el volumen de almacenamiento del motor de contenedores:

```
sudo mkfs.ext4 container-engine-storage-volume-device
```

2. Monte el volumen de almacenamiento del motor del contenedor:
   - Para Docker:

```
sudo mkdir -p /var/lib/docker
sudo mount container-storage-volume-device /var/lib/docker
```

   - Para Podman:

```
sudo mkdir -p /var/lib/containers
sudo mount container-storage-volume-device /var/lib/containers
```

3. Añada una entrada para contenedor-almacenamiento-volumen-dispositivo a /etc/fstab.

   Este paso garantiza que el volumen de almacenamiento se vuelva a montar automáticamente después de reiniciar el host.

Instale Docker

El sistema StorageGRID se ejecuta en Red Hat Enterprise Linux como una colección de contenedores. Si ha elegido utilizar el motor de contenedor Docker, siga estos pasos para instalar Docker. En caso contrario, Instalar Podman.

Pasos

1. Siga las instrucciones para su distribución de Linux para instalar Docker.

   Si Docker no se incluye con su distribución de Linux, puede descargarla en el sitio web de Docker.

2. Para asegurarse de que Docker se ha activado y se ha iniciado, ejecute los dos comandos siguientes:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Confirme que ha instalado la versión esperada de Docker; para ello, introduzca lo siguiente:

```
sudo docker version
```

Las versiones cliente y servidor deben ser 1.11.0 o posterior.

Instalar Podman

El sistema StorageGRID se ejecuta en Red Hat Enterprise Linux como una colección de contenedores. Si ha elegido utilizar el motor de contenedor de Podman, siga estos pasos para instalar Podman. En caso contrario, Instale Docker.

Podman solo es compatible con Red Hat Enterprise Linux (RHEL).

Pasos

1. Instale Podman y Podman-Docker siguiendo las instrucciones para su distribución de Linux.

También debe instalar el paquete Podman-Docker cuando instale Podman.

2. Confirme que ha instalado la versión esperada de Podman y Podman-Docker; para ello, introduzca lo siguiente:

```
sudo docker version
```

El paquete Podman-Docker le permite utilizar comandos Docker.

Las versiones de cliente y servidor deben ser 3.2.3 o posteriores.

```
Version: 3.2.3
API Version: 3.2.3
Go Version: go1.15.7
Built: Tue Jul 27 03:29:39 2021
OS/Arch: linux/amd64
```

Instale los servicios de host StorageGRID

Se utiliza el paquete de RPM de StorageGRID para instalar los servicios de host de StorageGRID.

Acerca de esta tarea

Estas instrucciones describen cómo instalar los servicios del host desde los paquetes RPM. Como alternativa, puede utilizar los metadatos del repositorio de Yum incluidos en el archivo de instalación para instalar los paquetes RPM de forma remota. Consulte las instrucciones del repositorio de Yum para el sistema operativo Linux.

Pasos

1. Copie los paquetes de RPM de StorageGRID en cada uno de sus hosts o haga que estén disponibles en el almacenamiento compartido.

   Por ejemplo, colóquelos en el `/tmp` directory, para poder utilizar el comando de ejemplo en el paso siguiente.

2. Inicie sesión en cada host como raíz o utilice una cuenta con permiso sudo y ejecute los siguientes comandos en el orden especificado:

   ```
   sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-version-SHA.rpm
   ```

   ```
   sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-version-SHA.rpm
   ```

   Primero debe instalar el paquete de imágenes y luego el paquete de servicio.

   Si colocó los paquetes en un directorio distinto de `/tmp`, modifique el comando para reflejar la ruta de acceso utilizada.

Automatice la instalación de StorageGRID en Red Hat Enterprise Linux

Puede automatizar la instalación del servicio de host de StorageGRID y la configuración de los nodos de grid.

La automatización de la puesta en marcha puede ser útil en cualquiera de los siguientes casos:

- Ya utiliza un marco de orquestación estándar, como Ansible, Puppet o Chef, para poner en marcha y configurar hosts físicos o virtuales.
- Tiene pensado implementar varias instancias de StorageGRID.
- Está poniendo en marcha una instancia de StorageGRID grande y compleja.

El servicio de host StorageGRID se instala mediante un paquete y está basado en archivos de configuración. Puede crear los archivos de configuración mediante uno de estos métodos:

- "Cree los archivos de configuración" interactivamente durante una instalación manual.
- Prepare los archivos de configuración por adelantado (o mediante programación) para permitir la instalación automatizada mediante marcos de orquestación estándar, como se describe en este artículo.

  StorageGRID proporciona scripts Python opcionales para automatizar la configuración de dispositivos

StorageGRID y todo el sistema StorageGRID (el «grid»). Puede utilizar estos scripts directamente, o puede inspeccionarlos para aprender a utilizar el "Instalación de StorageGRID API DE REST" en las herramientas de instalación y configuración de grid que se desarrolla a sí mismo.

Automatizar la instalación y configuración del servicio de host de StorageGRID

Puede automatizar la instalación del servicio de host de StorageGRID mediante marcos de orquestación estándar como Ansible, Puppet, Chef, Fabric o SaltStack.

El servicio de host de StorageGRID está empaquetado en un RPM y está basado en archivos de configuración que puede prepararse con anticipación (o mediante programación) para permitir la instalación automatizada. Si ya utiliza un marco de orquestación estándar para instalar y configurar RHEL, añadir StorageGRID a sus libros de estrategia o recetas debería ser sencillo.

Consulte el ejemplo de rol y libro de estrategia de Ansible en la `/extras` carpeta suministrada con el archivo de instalación. El libro de estrategia de Ansible muestra cómo `storagegrid` El rol prepara el host e instala StorageGRID en los servidores de destino. Puede personalizar el rol o el libro de estrategia según sea necesario.

> el libro de aplicaciones de ejemplo no incluye los pasos necesarios para crear dispositivos de red antes de iniciar el servicio de host StorageGRID. Añada estos pasos antes de finalizar y utilizar el libro de estrategia.

Es posible automatizar todos los pasos para preparar los hosts y implementar nodos de grid virtual.

Ejemplo de rol y libro de estrategia de Ansible

El rol y el libro de estrategia de Ansible de ejemplo se proporcionan con el archivo de instalación en `/extras` carpeta. El libro de estrategia de Ansible muestra cómo `storagegrid` El rol prepara los hosts e instala StorageGRID en los servidores de destino. Puede personalizar el rol o el libro de estrategia según sea necesario.

Automatice la configuración de StorageGRID

Después de implementar los nodos de grid, puede automatizar la configuración del sistema StorageGRID.

Antes de empezar

- Conoce la ubicación de los siguientes archivos del archivo de instalación.

Nombre de archivo	Descripción
configure-storagegrid.py	Script Python utilizado para automatizar la configuración
configure-storagegrid.sample.json	Archivo de configuración de ejemplo para utilizar con el script
configure-storagegrid.blank.json	Archivo de configuración en blanco para utilizar con el script

- Ha creado un `configure-storagegrid.json` archivo de configuración. Para crear este archivo, puede modificar el archivo de configuración de ejemplo (`configure-storagegrid.sample.json`) o el

archivo de configuración en blanco (`configure-storagegrid.blank.json`).

Acerca de esta tarea

Puede utilizar el `configure-storagegrid.py` El guión de Python y el `configure-storagegrid.json` Archivo de configuración para automatizar la configuración del sistema StorageGRID.

> También puede configurar el sistema mediante Grid Manager o la API de instalación.

Pasos

1. Inicie sesión en el equipo Linux que está utilizando para ejecutar el script Python.
2. Cambie al directorio en el que ha extraído el archivo de instalación.

   Por ejemplo:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   donde `platform` es `debs`, `rpms`, o. `vsphere`.

3. Ejecute el script Python y utilice el archivo de configuración que ha creado.

   Por ejemplo:

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

Resultado

Un paquete de recuperación `.zip` el archivo se genera durante el proceso de configuración y se descarga en el directorio en el que se ejecuta el proceso de instalación y configuración. Debe realizar una copia de seguridad del archivo de paquete de recuperación para poder recuperar el sistema StorageGRID si falla uno o más nodos de grid. Por ejemplo, cópielo en una ubicación de red segura y en una ubicación de almacenamiento en nube segura.

> El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

Si especificó que se generarán contraseñas aleatorias, abra el `Passwords.txt` File y busque las contraseñas que se necesitan para acceder al sistema StorageGRID.

```
#######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip           #####
#####   Safeguard this file as it will be needed in case of a     #####
#####                 StorageGRID node recovery.                  #####
#######################################################################
```

El sistema StorageGRID se instala y configura cuando se muestra un mensaje de confirmación.

```
StorageGRID has been configured and installed.
```

Información relacionada

"Información general de la instalación de la API de REST"

Ponga en marcha nodos de grid virtual (Red Hat)

Cree archivos de configuración de nodos para implementaciones de Red Hat Enterprise Linux

Los archivos de configuración de los nodos son archivos de texto pequeños que proporcionan la información que el servicio de host StorageGRID necesita para iniciar un nodo y conectarlo a la red adecuada y bloquear recursos de almacenamiento. Los archivos de configuración de nodos se usan para los nodos virtuales y no se usan para los nodos del dispositivo.

Ubicación de los archivos de configuración del nodo

Coloque el archivo de configuración de cada nodo StorageGRID en el `/etc/storagegrid/nodes` directorio en el host donde se ejecutará el nodo. Por ejemplo, si planea ejecutar un nodo de administración, un nodo de puerta de enlace y un nodo de almacenamiento en Hosta, debe colocar tres archivos de configuración de nodo en `/etc/storagegrid/nodes` En Hosta.

Puede crear los archivos de configuración directamente en cada host mediante un editor de texto, como vim o nano, o bien puede crearlos en otro lugar y moverlos a cada host.

Nomenclatura de los archivos de configuración de nodos

Los nombres de los archivos de configuración son significativos. El formato es `node-name.conf`, donde `node-name` es un nombre que asigna al nodo. Este nombre aparece en el instalador de StorageGRID y se utiliza para operaciones de mantenimiento de nodos, como la migración de nodos.

Los nombres de los nodos deben seguir estas reglas:

- Debe ser único
- Debe comenzar por una letra
- Puede contener los caracteres De La A a la Z y de la a a la Z.
- Puede contener los números del 0 al 9
- Puede contener uno o varios guiones (-)
- No debe tener más de 32 caracteres, sin incluir el `.conf` extensión

Todos los archivos incluidos `/etc/storagegrid/nodes` que no sigan estas convenciones de nomenclatura no serán analizadas por el servicio de host.

Si tiene una topología de varios sitios planificada para la cuadrícula, un esquema típico de nomenclatura de nodos podría ser:

```
site-nodetype-nodenumber.conf
```

Por ejemplo, podría utilizar `dc1-adm1.conf` Para el primer nodo de administrador en el centro de datos 1, y. `dc2-sn3.conf` Para el tercer nodo de almacenamiento en el centro de datos 2. Sin embargo, puede utilizar cualquier esquema que desee, siempre que todos los nombres de nodo sigan las reglas de nomenclatura.

Contenido de un archivo de configuración de nodo

Un archivo de configuración contiene pares clave/valor, con una clave y un valor por línea. Para cada par clave/valor, siga estas reglas:

- La clave y el valor deben estar separados por un signo igual (=) y espacios en blanco opcionales.
- Las teclas no pueden contener espacios.
- Los valores pueden contener espacios incrustados.
- Se ignora cualquier espacio en blanco inicial o final.

La siguiente tabla define los valores de todas las claves admitidas. Cada clave tiene una de las siguientes designaciones:

- **Requerido**: Requerido para cada nodo o para los tipos de nodo especificados
- **Mejor práctica**: Opcional, aunque recomendado
- **Opcional**: Opcional para todos los nodos

Claves de red de administración

IP_ADMINISTRADOR

Valor	Designación
La dirección IPv4 de red de grid del nodo de administrador principal para la cuadrícula a la que pertenece este nodo. Utilice el mismo valor especificado para GRID_NETWORK_IP para el nodo de grid con NODE_TYPE = VM_Admin_Node y ADMIN_ROLE = Primary. Si omite este parámetro, el nodo intenta detectar un nodo de administración principal con mDNS. "La forma en que los nodos de grid detectan el nodo de administrador principal" **Nota**: Este valor se ignora, y podría estar prohibido, en el nodo de administración principal.	Mejor práctica

ADMIN_NETWORK_CONFIG

Valor	Designación
DHCP, ESTÁTICO O DESHABILITADO	Opcional

ADMIN_NETWORK_ESL

Valor	Designación
Lista separada por comas de subredes en notación CIDR a la que este nodo debe comunicarse mediante la puerta de enlace de la red de administración. Ejemplo: `172.16.0.0/21,172.17.0.0/21`	Opcional

ADMIN_NETWORK_GATEWAY

Valor	Designación

La dirección IPv4 de la puerta de enlace de red de administrador local para este nodo. Debe estar en la subred definida por ADMIN_NETWORK_IP y ADMIN_NETWORK_MASK. Este valor se omite para redes configuradas con DHCP.
 	
Ejemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Obligatorio si `ADMIN_NETWORK_ESL` se especifica. Opcional de lo contrario.

IP_RED_ADMIN

Valor	Designación

La dirección IPv4 de este nodo en la red administrativa. Esta clave solo es necesaria cuando ADMIN_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
 	
Ejemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necesario cuando ADMIN_NETWORK_CONFIG = STATIC.
	
	Opcional de lo contrario.

ADMIN_NETWORK_MAC

Valor	Designación
La dirección MAC de la interfaz de red de administración en el contenedor. Este campo es opcional. Si se omite, se generará automáticamente una dirección MAC. Debe tener 6 pares de dígitos hexadecimales separados por dos puntos. Ejemplo: `b2:9c:02:c2:27:10`	Opcional

ADMIN_NETWORK_MASK

Valor	Designación

La máscara de red IPv4 para este nodo, en la red de administrador. Especifique esta clave cuando ADMIN_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
 	
Ejemplos:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necesario si se especifica ADMIN_NETWORK_IP y ADMIN_NETWORK_CONFIG = STATIC.
	
	Opcional de lo contrario.

MTU_RED_ADMIN

Valor	Designación

La unidad de transmisión máxima (MTU) para este nodo en la red de administración. No especifique si ADMIN_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se utiliza 1500.
 	
Si desea utilizar tramas gigantes, establezca el MTU en un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado.
 	
IMPORTANTE: El valor MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, pueden ocurrir problemas de rendimiento de red o pérdida de paquetes.
 	
Ejemplos:
 	
`1500`
 	
`8192`
	Opcional

ADMIN_NETWORK_TARGET

Valor	Designación

Nombre del dispositivo host que utilizará para el acceso a la red de administración mediante el nodo StorageGRID. Solo se admiten nombres de interfaces de red. Normalmente, se utiliza un nombre de interfaz diferente al especificado para GRID_NETWORK_TARGET o CLIENT_NETWORK_TARGET.
 	
Nota: No utilice dispositivos de enlace o puente como objetivo de red. Configure una VLAN (u otra interfaz virtual) en la parte superior del dispositivo de enlace o utilice un puente y un par Ethernet virtual (veth).
 	
Mejor práctica:especifique un valor aunque este nodo no tenga inicialmente una dirección IP de red de administración. Después, puede añadir una dirección IP de red de administrador más adelante, sin tener que volver a configurar el nodo en el host.
 	
Ejemplos:
 	
`bond0.1002`
 	
`ens256`
	Mejor práctica

ADMIN_NETWORK_TARGET_TYPE

Valor	Designación
Interfaz (este es el único valor admitido.)	Opcional

ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Designación

Verdadero o Falso Establezca la clave en "TRUE" para que el contenedor StorageGRID use la dirección MAC de la interfaz de destino del host en la red de administración. **Mejor práctica:** en redes donde se requiera el modo promiscuo, utilice la clave ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC en su lugar. Para obtener más información sobre la clonación de MAC: • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Red Hat Enterprise Linux)" • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)"	Mejor práctica

ADMIN_ROLE

Valor	Designación
Primario o no primario Esta clave solo es necesaria cuando NODE_TYPE = VM_ADMIN_Node; no la especifique para otros tipos de nodos.	Necesario cuando NODE_TYPE = VM_ADMIN_Node Opcional de lo contrario.

Bloquear las teclas del dispositivo

BLOCK_DEVICE_AUDIT_LOGS

Valor	Designación

La ruta y el nombre del archivo especial del dispositivo de bloque que este nodo utilizará para el almacenamiento persistente de los registros de auditoría.
 	
Ejemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	Necesario para nodos con NODE_TYPE = VM_ADMIN_Node. No lo especifique para otros tipos de nodo.

BLOQUE_DISPOSITIVO_RANGEDB_NNNN

Valor	Designación

Ruta y nombre del archivo especial del dispositivo de bloque que este nodo utilizará para el almacenamiento de objetos persistente. Esta clave solo es necesaria para los nodos con NODE_TYPE = VM_Storage_Node; no la especifique para otros tipos de nodos.
 	
Sólo SE requiere BLOCK_DEVICE_RANGEDB_000; el resto es opcional. El dispositivo de bloque especificado para BLOCK_DEVICE_RANGEDB_000 debe tener al menos 4 TB; los demás pueden ser más pequeños.
 	
No deje espacios vacíos. Si especifica BLOCK_DEVICE_RANGEDB_005, también debe especificar BLOCK_DEVICE_RANGEDB_004.
 	
Nota: Para la compatibilidad con las implementaciones existentes, las claves de dos dígitos son compatibles con los nodos actualizados.
 	
Ejemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	Obligatorio:
	
	BLOQUE_DISPOSITIVO_RANGEDB_000
	
	Opcional:
	
	BLOQUE_DISPOSITIVO_RANGEDB_001
	
	BLOQUE_DISPOSITIVO_RANGEDB_002
	
	BLOQUE_DISPOSITIVO_RANGEDB_003
	
	BLOQUE_DISPOSITIVO_RANGEDB_004
	
	BLOQUE_DISPOSITIVO_RANGEDB_005
	
	BLOQUE_DISPOSITIVO_RANGEDB_006
	
	BLOQUE_DISPOSITIVO_RANGEDB_007
	
	BLOQUE_DISPOSITIVO_RANGEDB_008
	
	BLOQUE_DISPOSITIVO_RANGEDB_009
	
	BLOQUE_DISPOSITIVO_RANGEDB_010
	
	BLOQUE_DISPOSITIVO_RANGEDB_011
	
	BLOQUE_DISPOSITIVO_RANGEDB_012
	
	BLOQUE_DISPOSITIVO_RANGEDB_013
	
	BLOQUE_DISPOSITIVO_RANGEDB_014
	
	BLOQUE_DISPOSITIVO_RANGEDB_015

BLOCK_DEVICE_TABLES

Valor	Designación

Ruta y nombre del archivo especial del dispositivo de bloque que este nodo utilizará para el almacenamiento persistente de tablas de bases de datos. Esta clave solo es necesaria para los nodos con NODE_TYPE = VM_ADMIN_Node; no la especifique para otros tipos de nodos.
 	
Ejemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	Obligatorio

BLOCK_DEVICE_VAR_LOCAL

Valor	Designación

Ruta de acceso y nombre del archivo especial del dispositivo de bloque que este nodo utilizará para su `/var/local` almacenamiento persistente.
 	
Ejemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	Obligatorio

Claves de red cliente

CLIENT_NETWORK_CONFIG

Valor	Designación
DHCP, ESTÁTICO O DESHABILITADO	Opcional

PUERTA_DE_ENLACE_RED_CLIENTE

Valor	Designación

Dirección IPv4 de la puerta de enlace de red de cliente local para este nodo, que debe estar en la subred definida por CLIENT_NETWORK_IP y CLIENT_NETWORK_MASK. Este valor se omite para redes configuradas con DHCP.
 	
Ejemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Opcional

IP_RED_CLIENTE

Valor	Designación

La dirección IPv4 de este nodo en la red cliente.
 	
Esta clave solo es necesaria cuando CLIENT_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
 	
Ejemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necesario cuando CLIENT_NETWORK_CONFIG = ESTÁTICO
	
	Opcional de lo contrario.

MAC_RED_CLIENTE

Valor	Designación
La dirección MAC de la interfaz de red de cliente en el contenedor. Este campo es opcional. Si se omite, se generará automáticamente una dirección MAC. Debe tener 6 pares de dígitos hexadecimales separados por dos puntos. Ejemplo: `b2:9c:02:c2:27:20`	Opcional

MÁSCARA_RED_CLIENTE

Valor	Designación

La máscara de red IPv4 para este nodo en la red de cliente.
 	
Especifique esta clave cuando CLIENT_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
 	
Ejemplos:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necesario si se especifica CLIENT_NETWORK_ip y CLIENT_NETWORK_CONFIG = ESTÁTICO
	
	Opcional de lo contrario.

MTU_RED_CLIENTE

Valor	Designación

La unidad de transmisión máxima (MTU) para este nodo en la red cliente. No especifique si CLIENT_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se utiliza 1500.
 	
Si desea utilizar tramas gigantes, establezca el MTU en un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado.
 	
IMPORTANTE: El valor MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, pueden ocurrir problemas de rendimiento de red o pérdida de paquetes.
 	
Ejemplos:
 	
`1500`
 	
`8192`
	Opcional

DESTINO_RED_CLIENTE

Valor	Designación

Nombre del dispositivo host que utilizará para el acceso a la red de cliente mediante el nodo StorageGRID. Solo se admiten nombres de interfaces de red. Normalmente, se utiliza un nombre de interfaz diferente al especificado para GRID_NETWORK_TARGET o ADMIN_NETWORK_TARGET.
 	
Nota: No utilice dispositivos de enlace o puente como objetivo de red. Configure una VLAN (u otra interfaz virtual) en la parte superior del dispositivo de enlace o utilice un puente y un par Ethernet virtual (veth).
 	
Mejor práctica: especifique un valor aunque este nodo no tenga inicialmente una dirección IP de red de cliente. Después puede añadir una dirección IP de red de cliente más tarde, sin tener que volver a configurar el nodo en el host.
 	
Ejemplos:
 	
`bond0.1003`
 	
`ens423`
	Mejor práctica

CLIENT_NETWORK_TARGET_TYPE

Valor	Designación
Interfaz (solo se admite este valor.)	Opcional

CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Designación
Verdadero o Falso Establezca la clave en "true" para hacer que el contenedor StorageGRID utilice la dirección MAC de la interfaz de destino del host en la red cliente. **Mejor práctica:** en redes donde se requiera el modo promiscuo, utilice la clave CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC en su lugar. Para obtener más información sobre la clonación de MAC: • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Red Hat Enterprise Linux)" • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)"	Mejor práctica

Claves de red de cuadrícula

GRID_NETWORK_CONFIG

Valor	Designación
ESTÁTICO o DHCP El valor por defecto es ESTÁTICO si no se especifica.	Mejor práctica

PUERTA_DE_ENLACE_RED_GRID

Valor	Designación
Dirección IPv4 de la puerta de enlace de red local para este nodo, que debe estar en la subred definida por GRID_NETWORK_IP y GRID_NETWORK_MASK. Este valor se omite para redes configuradas con DHCP. Si la red de red es una subred única sin puerta de enlace, utilice la dirección de puerta de enlace estándar de la subred (X.30 Z.1) o el valor DE GRID_NETWORK_IP de este nodo; cualquiera de los dos valores simplificará las posibles futuras expansiones de red de cuadrícula.	Obligatorio

IP_RED_GRID

Valor	Designación

Dirección IPv4 de este nodo en la red de cuadrícula. Esta clave solo es necesaria cuando GRID_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
 	
Ejemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necesario cuando GRID_NETWORK_CONFIG = ESTÁTICO
	
	Opcional de lo contrario.

MAC_RED_GRID

Valor	Designación

La dirección MAC de la interfaz de red de red del contenedor. Debe tener 6 pares de dígitos hexadecimales separados por dos puntos. Ejemplo: `b2:9c:02:c2:27:30`	Opcional Si se omite, se generará automáticamente una dirección MAC.

GRID_NETWORK_MASK

Valor	Designación

Máscara de red IPv4 para este nodo en la red de cuadrícula. Especifique esta clave cuando GRID_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
 	
Ejemplos:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necesario cuando se especifica GRID_NETWORK_ip y GRID_NETWORK_CONFIG = ESTÁTICO.
	
	Opcional de lo contrario.

MTU_RED_GRID

Valor	Designación

La unidad de transmisión máxima (MTU) para este nodo en la red Grid. No especifique si GRID_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se utiliza 1500.
 	
Si desea utilizar tramas gigantes, establezca el MTU en un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado.
 	
IMPORTANTE: El valor MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, pueden ocurrir problemas de rendimiento de red o pérdida de paquetes.
 	
IMPORTANTE: Para obtener el mejor rendimiento de red, todos los nodos deben configurarse con valores MTU similares en sus interfaces de red Grid. 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.
 	
Ejemplos:
 	
`1500`
 	
`8192`
	Opcional

GRID_NETWORK_TARGET

Valor	Designación

Nombre del dispositivo host que utilizará para el acceso a la red de cuadrícula mediante el nodo StorageGRID. Solo se admiten nombres de interfaces de red. Normalmente, se utiliza un nombre de interfaz diferente al especificado para ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET.
 	
Nota: No utilice dispositivos de enlace o puente como objetivo de red. Configure una VLAN (u otra interfaz virtual) en la parte superior del dispositivo de enlace o utilice un puente y un par Ethernet virtual (veth).
 	
Ejemplos:
 	
`bond0.1001`
 	
`ens192`
	Obligatorio

GRID_NETWORK_TARGET_TYPE

Valor	Designación

Interfaz (este es el único valor admitido.)	Opcional

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Designación
Verdadero o Falso Establezca el valor de la clave en "verdadero" para que el contenedor StorageGRID utilice la dirección MAC de la interfaz de destino del host en la red de red. **Mejor práctica:** en redes donde se requiera el modo promiscuo, utilice la clave GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC en su lugar. Para obtener más información sobre la clonación de MAC: • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Red Hat Enterprise Linux)" • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)"	Mejor práctica

Clave de interfaces

INTERFAZ_DESTINO_nnnn

Valor	Designación
Nombre y descripción opcional para una interfaz adicional que se desea añadir a este nodo. Puede añadir varias interfaces adicionales a cada nodo. Para *nnnn*, especifique un número único para cada entrada de INTERFAZ_DESTINO que agregue. Para el valor, especifique el nombre de la interfaz física en el host de configuración básica. A continuación, de manera opcional, añada una coma y proporcione una descripción de la interfaz, que se muestra en la página interfaces VLAN y en la página grupos de alta disponibilidad. Ejemplo: `INTERFACE_TARGET_0001=ens256, Trunk` Si añade una interfaz troncal, debe configurar una interfaz VLAN en StorageGRID. Si agrega una interfaz de acceso, puede añadir la interfaz directamente a un grupo de alta disponibilidad; no es necesario configurar una interfaz de VLAN.	Opcional

Clave RAM máxima

RAM_MÁXIMA

Valor	Designación

La cantidad máxima de RAM que se permite que este nodo consuma. Si se omite esta clave, el nodo no tiene restricciones de memoria. Al establecer este campo para un nodo de nivel de producción, especifique un valor que sea al menos 24 GB y 16 a 32 GB menor que la RAM total del sistema.
 	
Nota: El valor de la RAM afecta al espacio reservado real de metadatos de un nodo. Consulte "Descripción del espacio reservado de metadatos".
 	
El formato de este campo es *`numberunit`*, donde *`unit`* puede ser `b`, `k`, `m`, o. `g`.
 	
Ejemplos:
 	
`24g`
 	
`38654705664b`
 	
Nota: Si desea utilizar esta opción, debe activar el soporte de núcleo para grupos de memoria.
	Opcional

Clave de tipo de nodo

TIPO_NODO

Valor	Designación
Tipo de nodo: VM_Admin_Node VM_Storage_Node VM_Archive_Node Puerta de enlace_API_VM	Obligatorio

Claves de reasignación de puertos

REASIGNAR_PUERTO

Valor	Designación

Reasigna cualquier puerto que usa un nodo para las comunicaciones internas del nodo de grid o las comunicaciones externas. La reasignación de puertos es necesaria si las políticas de red de la empresa restringen uno o más puertos utilizados por StorageGRID, como se describe en "Comunicaciones internas de los nodos de grid" o. "Comunicaciones externas". **IMPORTANTE**: No reasigne los puertos que planea usar para configurar los puntos finales del equilibrador de carga. **Nota**: Si sólo SE establece PORT_REMAPP, la asignación que especifique se utiliza tanto para comunicaciones entrantes como salientes. Si TAMBIÉN se especifica PORT_REMAPP_INBOUND, PORT_REMAPP sólo se aplica a las comunicaciones salientes. El formato utilizado es: *`network type/protocol/default port used by grid node/new port`*, donde *`network type`* es grid, administrador o cliente, y. *`protocol`* es tcp o udp. Ejemplo: `PORT_REMAP = client/tcp/18082/443`	Opcional

PORT_REMAPP_INBOUND

Valor	Designación
Reasigna las comunicaciones entrantes al puerto especificado. Si especifica PORT_REMAP_INBOUND pero no especifica un valor para PORT_REMAP, las comunicaciones salientes para el puerto no cambian. **IMPORTANTE**: No reasigne los puertos que planea usar para configurar los puntos finales del equilibrador de carga. El formato utilizado es: *`network type/protocol/remapped port /default port used by grid node`*, donde *`network type`* es grid, administrador o cliente, y. *`protocol`* es tcp o udp. Ejemplo: `PORT_REMAP_INBOUND = grid/tcp/3022/22`	Opcional

La forma en que los nodos de grid detectan el nodo de administrador principal

Los nodos de grid se comunican con el nodo de administrador principal para realizar tareas de configuración y gestión. Cada nodo de grid debe conocer la dirección IP del nodo de administrador principal en la red de grid.

Para garantizar que un nodo de grid pueda acceder al nodo de administrador principal, puede realizar cualquiera de las siguientes acciones al implementar el nodo:

- Puede usar el parámetro ADMIN_IP para introducir la dirección IP del nodo administrador primario manualmente.

- Puede omitir el parámetro ADMIN_IP para que el nodo del grid detecte el valor automáticamente. La detección automática es especialmente útil cuando la red de cuadrícula utiliza DHCP para asignar la dirección IP al nodo de administración principal.

La detección automática del nodo de administración principal se realiza mediante un sistema de nombres de dominio de multidifusión (mDNS). Cuando se inicia por primera vez el nodo de administración principal, publica su dirección IP mediante mDNS. A continuación, otros nodos de la misma subred pueden consultar la dirección IP y adquirirla automáticamente. Sin embargo, debido a que el tráfico IP de multidifusión no se puede enrutar en subredes, los nodos de otras subredes no pueden adquirir directamente la dirección IP del nodo de administración principal.

Si utiliza la detección automática:

- Debe incluir la configuración ADMIN_IP para al menos un nodo de grid en las subredes a las que no está conectado directamente el nodo de administración principal. A continuación, este nodo de cuadrícula publicará la dirección IP del nodo de administración principal para otros nodos de la subred a fin de detectar con mDNS.
- Asegúrese de que la infraestructura de red admite la transferencia de tráfico IP multifundido dentro de una subred.

Archivos de configuración del nodo de ejemplo

Puede usar los archivos de configuración del nodo de ejemplo para ayudar a configurar los archivos de configuración del nodo para el sistema StorageGRID. Los ejemplos muestran archivos de configuración de nodo para todos los tipos de nodos de cuadrícula.

En la mayoría de los nodos, puede agregar información de direccionamiento de red de administrador y cliente (IP, máscara, puerta de enlace, etc.) al configurar la cuadrícula mediante Grid Manager o la API de instalación. La excepción es el nodo de administrador principal. Si desea examinar la dirección IP de red de administrador del nodo de administración principal para completar la configuración de grid (porque la red de grid no se enrutó, por ejemplo), debe configurar la conexión de red de administración para el nodo de administración principal en su archivo de configuración de nodo. Esto se muestra en el ejemplo.

En los ejemplos, el destino de red de cliente se ha configurado como práctica recomendada, aunque la red de cliente esté deshabilitada de forma predeterminada.

Ejemplo de nodo de administración primario

Ejemplo de nombre de archivo: `/etc/storagegrid/nodes/dc1-adm1.conf`

Ejemplo del contenido del archivo:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Ejemplo para Storage Node

Ejemplo de nombre de archivo: `/etc/storagegrid/nodes/dc1-sn1.conf`

Ejemplo del contenido del archivo:

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Ejemplo para nodo de archivado

Ejemplo de nombre de archivo: `/etc/storagegrid/nodes/dc1-arc1.conf`

Ejemplo del contenido del archivo:

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Ejemplo para Gateway Node

Ejemplo de nombre de archivo: `/etc/storagegrid/nodes/dc1-gw1.conf`

Ejemplo del contenido del archivo:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Ejemplo de un nodo de administrador que no es primario

Ejemplo de nombre de archivo: `/etc/storagegrid/nodes/dc1-adm2.conf`

Ejemplo del contenido del archivo:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Validar la configuración de StorageGRID

Después de crear archivos de configuración en `/etc/storagegrid/nodes` Debe validar el contenido de cada uno de los nodos StorageGRID.

Para validar el contenido de los archivos de configuración, ejecute el siguiente comando en cada host:

```
sudo storagegrid node validate all
```

Si los archivos son correctos, el resultado muestra **PASADO** para cada archivo de configuración, como se muestra en el ejemplo.

Cuando se usa solo una LUN en los nodos de solo metadatos, puede recibir un mensaje de advertencia que se puede ignorar.

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

Para una instalación automatizada, puede suprimir este resultado utilizando `-q` o. `--quiet` de la `storagegrid` (por ejemplo, `storagegrid --quiet…`). Si suprime el resultado, el comando tendrá un valor de salida que no es cero si se detectan advertencias o errores de configuración.

Si los archivos de configuración son incorrectos, los problemas se muestran como **ADVERTENCIA** y **ERROR**, como se muestra en el ejemplo. Si se encuentra algún error de configuración, debe corregirlo antes de

continuar con la instalación.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Inicie el servicio de host StorageGRID

Para iniciar los nodos de StorageGRID y asegurarse de que reinicien después del reinicio de un host, debe habilitar e iniciar el servicio de host StorageGRID.

Pasos

1. Ejecute los siguientes comandos en cada host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Ejecute el siguiente comando para asegurarse de que se sigue la implementación:

```
sudo storagegrid node status node-name
```

3. Si alguno de los nodos devuelve el estado «Sin ejecución» o «Detenido», ejecute el siguiente comando:

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

4. Si anteriormente habilitó e inició el servicio de host de StorageGRID (o si no está seguro de si el servicio se ha habilitado e iniciado), también debe ejecutar el siguiente comando:

```
sudo systemctl reload-or-restart storagegrid
```

Configurar la cuadrícula y completar la instalación (Red Hat)

Desplácese hasta Grid Manager

El Gestor de cuadrícula se utiliza para definir toda la información necesaria para configurar el sistema StorageGRID.

Antes de empezar

El nodo de administración principal debe estar implementado y haber completado la secuencia de inicio inicial.

Pasos

1. Abra el explorador web y desplácese hasta una de las siguientes direcciones:

   `https://primary_admin_node_ip`

   `client_network_ip`

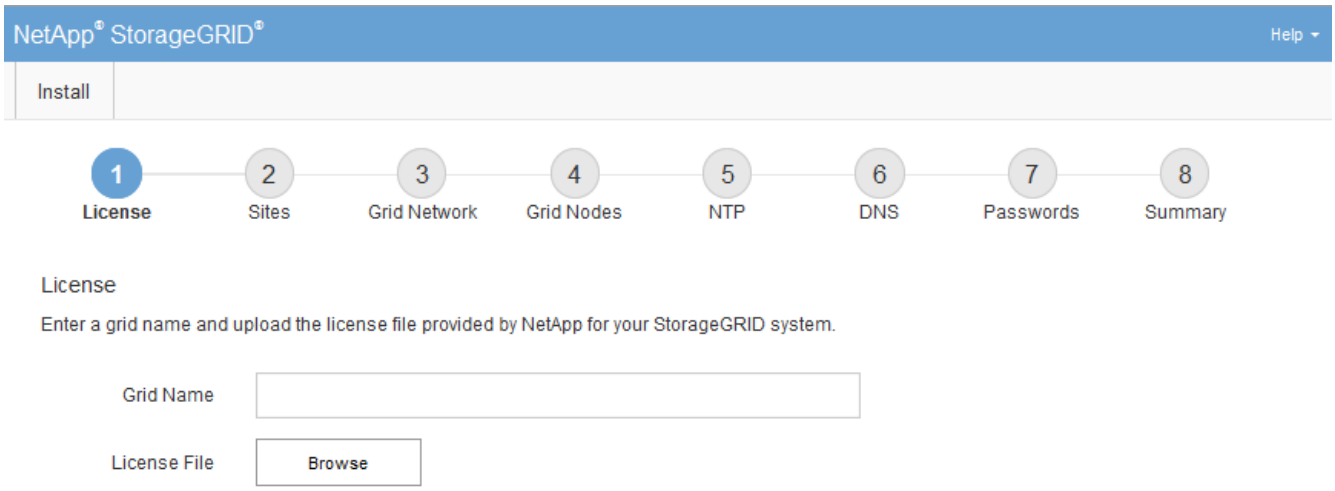
   También puede acceder a Grid Manager en el puerto 8443:

   `https://primary_admin_node_ip:8443`

   > Puede usar la dirección IP para la IP del nodo de administración principal en la red de grid o en la red de administración, según corresponda a su configuración de red.

2. Selecciona **Instalar un sistema StorageGRID**.

   Se muestra la página que se utiliza para configurar un sistema StorageGRID.



Especifique la información de licencia de StorageGRID

Debe especificar el nombre del sistema StorageGRID y cargar el archivo de licencia proporcionado por NetApp.

Pasos

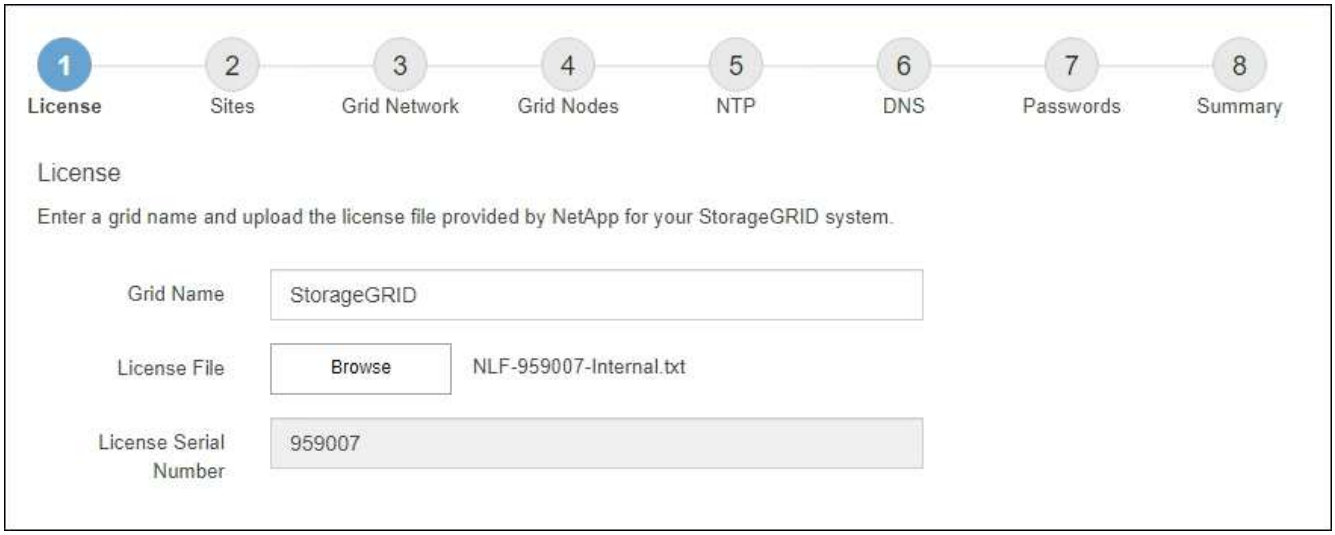
1. En la página Licencia, introduzca un nombre significativo para su sistema StorageGRID en el campo **Nombre de cuadrícula**.

   Tras la instalación, el nombre se muestra en la parte superior del menú nodos.

2. Seleccione **Examinar** y busque el archivo de licencia de NetApp (`NLF-unique-id.txt`) Y seleccione **Abrir**.

   El archivo de licencia se valida y se muestra el número de serie.

   > El archivo de instalación de StorageGRID incluye una licencia gratuita que no proporciona ningún derecho de soporte para el producto. Puede actualizar a una licencia que ofrezca soporte tras la instalación.



3. Seleccione **Siguiente**.

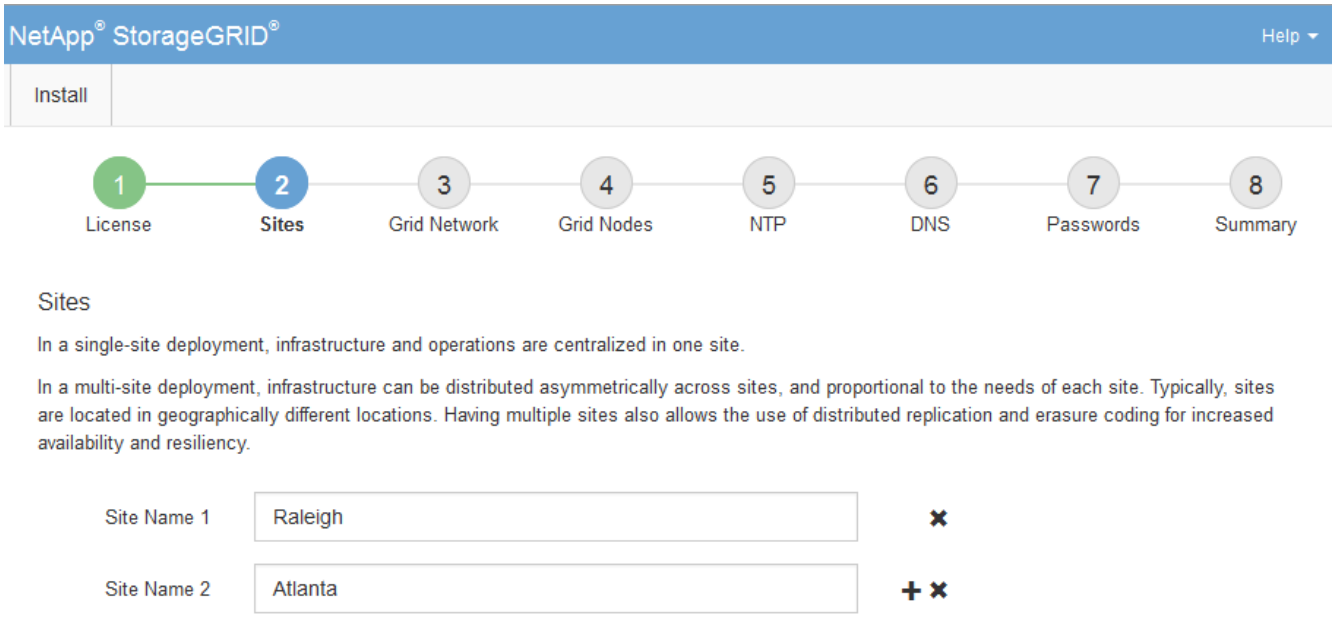
Agregar sitios

Debe crear al menos un sitio cuando instale StorageGRID. Puede crear sitios adicionales para aumentar la fiabilidad y la capacidad de almacenamiento de su sistema StorageGRID.

Pasos

1. En la página Sitios, introduzca el **Nombre del sitio**.
2. Para agregar sitios adicionales, haga clic en el signo más situado junto a la última entrada del sitio e introduzca el nombre en el nuevo cuadro de texto **Nombre del sitio**.

   Agregue tantos sitios adicionales como sea necesario para la topología de la cuadrícula. Puede agregar hasta 16 sitios.



3. Haga clic en **Siguiente**.

Especifique las subredes de red de red

Debe especificar las subredes que se utilizan en la red de cuadrícula.

Acerca de esta tarea

Las entradas de subred incluyen las subredes de la red de grid para cada sitio del sistema de StorageGRID, junto con las subredes a las que sea necesario acceder a través de la red de grid.

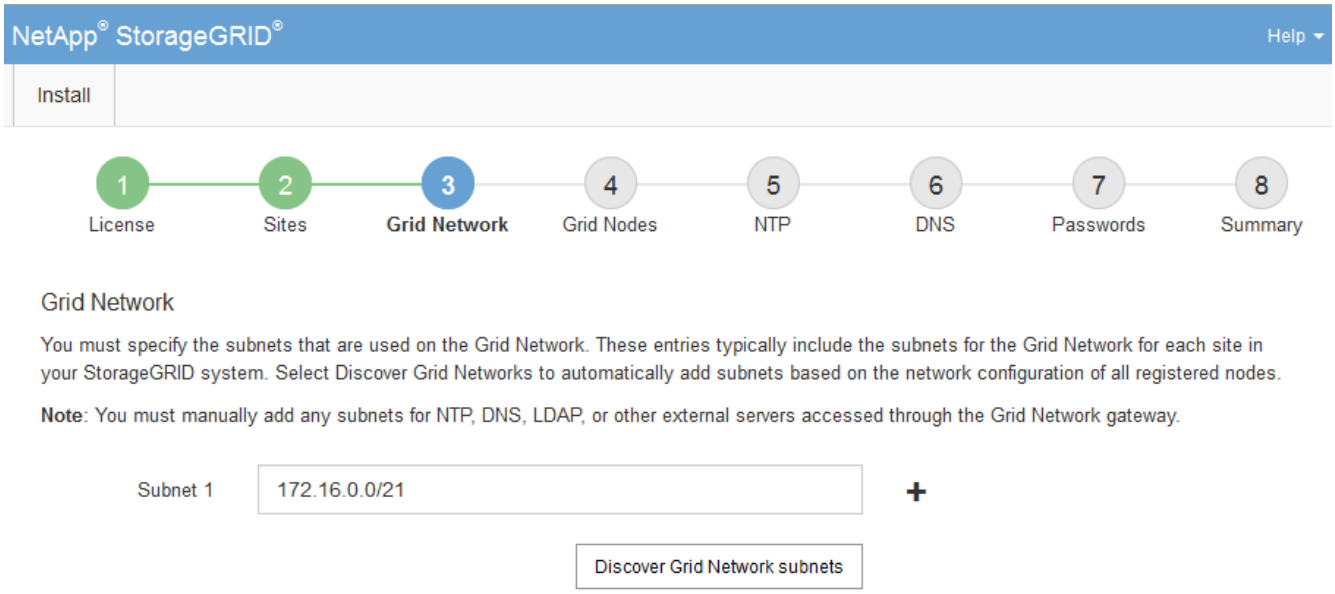
Si tiene varias subredes de cuadrícula, se requiere la puerta de enlace de red de cuadrícula. Todas las subredes de la cuadrícula especificadas deben ser accesibles a través de esta puerta de enlace.

Pasos

1. Especifique la dirección de red CIDR para al menos una red de cuadrícula en el cuadro de texto **Subnet 1**.
2. Haga clic en el signo más situado junto a la última entrada para añadir una entrada de red adicional.

   Si ya ha implementado al menos un nodo, haga clic en **detectar subredes** de redes de cuadrícula para rellenar automáticamente la Lista de subredes de red de cuadrícula con las subredes notificadas por los

nodos de cuadrícula que se han registrado en el Gestor de cuadrícula.



3. Haga clic en **Siguiente**.

Aprobar los nodos de cuadrícula pendientes

Debe aprobar cada nodo de cuadrícula para poder unirse al sistema StorageGRID.

Antes de empezar

Ha puesto en marcha todos los nodos de grid de dispositivos virtuales y StorageGRID.

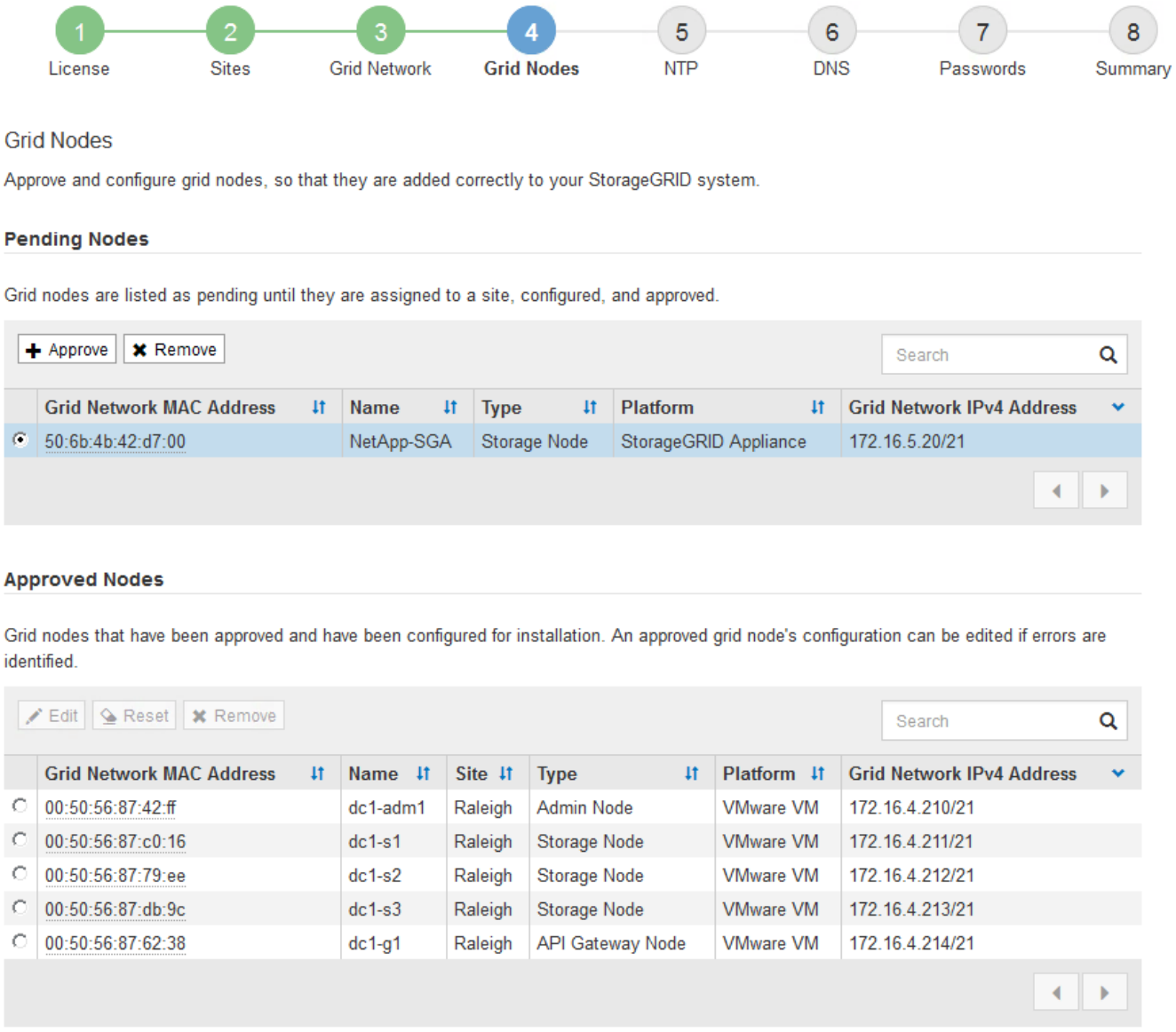
> Es más eficiente realizar una instalación única de todos los nodos, en lugar de instalar algunos ahora y algunos nodos más adelante.

Pasos

1. Revise la lista Pending Nodes y confirme que se muestran todos los nodos de grid que ha implementado.

> Si falta un nodo de cuadrícula, confirme que se ha implementado correctamente.

2. Seleccione el botón de opción situado junto al nodo pendiente que desea aprobar.



3. Haga clic en **aprobar**.
4. En Configuración general, modifique la configuración de las siguientes propiedades según sea necesario:
   - **Sitio**: El nombre del sistema del sitio para este nodo de cuadrícula.
   - **Nombre**: El nombre del sistema para el nodo. El nombre predeterminado es el nombre que especifique cuando configure el nodo.

     Los nombres de sistema son necesarios para las operaciones internas de StorageGRID y no se pueden cambiar después de completar la instalación. Sin embargo, durante este paso del proceso de instalación, puede cambiar los nombres del sistema según sea necesario.

   - **Función NTP**: La función de Protocolo de hora de red (NTP) del nodo de red. Las opciones son **automático**, **primario** y **Cliente**. Al seleccionar **automático**, se asigna la función principal a los nodos de administración, los nodos de almacenamiento con servicios ADC, los nodos de puerta de enlace y cualquier nodo de cuadrícula que tenga direcciones IP no estáticas. Al resto de los nodos de grid se le asigna el rol de cliente.

Asegúrese de que al menos dos nodos de cada sitio puedan acceder a al menos cuatro fuentes de NTP externas. Si solo un nodo de un sitio puede acceder a los orígenes NTP, se producirán problemas de tiempo si ese nodo falla. Además, designar dos nodos por sitio como orígenes NTP primarios garantiza una sincronización precisa si un sitio está aislado del resto de la cuadrícula.

- **Tipo de almacenamiento** (solo nodos de almacenamiento): Especifique que un nuevo nodo de almacenamiento se utilice exclusivamente para metadatos. Las opciones son **Objetos y metadatos** y **Solo metadatos**. Consulte "Tipos de nodos de almacenamiento" Para obtener más información sobre nodos de almacenamiento solo de metadatos.

  Cuando se instala un grid con nodos solo metadatos, este también debe contener un número mínimo de nodos para el almacenamiento de objetos. Para un grid de sitio único, hay al menos dos nodos de almacenamiento configurados para objetos y metadatos. Para un grid de varios sitios, al menos un nodo de almacenamiento por sitio está configurado para objetos y metadatos.

- **Servicio ADC** (sólo nodos de almacenamiento): Seleccione **automático** para que el sistema determine si el nodo requiere el servicio controlador de dominio administrativo (ADC). El servicio ADC realiza un seguimiento de la ubicación y disponibilidad de los servicios de red. Al menos tres nodos de almacenamiento en cada sitio deben incluir el servicio ADC. No puede agregar el servicio ADC a un nodo después de que se haya desplegado.

5. En Red de cuadrícula, modifique la configuración de las siguientes propiedades según sea necesario:

   - **Dirección IPv4 (CIDR)**: La dirección de red CIDR para la interfaz de red Grid (eth0 dentro del contenedor). Por ejemplo: 192.168.1.234/21
   - **Gateway**: El gateway de red de red de red de red de red de red de Por ejemplo: 192.168.0.1

     La puerta de enlace es necesaria si hay varias subredes de la cuadrícula.

   Si seleccionó DHCP para la configuración de red de cuadrícula y cambia el valor aquí, el nuevo valor se configurará como dirección estática en el nodo. Debe asegurarse de que la dirección IP resultante no esté dentro del pool de direcciones de DHCP.

6. Si desea configurar la red administrativa para el nodo de grid, añada o actualice los ajustes en la sección Admin Network, según sea necesario.

   Introduzca las subredes de destino de las rutas fuera de esta interfaz en el cuadro de texto **subredes (CIDR)**. Si hay varias subredes de administración, se requiere la puerta de enlace de administración.

   Si seleccionó DHCP para la configuración de red del administrador y cambia el valor aquí, el nuevo valor se configurará como dirección estática en el nodo. Debe asegurarse de que la dirección IP resultante no esté dentro del pool de direcciones de DHCP.

   Dispositivos: Para un dispositivo StorageGRID, si la red de administración no se configuró durante la instalación inicial mediante el instalador de dispositivos StorageGRID, no se puede configurar en este cuadro de diálogo Administrador de grid. En su lugar, debe seguir estos pasos:

   a. Reinicie el dispositivo: En el instalador del equipo, seleccione **Avanzado** > **Reiniciar**.

      El reinicio puede tardar varios minutos.

b. Seleccione **Configurar redes** > **Configuración de enlaces** y active las redes apropiadas.
c. Seleccione **Configurar redes** > **Configuración IP** y configure las redes habilitadas.
d. Vuelva a la página de inicio y haga clic en **Iniciar instalación**.
e. En Grid Manager: Si el nodo aparece en la tabla Nodos aprobados, elimine el nodo.
f. Quite el nodo de la tabla Pending Nodes.
g. Espere a que el nodo vuelva a aparecer en la lista Pending Nodes.
h. Confirme que puede configurar las redes adecuadas. Ya deben rellenarse con la información proporcionada en la página de configuración de IP del instalador de dispositivos.

   Para obtener información adicional, consulte las instrucciones de instalación de su modelo de dispositivo.

7. Si desea configurar la Red cliente para el nodo de cuadrícula, agregue o actualice los ajustes en la sección Red cliente según sea necesario. Si se configura la red de cliente, se requiere la puerta de enlace y se convierte en la puerta de enlace predeterminada del nodo después de la instalación.

   > Si seleccionó DHCP para la configuración de red de cliente y cambia el valor aquí, el nuevo valor se configurará como dirección estática en el nodo. Debe asegurarse de que la dirección IP resultante no esté dentro del pool de direcciones de DHCP.

   Electrodomésticos: Para un dispositivo StorageGRID, si la red cliente no se configuró durante la instalación inicial mediante el instalador de dispositivos StorageGRID, no se puede configurar en este cuadro de diálogo Administrador de grid. En su lugar, debe seguir estos pasos:

   a. Reinicie el dispositivo: En el instalador del equipo, seleccione **Avanzado** > **Reiniciar**.

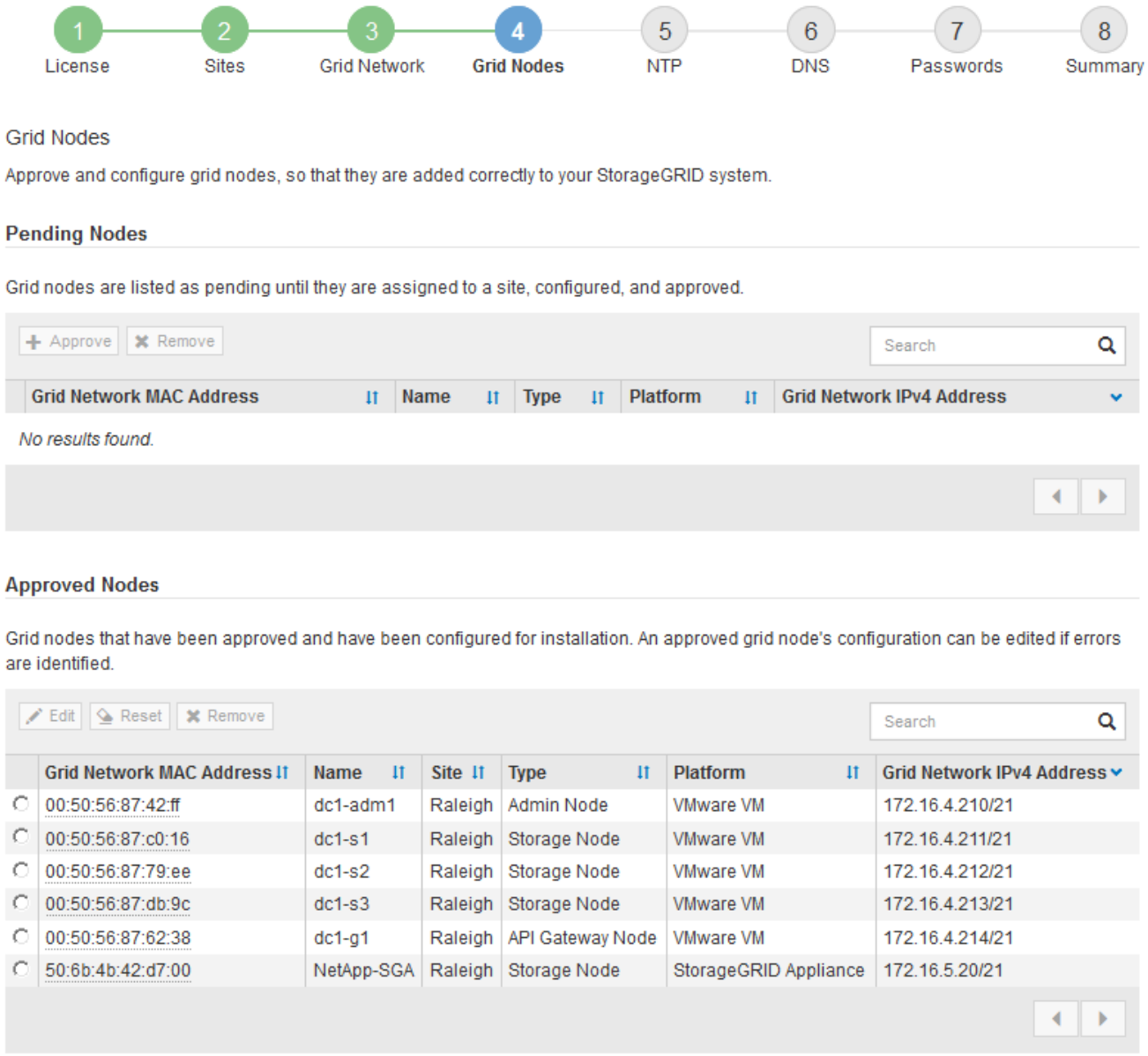
      El reinicio puede tardar varios minutos.

   b. Seleccione **Configurar redes** > **Configuración de enlaces** y active las redes apropiadas.
   c. Seleccione **Configurar redes** > **Configuración IP** y configure las redes habilitadas.
   d. Vuelva a la página de inicio y haga clic en **Iniciar instalación**.
   e. En Grid Manager: Si el nodo aparece en la tabla Nodos aprobados, elimine el nodo.
   f. Quite el nodo de la tabla Pending Nodes.
   g. Espere a que el nodo vuelva a aparecer en la lista Pending Nodes.
   h. Confirme que puede configurar las redes adecuadas. Ya deben rellenarse con la información proporcionada en la página de configuración de IP del instalador de dispositivos.

      Para obtener más información, consulte las instrucciones de instalación del aparato.

8. Haga clic en **Guardar**.

   La entrada del nodo de grid se mueve a la lista de nodos aprobados.



9. Repita estos pasos para cada nodo de cuadrícula pendiente que desee aprobar.

   Debe aprobar todos los nodos que desee de la cuadrícula. Sin embargo, puede volver a esta página en cualquier momento antes de hacer clic en **instalar** en la página Resumen. Puede modificar las propiedades de un nodo de cuadrícula aprobado seleccionando su botón de opción y haciendo clic en **Editar**.

10. Cuando haya terminado de aprobar nodos de cuadrícula, haga clic en **Siguiente**.

Especifique la información del servidor de protocolo de tiempo de redes

Es necesario especificar la información de configuración del protocolo de tiempo de redes (NTP) para el sistema StorageGRID, de manera que se puedan mantener sincronizadas las operaciones realizadas en servidores independientes.

Acerca de esta tarea

Debe especificar las direcciones IPv4 para los servidores NTP.

Debe especificar servidores NTP externos. Los servidores NTP especificados deben usar el protocolo NTP.

Debe especificar cuatro referencias de servidor NTP de estrato 3 o superior para evitar problemas con la desviación del tiempo.

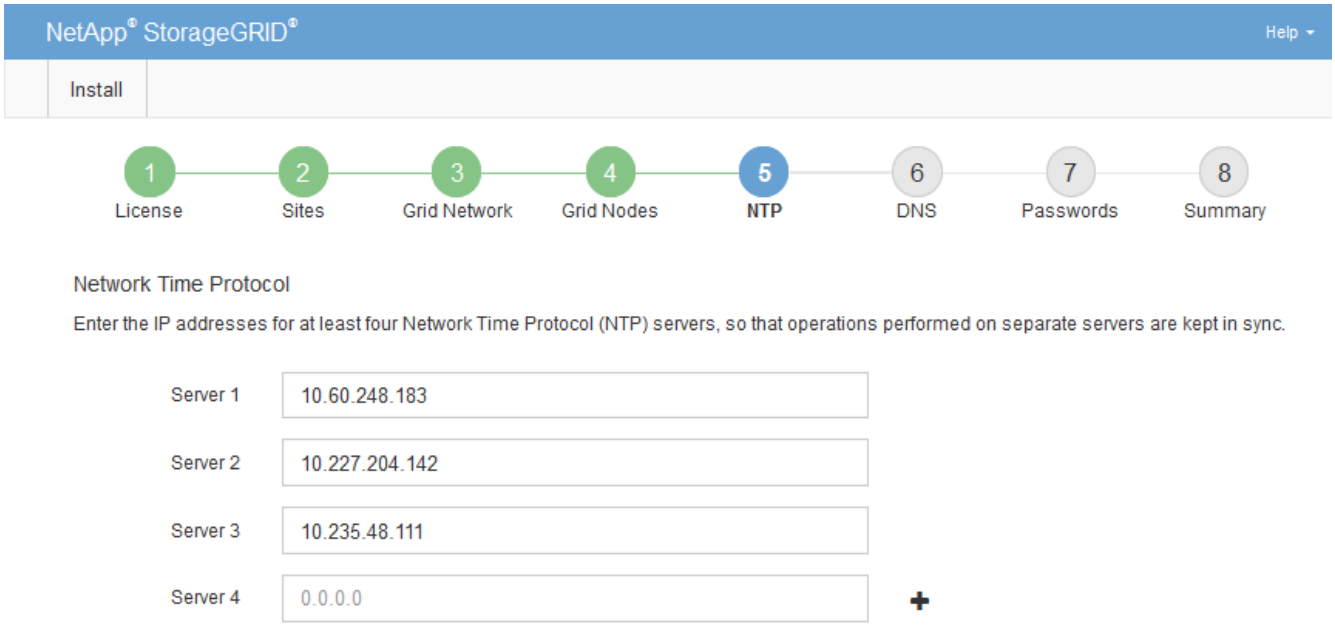
> Al especificar el origen NTP externo para una instalación de StorageGRID en el nivel de producción, no use el servicio Windows Time (W32Time) en una versión de Windows anterior a Windows Server 2016. El servicio de tiempo en versiones anteriores de Windows no es lo suficientemente preciso y no es compatible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

Los nodos a los que asignó previamente roles NTP primarios utilizan los servidores NTP externos.

> Asegúrese de que al menos dos nodos de cada sitio puedan acceder a al menos cuatro fuentes de NTP externas. Si solo un nodo de un sitio puede acceder a los orígenes NTP, se producirán problemas de tiempo si ese nodo falla. Además, designar dos nodos por sitio como orígenes NTP primarios garantiza una sincronización precisa si un sitio está aislado del resto de la cuadrícula.

Pasos

1. Especifique las direcciones IPv4 para al menos cuatro servidores NTP en los cuadros de texto **servidor 1** a **servidor 4** .
2. Si es necesario, seleccione el signo más junto a la última entrada para agregar entradas adicionales del servidor.



3. Seleccione **Siguiente**.

Especifique la información del servidor DNS

Debe especificar la información DNS del sistema StorageGRID, de modo que pueda

acceder a los servidores externos con nombres de host en lugar de direcciones IP.

Acerca de esta tarea

Especificando "Información del servidor DNS" Permite usar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP para notificaciones por correo electrónico y AutoSupport.

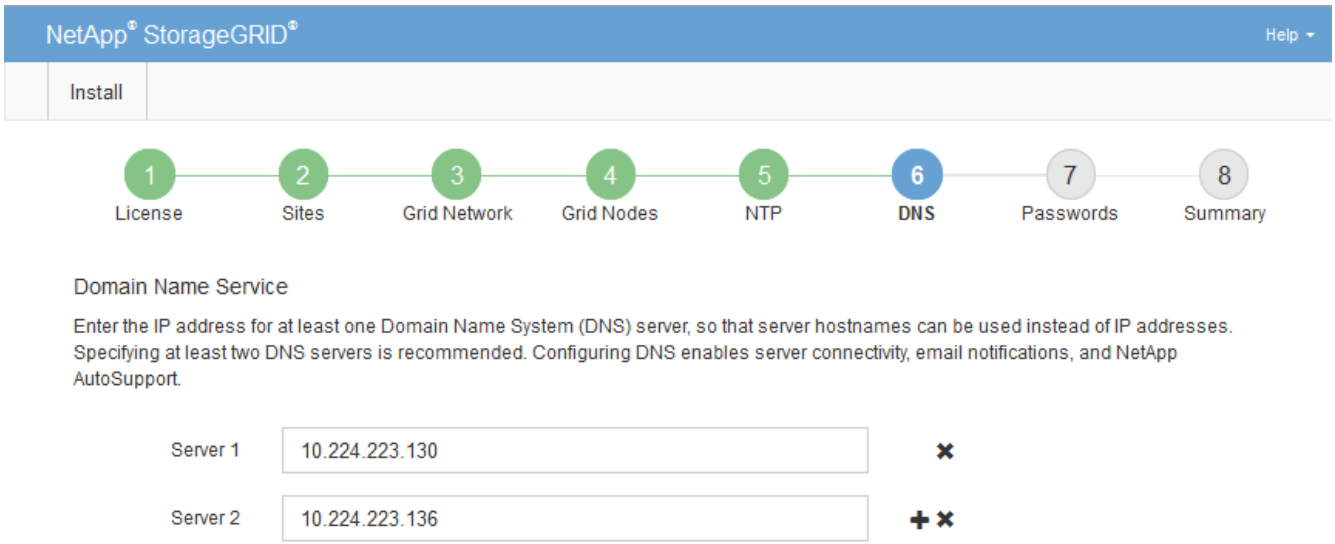
Para garantizar que el funcionamiento sea correcto, especifique dos o tres servidores DNS. Si especifica más de tres, es posible que solo se utilicen tres debido a las limitaciones conocidas del sistema operativo en algunas plataformas. Si tiene restricciones de enrutamiento en su entorno, puede "Personalice la lista de servidores DNS" Para nodos individuales (normalmente todos los nodos en un sitio) para usar un conjunto diferente de hasta tres servidores DNS.

Si es posible, utilice servidores DNS a los que cada sitio puede acceder localmente para asegurarse de que un sitio islandn pueda resolver los FQDN para destinos externos.

Si se omite o se configura incorrectamente la información del servidor DNS, se activa una alarma DNST en el servicio SSM de cada nodo de cuadrícula. La alarma se borra cuando DNS está configurado correctamente y la nueva información del servidor ha llegado a todos los nodos de la cuadrícula.

Pasos

1. Especifique la dirección IPv4 para al menos un servidor DNS en el cuadro de texto **servidor 1**.
2. Si es necesario, seleccione el signo más junto a la última entrada para agregar entradas adicionales del servidor.



La práctica recomendada es especificar al menos dos servidores DNS. Puede especificar hasta seis servidores DNS.

3. Seleccione **Siguiente**.

Especifique las contraseñas del sistema StorageGRID

Como parte de la instalación del sistema StorageGRID, debe introducir las contraseñas que se utilizarán para proteger el sistema y realizar tareas de mantenimiento.

Acerca de esta tarea

Utilice la página instalar contraseñas para especificar la contraseña de acceso de aprovisionamiento y la

contraseña de usuario raíz de administración de grid.

- La clave de acceso de aprovisionamiento se usa como clave de cifrado y el sistema StorageGRID no la almacena.
- Debe disponer de la clave de acceso de aprovisionamiento para los procedimientos de instalación, ampliación y mantenimiento, incluida la descarga del paquete de recuperación. Por lo tanto, es importante almacenar la frase de contraseña de aprovisionamiento en una ubicación segura.
- Puede cambiar la frase de acceso de aprovisionamiento desde Grid Manager si tiene la actual.
- La contraseña de usuario raíz de gestión de grid se puede cambiar mediante Grid Manager.
- Las contraseñas de SSH y la consola de línea de comandos generadas aleatoriamente se almacenan en la `Passwords.txt` En el paquete de recuperación.

Pasos

1. En **frase de paso de aprovisionamiento**, introduzca la contraseña de provisión que será necesaria para realizar cambios en la topología de la red del sistema StorageGRID.

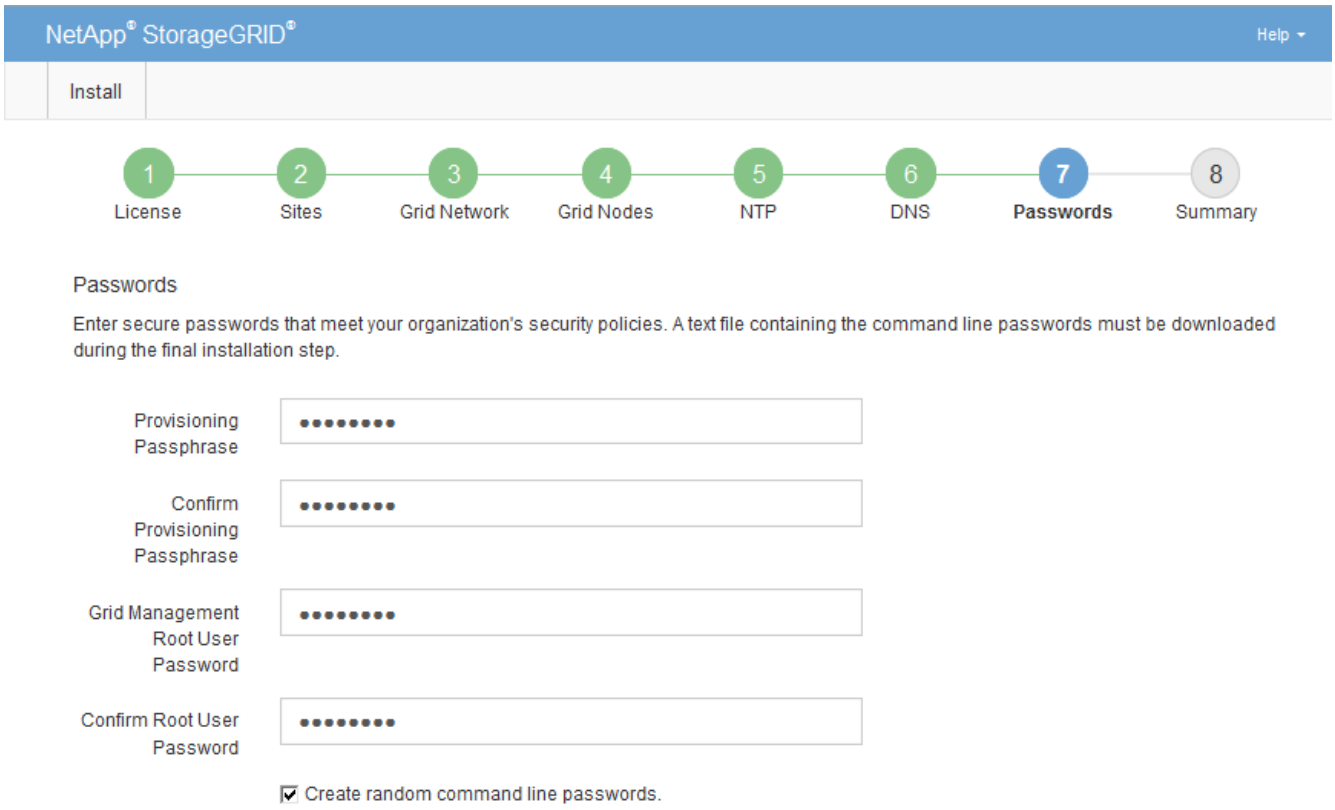
   Almacenar la clave de acceso de aprovisionamiento en un lugar seguro.

   > Si después de la instalación ha finalizado y desea cambiar la contraseña de acceso de aprovisionamiento más tarde, puede utilizar Grid Manager. Seleccione **CONFIGURACIÓN** > **Control de acceso**> **contraseñas de cuadrícula**.

2. En **Confirmar la frase de paso de aprovisionamiento**, vuelva a introducir la contraseña de aprovisionamiento para confirmarla.
3. En **Grid Management Root User Password**, introduzca la contraseña que se utilizará para acceder a Grid Manager como usuario “root”.

   Guarde la contraseña en un lugar seguro.

4. En **Confirmar contraseña de usuario raíz**, vuelva a introducir la contraseña de Grid Manager para confirmarla.



5. Si va a instalar una cuadrícula con fines de prueba de concepto o demostración, opcionalmente desactive la casilla de verificación **Crear contraseñas de línea de comandos aleatorias**.

   En las implementaciones de producción, las contraseñas aleatorias deben utilizarse siempre por motivos de seguridad. Borrar **Crear contraseñas de línea de comandos aleatorias** solo para las cuadrículas de demostración si desea utilizar contraseñas predeterminadas para acceder a los nodos de la cuadrícula desde la línea de comandos usando la cuenta “root” o “admin”.

   > Se le solicitará que descargue el archivo del paquete de recuperación (`sgws-recovery-package-id-revision.zip`) Después de hacer clic en **instalar** en la página Resumen. Debe "descargue este archivo" para completar la instalación. Las contraseñas que se necesitan para acceder al sistema se almacenan en la `Passwords.txt` Archivo, incluido en el archivo del paquete de recuperación.

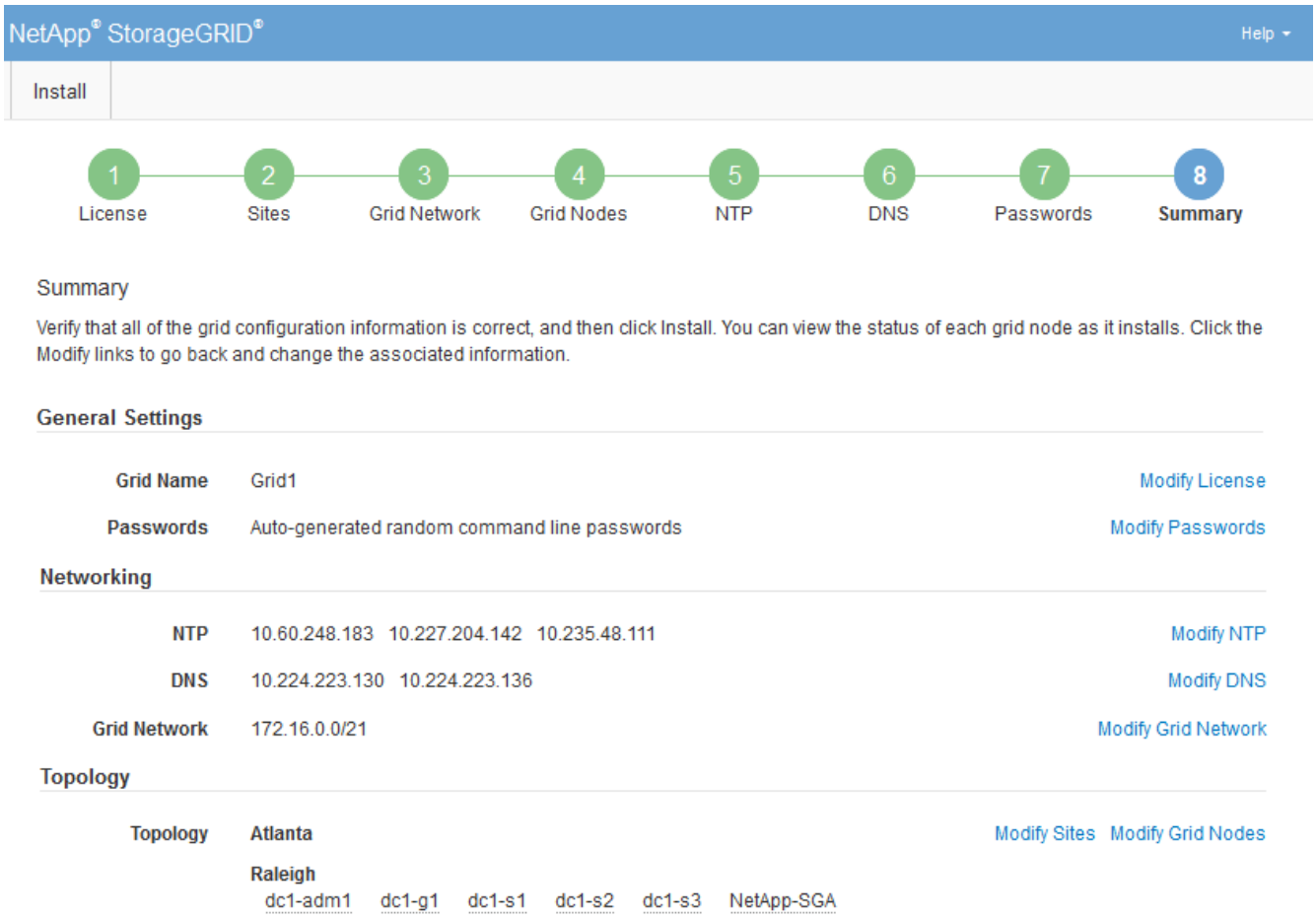
6. Haga clic en **Siguiente**.

Revise la configuración y complete la instalación

Debe revisar con cuidado la información de configuración que ha introducido para asegurarse de que la instalación se complete correctamente.

Pasos

1. Abra la página **Resumen**.



2. Verifique que toda la información de configuración de la cuadrícula sea correcta. Utilice los enlaces Modify de la página Summary para volver atrás y corregir los errores.
3. Haga clic en **instalar**.

> Si un nodo está configurado para utilizar la red de cliente, la puerta de enlace predeterminada para ese nodo cambia de la red de cuadrícula a la red de cliente cuando hace clic en **instalar**. Si se pierde la conectividad, debe asegurarse de acceder al nodo de administración principal a través de una subred accesible. Consulte "Directrices sobre redes" para obtener más detalles.

4. Haga clic en **Descargar paquete de recuperación**.

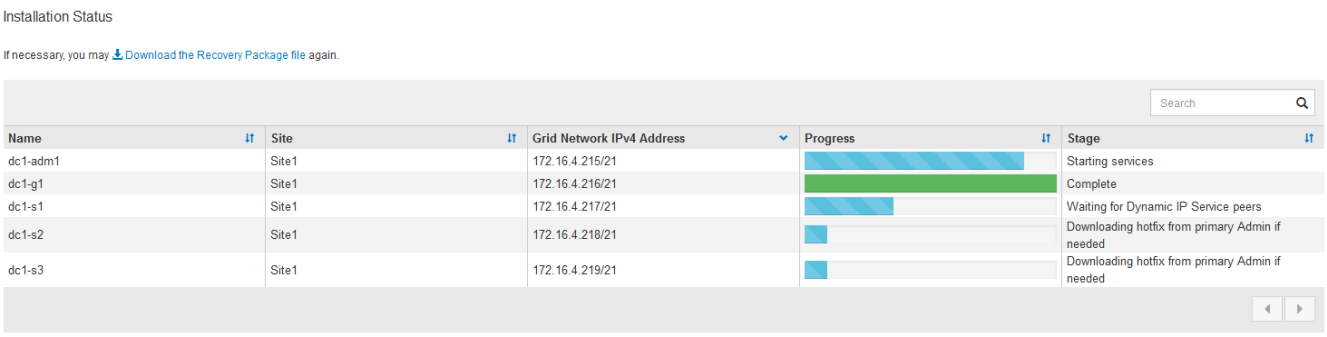
   Cuando la instalación avance hasta el punto en el que se define la topología de la cuadrícula, se le pedirá que descargue el archivo del paquete de recuperación (`.zip`), y confirme que puede obtener acceso al contenido de este archivo. Debe descargar el archivo de paquete de recuperación para que pueda recuperar el sistema StorageGRID si falla uno o más nodos de grid. La instalación continúa en segundo plano, pero no es posible completar la instalación y acceder al sistema StorageGRID hasta que se descargue y verifique este archivo.

5. Compruebe que puede extraer el contenido del `.zip` archivar y, a continuación, guardarlo en dos ubicaciones seguras, seguras e independientes.

> El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

6. Seleccione la casilla de verificación **He descargado y verificado correctamente el archivo del paquete de recuperación** y haga clic en **Siguiente**.

   Si la instalación sigue en curso, aparece la página de estado. Esta página indica el progreso de la instalación para cada nodo de cuadrícula.



   Cuando se llega a la fase completa de todos los nodos de cuadrícula, aparece la página de inicio de sesión de Grid Manager.

7. Inicie sesión en Grid Manager con el usuario "root" y la contraseña que especificó durante la instalación.

Directrices posteriores a la instalación

Después de completar la implementación y la configuración de un nodo de grid, siga estas directrices para el direccionamiento DHCP y los cambios de configuración de red.

- Si se utilizó DHCP para asignar direcciones IP, configure una reserva DHCP para cada dirección IP en las redes que se estén utilizando.

  DHCP solo puede configurarse durante la fase de implementación. No puede configurar DHCP durante la configuración.

  > Los nodos se reinician cuando cambian sus direcciones IP, lo que puede provocar interrupciones de servicio si un cambio de dirección DHCP afecta a varios nodos al mismo tiempo.

- Debe usar los procedimientos de cambio IP si desea cambiar direcciones IP, máscaras de subred y puertas de enlace predeterminadas para un nodo de grid. Consulte "Configurar las direcciones IP".
- Si realiza cambios de configuración de redes, incluidos los cambios de enrutamiento y puerta de enlace, es posible que se pierda la conectividad de cliente al nodo de administración principal y a otros nodos de grid. En función de los cambios de red aplicados, es posible que deba restablecer estas conexiones.

Información general de la instalación de la API de REST

StorageGRID proporciona la API de instalación de StorageGRID para realizar tareas de instalación.

La API utiliza la plataforma API de código abierto de Swagger para proporcionar la documentación de API. Swagger permite que tanto desarrolladores como no desarrolladores interactúen con la API en una interfaz de usuario que ilustra cómo responde la API a los parámetros y las opciones. En esta documentación se asume que está familiarizado con las tecnologías web estándar y el formato de datos JSON.

Cualquier operación de API que realice mediante la página web de documentos de API es una operación en directo. Tenga cuidado de no crear, actualizar o eliminar datos de configuración u otros datos por error.

Cada comando de API REST incluye la URL de la API, una acción HTTP, los parámetros de URL necesarios o opcionales y una respuesta de API esperada.

API de instalación de StorageGRID

La API de instalación de StorageGRID solo está disponible cuando está configurando inicialmente el sistema StorageGRID y si necesita realizar una recuperación de nodo de administración principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de la API, vaya a la página web de instalación en el nodo de administración principal y seleccione **Ayuda** > **Documentación de la API** en la barra de menús.

La API de instalación de StorageGRID incluye las siguientes secciones:

- **Config** — Operaciones relacionadas con la versión del producto y las versiones de la API. Puede mostrar la versión de la versión del producto y las versiones principales de la API que admite esa versión.
- **Grid** — Operaciones de configuración a nivel de cuadrícula. Puede obtener y actualizar la configuración de la cuadrícula, incluidos los detalles de la cuadrícula, las subredes de la red de cuadrícula, las contraseñas de la cuadrícula y las direcciones IP del servidor NTP y DNS.
- **Nodes** — Operaciones de configuración a nivel de nodo. Puede recuperar una lista de nodos de cuadrícula, eliminar un nodo de cuadrícula, configurar un nodo de cuadrícula, ver un nodo de cuadrícula y restablecer la configuración de un nodo de cuadrícula.
- **Aprovisionamiento** — Operaciones de aprovisionamiento. Puede iniciar la operación de aprovisionamiento y ver el estado de la operación de aprovisionamiento.
- **Recuperación** — Operaciones de recuperación del nodo de administración principal. Puede restablecer la información, cargar el paquete de recuperación, iniciar la recuperación y ver el estado de la operación de recuperación.
- **Paquete de recuperación** — Operaciones para descargar el paquete de recuperación.
- **Esquemas** — esquemas API para implementaciones avanzadas
- **Sites** — Operaciones de configuración a nivel de sitio. Puede crear, ver, eliminar y modificar un sitio.

A continuación, ¿dónde ir

Después de completar una instalación, realice las tareas de integración y configuración necesarias. Puede realizar las tareas opcionales según sea necesario.

Tareas requeridas

- "Cree una cuenta de inquilino" Para cada protocolo de cliente (Swift o S3) que se utilizará para almacenar objetos en el sistema StorageGRID.
- "Acceso al sistema de control" mediante la configuración de grupos y cuentas de usuario. Opcionalmente, puede hacerlo "configurar un origen de identidad federado" (Como Active Directory u OpenLDAP), para que pueda importar grupos y usuarios de administración. O bien, puede hacerlo "crear usuarios y grupos locales".
- Integre y pruebe el "S3 API" o. "API Swift" Aplicaciones cliente que utilizará para cargar objetos en el

sistema StorageGRID.

- "Configure las reglas de gestión de la vida útil de la información (ILM) y la política de ILM" se desea utilizar para proteger los datos de objetos.
- Si la instalación incluye nodos de almacenamiento del dispositivo, utilice el sistema operativo SANtricity para realizar las siguientes tareas:
  - Conéctese a cada dispositivo StorageGRID.
  - Comprobar recepción de datos AutoSupport.

  Consulte "Configure el hardware".
- Revise y siga el "Directrices de fortalecimiento del sistema StorageGRID" eliminar los riesgos de seguridad.
- "Configure las notificaciones por correo electrónico para las alertas del sistema".
- Si el sistema StorageGRID incluye algún nodo de archivado (obsoleto), configure la conexión del nodo de archivado al sistema de almacenamiento de archivado externo de destino.

Tareas opcionales

- "Actualice las direcciones IP del nodo de grid" Si han cambiado desde que planificó el despliegue y generó el paquete de recuperación.
- "Configurar el cifrado del almacenamiento", si es necesario.
- "Configurar la compresión del almacenamiento" para reducir el tamaño de los objetos almacenados, si es necesario.

Solucionar problemas de instalación

Si se produce algún problema durante la instalación del sistema StorageGRID, puede acceder a los archivos de registro de la instalación. Es posible que el soporte técnico también deba utilizar los archivos de registro de instalación para resolver problemas.

Los siguientes archivos de registro de instalación están disponibles en el contenedor que ejecuta cada nodo:

- `/var/local/log/install.log` (se encuentra en todos los nodos de grid)
- `/var/local/log/gdu-server.log` (Encontrado en el nodo de administración principal)

Los siguientes archivos de registro de instalación están disponibles en el host:

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

Para obtener información sobre cómo acceder a los archivos de registro, consulte "Recopilar archivos de registro y datos del sistema".

Información relacionada

"Solucionar los problemas de un sistema StorageGRID"

Ejemplo de /etc/sysconfig/network-scripts

Se pueden utilizar los archivos de ejemplo para agregar cuatro interfaces físicas de Linux en un único enlace LACP y, a continuación, establecer tres interfaces de VLAN que tendencia al vínculo para su uso como interfaces de red Grid, de administrador y de cliente de StorageGRID.

Interfaces físicas

Tenga en cuenta que los switches de los otros extremos de los enlaces también deben tratar los cuatro puertos como un único enlace troncal o canal de puerto LACP y deben pasar, al menos, las tres VLAN de referencia con etiquetas.

/etc/sysconfig/network-scripts/ifcfg-ens160

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens192

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens224

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens256

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

Interfaz de vínculo

/etc/sysconfig/network-scripts/ifcfg-bond0

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

Interfaces de VLAN

/etc/sysconfig/network-scripts/ifcfg-bond0.1001

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1002

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1003

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

Instalar StorageGRID en Ubuntu o Debian

Inicio rápido para instalar StorageGRID en Ubuntu o Debian

Siga estos pasos de alto nivel para instalar un nodo StorageGRID Ubuntu o Debian.

1 **Preparación**

- Descubra "Arquitectura de StorageGRID y topología de red".
- Conozca los aspectos específicos de "Redes StorageGRID".
- Reúna y prepare el "Información y materiales requeridos".
- Prepare lo necesario "CPU y RAM".
- Prevea "requisitos de rendimiento y almacenamiento".
- "Prepare los servidores Linux" Que alojará sus nodos de StorageGRID.

2 **Puesta en marcha**

Desplegar nodos de grid. Cuando se implementan nodos de grid, se crean como parte del sistema StorageGRID y se conectan a una o varias redes.

- Para implementar nodos de grid basados en software en los hosts que preparó en el paso 1, utilice la línea de comandos de Linux y. "archivos de configuración de nodos".
- Para poner en marcha los nodos de dispositivos StorageGRID, siga el "Inicio rápido para la instalación de hardware".

3 Configuración

Cuando se hayan desplegado todos los nodos, utilice Grid Manager a. "configure la cuadrícula y complete la instalación".

Automatizar la instalación

Para ahorrar tiempo y proporcionar coherencia, puede automatizar la instalación del servicio de host de StorageGRID y la configuración de nodos de grid.

- Use un marco de orquestación estándar como Ansible, Puppet o Chef para automatizar:
  - Instalación de RHEL
  - La configuración de redes y almacenamiento
  - Instalación del motor de contenedor y del servicio de host StorageGRID
  - Puesta en marcha de nodos de grid virtual

  Consulte "Automatizar la instalación y configuración del servicio de host de StorageGRID".
- Después de implementar los nodos de grid, "Automatice la configuración del sistema StorageGRID" Usando el script de configuración de Python proporcionado en el archivo de instalación.
- "Automatice la instalación y la configuración de los nodos de grid de dispositivos"
- Si es un desarrollador avanzado de implementaciones de StorageGRID, automatice la instalación de los nodos de grid mediante el "Instalación de la API de REST".

Planificar y preparar la instalación en Ubuntu o Debian

Información y materiales requeridos

Antes de instalar StorageGRID, recopile y prepare la información y los materiales necesarios.

Información obligatoria

Plan de red

Qué redes pretende conectar a cada nodo StorageGRID. StorageGRID admite múltiples redes para la separación del tráfico, la seguridad y la conveniencia administrativa.

Consulte StorageGRID "Directrices sobre redes".

Información de red

A menos que se utilice DHCP, las direcciones IP para asignar a cada nodo de grid y las direcciones IP de los servidores DNS y NTP.

Servidores para nodos de grid

Identificar un conjunto de servidores (físicos, virtuales o ambos) que, agregado, proporcione los recursos suficientes para respaldar el número y el tipo de nodos de StorageGRID que va a implementar.

> Si la instalación de StorageGRID no utilizará nodos de almacenamiento del dispositivo StorageGRID (hardware), debe usar almacenamiento RAID de hardware con caché de escritura respaldada por batería (BBWC). StorageGRID no admite el uso de redes de área de almacenamiento virtuales (VSAN), RAID de software ni ninguna protección RAID.

Migración de nodos (si es necesario)

Comprenda el "requisitos para la migración de nodos", si desea realizar el mantenimiento programado en hosts físicos sin ninguna interrupción del servicio.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Materiales requeridos

Licencia de StorageGRID de NetApp

Debe tener una licencia de NetApp válida y con firma digital.

> En el archivo de instalación de StorageGRID se incluye una licencia que no sea de producción, y que se puede utilizar para pruebas y entornos Grid de prueba de concepto.

Archivo de instalación de StorageGRID

"Descargue el archivo de instalación de StorageGRID y extraiga los archivos".

Portátil de servicio

El sistema StorageGRID se instala a través de un ordenador portátil de servicio.

El portátil de servicio debe tener:

- Puerto de red
- Cliente SSH (por ejemplo, PuTTY)
- "Navegador web compatible"

Documentación de StorageGRID

- "Notas de la versión"
- "Instrucciones para administrar StorageGRID"

Descargue y extraiga los archivos de instalación de StorageGRID

Debe descargar el archivo de instalación de StorageGRID y extraer los archivos necesarios.

Pasos

1. Vaya a la "Página de descargas de NetApp para StorageGRID".
2. Seleccione el botón para descargar la última versión, o seleccione otra versión en el menú desplegable y seleccione **Ir**.

3. Inicie sesión con el nombre de usuario y la contraseña de su cuenta de NetApp.
4. Si aparece una declaración Precaution/MustRead, léala y seleccione la casilla de verificación.

> Debe aplicar cualquier revisión requerida después de instalar la versión de StorageGRID. Para obtener más información, consulte "procedimiento de revisión en las instrucciones de recuperación y mantenimiento"

5. Lea el Contrato de licencia de usuario final, seleccione la casilla de verificación y, a continuación, seleccione * Aceptar y continuar *.

   Aparece la página de descargas de la versión seleccionada. La página contiene tres columnas:

6. En la columna **instalar StorageGRID**, seleccione el archivo .tgz o .zip para Ubuntu o Debian.

> Seleccione la `.zip` Archivo si está ejecutando Windows en el portátil de servicio.

7. Guarde y extraiga el archivo de archivado.
8. Elija los archivos que necesite en la siguiente lista.

   El conjunto de archivos que necesita depende de la topología de grid planificada y de cómo se implementará la cuadrícula StorageGRID.

> Las rutas enumeradas en la tabla son relativas al directorio de nivel superior instalado por el archivo de instalación extraído.

Ruta y nombre de archivo	Descripción
	Archivo de texto que describe todos los archivos contenidos en el archivo de descarga de StorageGRID.
	Un archivo de licencia de NetApp que no es de producción y que se puede usar para pruebas e implementaciones conceptuales.
	PAQUETE DEB para instalar las imágenes del nodo StorageGRID en hosts de Ubuntu o Debian.
	Suma de comprobación MD5 para el archivo `/debs/storagegrid-webscale-images-version-SHA.deb`.
	PAQUETE DEB para instalar el servicio de host de StorageGRID en hosts de Ubuntu o Debian.
Herramienta de secuencia de comandos de la implementación	Descripción

Ruta y nombre de archivo	Descripción
	Script Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Una secuencia de comandos Python que se utiliza para automatizar la configuración de los dispositivos StorageGRID.
	Ejemplo de secuencia de comandos Python que puede utilizar para iniciar sesión en la API de gestión de grid cuando está activado el inicio de sesión único. También puede utilizar este script para ping federate.
	Ejemplo de archivo de configuración para utilizar con `configure-storagegrid.py` guión.
	Un archivo de configuración en blanco para usar con el `configure-storagegrid.py` guión.
	Ejemplo de rol de Ansible y libro de aplicaciones para configurar hosts Ubuntu o Debian para la implementación del contenedor StorageGRID. Puede personalizar el rol o el libro de estrategia según sea necesario.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de grid cuando se activa el inicio de sesión único (SSO) mediante Active Directory o ping federate.
	Un guion de ayuda llamado por el compañero `storagegrid-ssoauth-azure.py` Script de Python para realizar interacciones SSO con Azure.
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno StorageGRID que no sea de producción para probar la compatibilidad de la actualización.

Requisitos de software para Ubuntu y Debian

Es posible usar una máquina virtual para alojar cualquier tipo de nodo StorageGRID. Se necesita una máquina virtual para cada nodo de grid.

Para instalar StorageGRID en Ubuntu o Debian, debe instalar algunos paquetes de software de terceros. Algunas distribuciones de Linux soportadas no contienen estos paquetes por defecto. Las versiones del paquete de software en las que se han probado las instalaciones de StorageGRID incluyen las que se indican en esta página.

> Si selecciona una opción de instalación en tiempo de ejecución de contenedor y distribución de Linux que requiera alguno de estos paquetes y la distribución de Linux no los instala automáticamente, instale una de las versiones que se enumeran aquí, si está disponible en su proveedor o en el proveedor de soporte para su distribución de Linux. De lo contrario, utilice las versiones de paquete predeterminadas disponibles en su proveedor.

> Todas las opciones de instalación requieren Podman o Docker. No instale ambos paquetes. Instale solo el paquete requerido por su opción de instalación.

Versiones de Python probadas

- 3,5.2-2
- 3,6.8-2
- 3,6.8-38
- 3,6.9-1
- 3,7.3-1
- 3,8.10-0
- 3,9.2-1
- 3,9.10-2
- 3,9.16-1
- 3.10.6-1
- 3.11.2-6

Versiones de Podman probadas

- 3,2.3-0
- 3,4.4+ds1
- 4,1.1-7
- 4,2.0-11
- 4,3.1+ds1-8+b1
- 4,4.1-8
- 4,4.1-12

Versiones de Docker probadas

> La compatibilidad de Docker está obsoleta y se eliminará en un lanzamiento futuro.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23,0.6-1

- Docker-CE 24,0.2-1
- Docker-CE 24,0.4-1
- Docker-CE 24,0.5-1
- Docker-CE 24,0.7-1
- 1.5-2

Requisitos de CPU y RAM

Antes de instalar el software StorageGRID, verifique y configure el hardware de manera que esté listo para admitir el sistema StorageGRID.

Cada nodo StorageGRID requiere los siguientes recursos mínimos:

- Núcleos de CPU: 8 por nodo
- RAM: Al menos 24 GB por nodo y de 2 a 16 GB menos que la RAM total del sistema, en función de la RAM total disponible y la cantidad de software que no sea StorageGRID que se ejecute en el sistema

Asegúrese de que el número de nodos StorageGRID que tiene previsto ejecutar en cada host físico o virtual no supere el número de núcleos de CPU o la RAM física disponible. Si los hosts no están dedicados a ejecutar StorageGRID (no se recomienda), asegúrese de tener en cuenta los requisitos de recursos de las otras aplicaciones.

> Supervise el uso de la CPU y la memoria de forma regular para garantizar que estos recursos siguen teniendo la capacidad de adaptarse a su carga de trabajo. Por ejemplo, si se dobla la asignación de RAM y CPU de los nodos de almacenamiento virtual, se proporcionarán recursos similares a los que se proporcionan para los nodos de dispositivos StorageGRID. Además, si la cantidad de metadatos por nodo supera los 500 GB, puede aumentar la memoria RAM por nodo a 48 GB o más. Para obtener información sobre la gestión del almacenamiento de metadatos de objetos, el aumento del valor de Espacio Reservado de Metadatos y la supervisión del uso de CPU y memoria, consulte las instrucciones para "administración", "Supervisión", y. "actualizar" StorageGRID

Si la tecnología de subprocesos múltiples está habilitada en los hosts físicos subyacentes, puede proporcionar 8 núcleos virtuales (4 núcleos físicos) por nodo. Si el subprocesamiento no está habilitado en los hosts físicos subyacentes, debe proporcionar 8 núcleos físicos por nodo.

Si utiliza máquinas virtuales como hosts y tiene control del tamaño y el número de máquinas virtuales, debe utilizar una única máquina virtual para cada nodo StorageGRID y ajustar el tamaño de la máquina virtual según corresponda.

Para implementaciones de producción, no debe ejecutar varios nodos de almacenamiento en el mismo hardware de almacenamiento físico o host virtual. Cada nodo de almacenamiento de una única puesta en marcha de StorageGRID debe tener su propio dominio de fallos aislado. Puede maximizar la durabilidad y disponibilidad de los datos de objetos si se asegura de que un único error de hardware solo pueda afectar a un único nodo de almacenamiento.

Consulte también "Los requisitos de almacenamiento y rendimiento".

Los requisitos de almacenamiento y rendimiento

Debe comprender los requisitos de almacenamiento de los nodos de StorageGRID, de

tal modo que pueda proporcionar espacio suficiente para admitir la configuración inicial y la ampliación de almacenamiento futura.

Los nodos de StorageGRID requieren tres categorías lógicas de almacenamiento:

- * Container pool*: Almacenamiento de nivel de rendimiento (10K SAS o SSD) para los contenedores de nodos, que se asignará al controlador de almacenamiento Docker cuando instale y configure Docker en los hosts que serán compatibles con sus nodos StorageGRID.
- **Datos del sistema** — almacenamiento de nivel de rendimiento (10K SAS o SSD) para almacenamiento persistente por nodo de datos del sistema y registros de transacciones, que los servicios host StorageGRID consumirán y asignarán a nodos individuales.
- **Almacenamiento masivo de datos de objetos**: Almacenamiento en niveles de rendimiento (10K SAS o SSD) y capacidad (NL-SAS/SATA) para el almacenamiento persistente de datos de objetos y metadatos de objetos.

Se deben utilizar dispositivos de bloques respaldados por RAID para todas las categorías de almacenamiento. No se admiten discos, SSD o JBOD no redundantes. Puede usar almacenamiento RAID compartido o local para cualquiera de las categorías de almacenamiento; sin embargo, si desea usar la funcionalidad de migración de nodos en StorageGRID, debe almacenar tanto los datos del sistema como los datos de objetos en almacenamiento compartido. Para obtener más información, consulte "Requisitos de migración de contenedores de nodos".

Requisitos de rendimiento

El rendimiento de los volúmenes utilizados para el pool de contenedores, los datos del sistema y los metadatos de objetos afecta significativamente el rendimiento general del sistema. Debe usar almacenamiento de nivel de rendimiento (10 000 SAS o SSD) para estos volúmenes a fin de garantizar que el rendimiento de disco sea adecuado en términos de latencia, operaciones de entrada/salida por segundo (IOPS) y rendimiento. Puede usar almacenamiento en niveles de capacidad (NL-SAS/SATA) para el almacenamiento persistente de datos de objetos.

Los volúmenes utilizados para el pool de contenedores, los datos del sistema y los datos de objetos deben tener el almacenamiento en caché de devolución de escritura habilitado. La caché debe estar en un medio protegido o persistente.

Requisitos para hosts que usan almacenamiento de NetApp ONTAP

Si el nodo StorageGRID utiliza almacenamiento asignado de un sistema NetApp ONTAP, confirme que el volumen no tiene una política de organización en niveles de FabricPool habilitada. Al deshabilitar el almacenamiento en niveles de FabricPool para los volúmenes que se usan con los nodos StorageGRID, se simplifica la solución de problemas y las operaciones de almacenamiento.

> No utilice nunca FabricPool para colocar en niveles datos relacionados con StorageGRID en el propio StorageGRID. La organización en niveles de los datos de StorageGRID en StorageGRID aumenta la solución de problemas y la complejidad operativa.

Número de hosts requeridos

Cada sitio StorageGRID requiere como mínimo tres nodos de almacenamiento.

> En una puesta en marcha de producción, no ejecute más de un nodo de almacenamiento en un solo host físico o virtual. El uso de un host dedicado para cada nodo de almacenamiento proporciona un dominio de fallo aislado.

Pueden ponerse en marcha otros tipos de nodos, como los nodos de administrador o los nodos de pasarela, en los mismos hosts o bien en sus propios hosts dedicados, según sea necesario.

Número de volúmenes de almacenamiento para cada host

En la siguiente tabla se muestra el número de volúmenes de almacenamiento (LUN) necesarios para cada host y el tamaño mínimo requerido para cada LUN, en función del cual se pondrán en marcha los nodos en ese host.

El tamaño máximo de LUN probado es 39 TB.

Estos números son para cada host, no para toda la cuadrícula.

Propósito de LUN	Categoría de almacenamiento	Número de LUN	Tamaño mínimo/LUN
Bloque de almacenamiento del motor del contenedor	Pool de contenedores	1	Número total de nodos × 100 GB
`/var/local` volumen	Datos del sistema	1 para cada nodo de este host	90 GB
Nodo de almacenamiento	Datos de objetos	3 para cada nodo de almacenamiento de este host **Nota:** un nodo de almacenamiento basado en software puede tener de 1 a 16 volúmenes de almacenamiento; se recomiendan al menos 3 volúmenes de almacenamiento.	12 TB (4 TB/LUN) CONSULTE Requisitos de almacenamiento para nodos de almacenamiento si quiere más información.
Nodo de almacenamiento (solo metadatos)	Metadatos de objetos	1	4 TB consulte Requisitos de almacenamiento para nodos de almacenamiento si quiere más información. **Nota**: Solo se requiere un rangedb para los nodos de almacenamiento solo de metadatos.
Registros de auditoría del nodo de administrador	Datos del sistema	1 para cada nodo de administrador de este host	200 GB

Propósito de LUN	Categoría de almacenamiento	Número de LUN	Tamaño mínimo/LUN
Tablas Admin Node	Datos del sistema	1 para cada nodo de administrador de este host	200 GB

> En función del nivel de auditoría configurado, el tamaño de las entradas de usuario, como el nombre de clave de objeto S3, Y cuántos datos de registro de auditoría debe conservar, es posible que necesite aumentar el tamaño del LUN del registro de auditoría en cada nodo de administración.Por lo general, un grid genera aproximadamente 1 KB de datos de auditoría por operación de S3. Lo que significaría que un LUN de 200 GB admitiría 70 millones de operaciones al día o 800 operaciones por segundo durante dos o tres días.

Espacio de almacenamiento mínimo para un host

En la siguiente tabla se muestra el espacio de almacenamiento mínimo necesario para cada tipo de nodo. Puede utilizar esta tabla para determinar la cantidad mínima de almacenamiento que debe proporcionar al host en cada categoría de almacenamiento, según la cual se pondrán en marcha los nodos en ese host.

> Las instantáneas de disco no se pueden utilizar para restaurar los nodos de grid. En su lugar, consulte "recuperación de nodo de grid" procedimientos para cada tipo de nodo.

Tipo de nodo	Pool de contenedores	Datos del sistema	Datos de objetos
Nodo de almacenamiento	100 GB	90 GB	4.000 GB
Nodo de administración	100 GB	490 GB (3 LUN)	*no aplicable*
Nodo de puerta de enlace	100 GB	90 GB	*no aplicable*
Nodo de archivado	100 GB	90 GB	*no aplicable*

Ejemplo: Calcular los requisitos de almacenamiento para un host

Suponga que planea implementar tres nodos en el mismo host: Un nodo de almacenamiento, un nodo de administración y un nodo de puerta de enlace. Debe proporcionar un mínimo de nueve volúmenes de almacenamiento al host. Necesitará un mínimo de 300 GB de almacenamiento de nivel de rendimiento para los contenedores de nodos, 670 GB de almacenamiento de nivel de rendimiento para los datos del sistema y los registros de transacciones, y 12 TB de almacenamiento de nivel de capacidad para los datos de objetos.

Tipo de nodo	Propósito de LUN	Número de LUN	Tamaño de LUN
Nodo de almacenamiento	Pool de almacenamiento de Docker	1	300 GB (100 GB/nodo)
Nodo de almacenamiento	`/var/local` volumen	1	90 GB

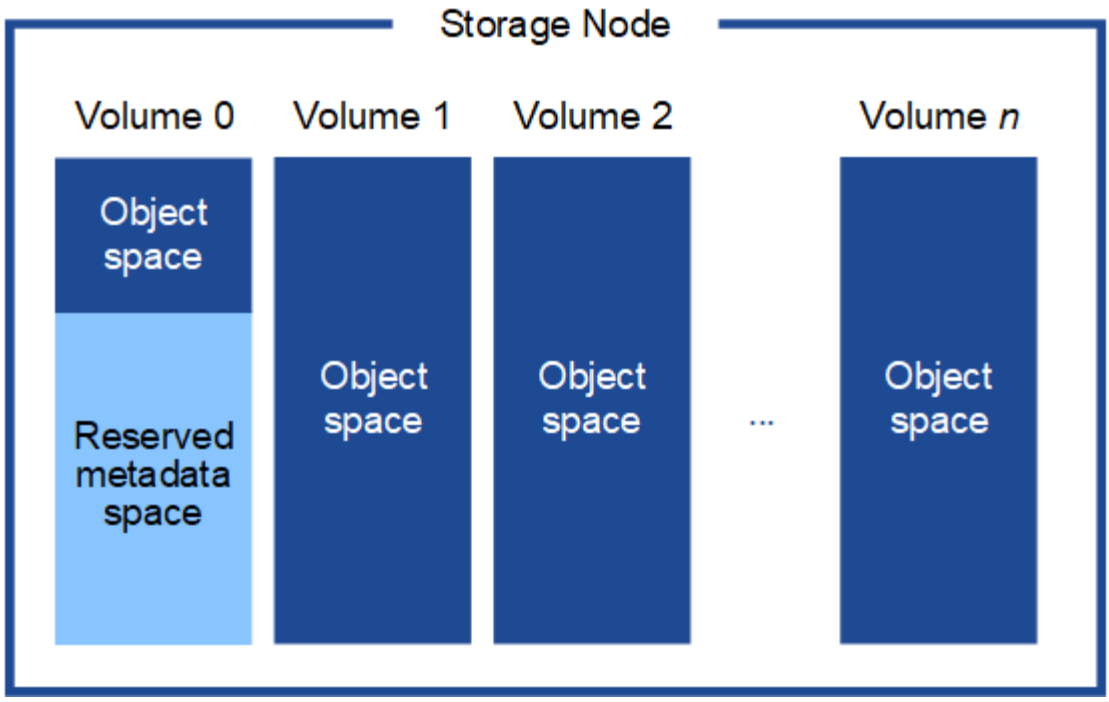
Tipo de nodo	Propósito de LUN	Número de LUN	Tamaño de LUN
Nodo de almacenamiento	Datos de objetos	3	12 TB (4 TB/LUN)
Nodo de administración	`/var/local` volumen	1	90 GB
Nodo de administración	Registros de auditoría del nodo de administrador	1	200 GB
Nodo de administración	Tablas Admin Node	1	200 GB
Nodo de puerta de enlace	`/var/local` volumen	1	90 GB
Total		**9**	• Piscina de contenedores:* 300 GB **Datos del sistema:** 670 GB **Datos del objeto:** 12,000 GB

Requisitos de almacenamiento para nodos de almacenamiento

Un nodo de almacenamiento basado en software puede tener de 1 a 16 volúmenes de almacenamiento: Se recomiendan -3 o más volúmenes de almacenamiento. Cada volumen de almacenamiento debe ser 4 TB o mayor.

> Un nodo de almacenamiento de dispositivo puede tener hasta 48 volúmenes de almacenamiento.

Como se muestra en la figura, StorageGRID reserva espacio para los metadatos del objeto en el volumen de almacenamiento 0 de cada nodo de almacenamiento. Cualquier espacio restante en el volumen de almacenamiento 0 y cualquier otro volumen de almacenamiento en el nodo de almacenamiento se utilizan exclusivamente para los datos de objetos.



Para proporcionar redundancia y proteger los metadatos de objetos de la pérdida, StorageGRID almacena tres copias de los metadatos para todos los objetos del sistema en cada sitio. Las tres copias de metadatos de objetos se distribuyen uniformemente por todos los nodos de almacenamiento de cada sitio.

Cuando se instala un grid con nodos de almacenamiento solo de metadatos, el grid también debe contener un número mínimo de nodos para el almacenamiento de objetos. Consulte "Tipos de nodos de almacenamiento" Para obtener más información sobre nodos de almacenamiento solo de metadatos.

- Para un grid de sitio único, hay al menos dos nodos de almacenamiento configurados para objetos y metadatos.
- Para un grid de varios sitios, al menos un nodo de almacenamiento por sitio está configurado para objetos y metadatos.

Cuando se asigna espacio al volumen 0 de un nuevo nodo de almacenamiento, se debe garantizar que haya espacio suficiente para la porción de ese nodo de todos los metadatos de objetos.

- Como mínimo, debe asignar al menos 4 TB al volumen 0.

> Si solo se utiliza un volumen de almacenamiento para un nodo de almacenamiento y se asignan 4 TB o menos al volumen, es posible que el nodo de almacenamiento introduzca el estado de solo lectura de almacenamiento al inicio y almacene solo metadatos de objetos.

> Si se asigna menos de 500 GB al volumen 0 (solo para uso no en producción), el 10 % de la capacidad del volumen de almacenamiento se reserva para metadatos.

- Si va a instalar un nuevo sistema (StorageGRID 11,6 o superior) y cada nodo de almacenamiento tiene 128 GB o más de RAM, asigne 8 TB o más al volumen 0. Al usar un valor mayor para el volumen 0, se puede aumentar el espacio permitido para los metadatos en cada nodo de almacenamiento.
- Al configurar nodos de almacenamiento diferentes para un sitio, utilice el mismo ajuste para el volumen 0 si es posible. Si un sitio contiene nodos de almacenamiento de distintos tamaños, el nodo de almacenamiento con el volumen más pequeño 0 determinará la capacidad de metadatos de ese sitio.

Para obtener más información, vaya a. "Gestione el almacenamiento de metadatos de objetos".

Requisitos de migración de contenedores de nodos

La función de migración de nodos permite mover manualmente un nodo de un host a otro. Normalmente, ambos hosts están en el mismo centro de datos físico.

La migración de nodos le permite realizar el mantenimiento de un host físico sin interrumpir las operaciones de grid. Se mueven todos los nodos de StorageGRID, uno por vez, a otro host antes de desconectar el host físico. La migración de nodos requiere solamente un corto tiempo de inactividad para cada nodo y no debe afectar al funcionamiento o a la disponibilidad de los servicios de grid.

Si desea utilizar la función de migración de nodos StorageGRID, la implementación debe satisfacer requisitos adicionales:

- Nombres de interfaces de red consistentes entre los hosts de un único centro de datos físico
- Almacenamiento compartido para metadatos de StorageGRID y volúmenes de repositorios de objetos al que todos los hosts pueden acceder en un único centro de datos físico. Por ejemplo, puede usar cabinas de almacenamiento E-Series de NetApp.

Si utiliza hosts virtuales y la capa de hipervisor subyacente admite la migración de máquinas virtuales, es posible que desee utilizar esta función en lugar de la función de migración de nodos de StorageGRID. En este caso, puede ignorar estos requisitos adicionales.

Antes de realizar una migración o mantenimiento del hipervisor, apague los nodos correctamente. Consulte las instrucciones para "apagar un nodo de grid".

No se admite la migración en vivo de VMware

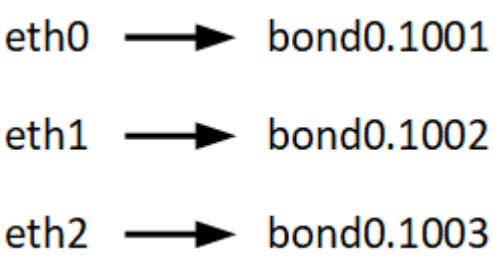
Al realizar una instalación completa en máquinas virtuales de VMware, OpenStack Live Migration y VMware LIVE vMotion provocan que la hora del reloj de la máquina virtual cambie y que los nodos de grid de ningún tipo no sean compatibles. Aunque es poco frecuente, las horas de reloj incorrectas pueden provocar la pérdida de datos o actualizaciones de configuración.

Es compatible con la migración de datos fríos. En la migración en frío, debe apagar los nodos de StorageGRID antes de migrarlos entre hosts. Consulte las instrucciones para "apagar un nodo de grid".

Nombres de interfaces de red consistentes

Para mover un nodo de un host a otro, el servicio de host StorageGRID debe tener cierta confianza en que la conectividad de red externa que tiene el nodo en su ubicación actual puede duplicarse en la nueva ubicación. Obtiene esta confianza mediante el uso de nombres de interfaz de red consistentes en los hosts.

Suponga, por ejemplo, que StorageGRID NodeA que se ejecuta en Host1 se ha configurado con las siguientes asignaciones de interfaz:



El lado izquierdo de las flechas corresponde a las interfaces tradicionales vistas desde un contenedor StorageGRID (es decir, las interfaces Grid, Admin y Client Network, respectivamente). El lado derecho de las flechas corresponde a las interfaces de host reales que proporcionan estas redes, que son tres interfaces VLAN subordinadas al mismo vínculo de interfaz física.

Ahora, supongamos que desea migrar NodeA a Host2. Si Host2 también tiene interfaces denominadas bond0.1001, bond0.1002, y bond0.1003, el sistema permitirá el movimiento, suponiendo que las interfaces con nombre similar proporcionarán la misma conectividad en Host2 que en Host1. Si Host2 no tiene interfaces con los mismos nombres, no se permitirá la transferencia.

Existen muchas formas de lograr una nomenclatura de interfaz de red coherente en varios hosts; consulte "Configure la red del host" para algunos ejemplos.

Almacenamiento compartido

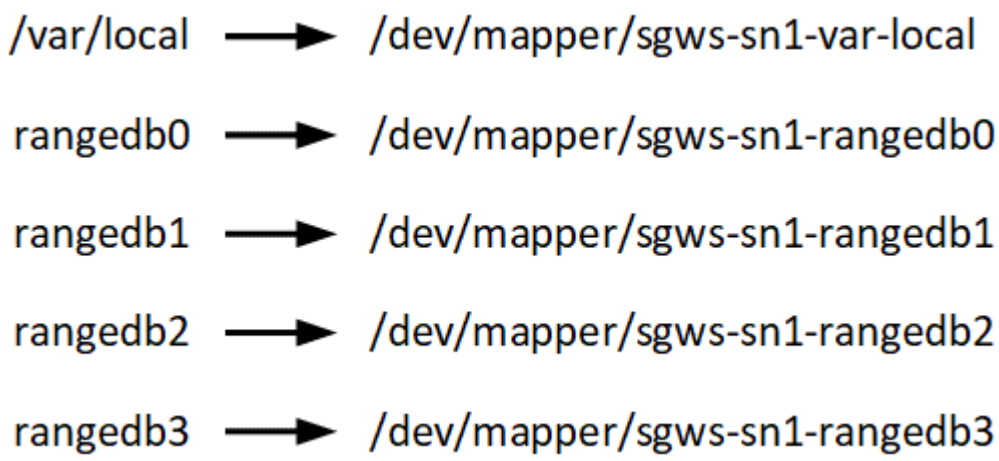
Para lograr migraciones de nodos rápidas y de baja sobrecarga, la función de migración de nodos de StorageGRID no mueve físicamente datos del nodo. En su lugar, la migración de nodos se realiza como par de operaciones de exportación e importación, de la siguiente manera:

Pasos

1. Durante la operación de «exportación de nodo», se extrae una pequeña cantidad de datos de estado persistente del contenedor de nodos que se ejecuta en el HostA y se almacena en caché en el volumen de datos del sistema de ese nodo. A continuación, se instancia el contenedor de nodos en Hosta.
2. Durante la operación de importación de nodos, se instancian el contenedor de nodos en el host B que utiliza la misma interfaz de red y las asignaciones de almacenamiento en bloque que estaban vigentes en el host. A continuación, los datos de estado persistente en caché se insertan en la nueva instancia.

Dado este modo de funcionamiento, es necesario acceder a todos los volúmenes de almacenamiento de objetos y datos del sistema del nodo desde Hosta y HostB para permitir la migración y funcionar. Además, deben haberse asignado al nodo utilizando nombres que se garanticen que hacen referencia a las mismas LUN en Hosta y HostB.

En el siguiente ejemplo se muestra una solución para la asignación de dispositivos de bloque para un nodo de almacenamiento de StorageGRID, donde se está utilizando el acceso múltiple de DM en los hosts y se ha utilizado el campo de alias en `/etc/multipath.conf` para proporcionar nombres de dispositivos de bloque coherentes y fáciles de usar disponibles en todos los hosts.



Preparar los hosts (Ubuntu o Debian)

Cómo cambia la configuración de todo el host durante la instalación

En sistemas con configuración básica, StorageGRID realiza algunos cambios en todo el host `sysctl` configuración.

Se realizan los siguientes cambios:

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
```

```
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Instale Linux

Debe instalar StorageGRID en todos los hosts de grid de Ubuntu o Debian. Para ver una lista de las versiones admitidas, use la herramienta de matriz de interoperabilidad de NetApp.

Asegúrese de que su sistema operativo esté actualizado al kernel 4,15 de Linux o superior.

Pasos

1. Instalar Linux en todos los hosts de grid físicos o virtuales de acuerdo con las instrucciones del mayorista o del procedimiento estándar.

> No instale ningún entorno de escritorio gráfico. Al instalar Ubuntu, debe seleccionar **utilidades estándar del sistema**. Se recomienda seleccionar **OpenSSH Server** para habilitar el acceso ssh a sus hosts Ubuntu. Todas las demás opciones pueden permanecer desactivadas.

2. Asegúrese de que todos los hosts tengan acceso a los repositorios de paquetes de Ubuntu o Debian.
3. Si el intercambio está activado:
   a. Ejecute el siguiente comando: `$ sudo swapoff --all`
   b. Eliminar todas las entradas de intercambio de `/etc/fstab` para mantener los ajustes.

> Si no se deshabilita por completo el intercambio, el rendimiento se puede reducir considerablemente.

Comprender la instalación del perfil de AppArmor

Si trabaja en un entorno Ubuntu autoimplementado y utiliza el sistema de control de acceso obligatorio AppArmor, los perfiles AppArmor asociados a los paquetes que instala en el sistema base pueden estar bloqueados por los paquetes correspondientes instalados con StorageGRID.

De forma predeterminada, los perfiles AppArmor se instalan para los paquetes que instale en el sistema operativo base. Cuando ejecuta estos paquetes desde el contenedor del sistema StorageGRID, los perfiles AppArmor están bloqueados. Los paquetes base DHCP, MySQL, NTP y tcdump entran en conflicto con AppArmor y otros paquetes base también pueden entrar en conflicto.

Tiene dos opciones para gestionar los perfiles de AppArmor:

- Deshabilite perfiles individuales para los paquetes instalados en el sistema base que se solapen con los paquetes del contenedor del sistema StorageGRID. Al deshabilitar perfiles individuales, aparece una entrada en los archivos de registro de StorageGRID que indica que AppArmor está activado.

  Utilice los siguientes comandos:

  ```
  sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
  ```

  Ejemplo:

  ```
  sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/bin.ping
  ```

- Desactive por completo AppArmor. Para Ubuntu 9.10 o posterior, siga las instrucciones de la comunidad en línea Ubuntu: "Desactive AppArmor". Es posible que deshabilitar AppArmor por completo no sea posible en las versiones más recientes de Ubuntu.

Después de desactivar AppArmor, no aparecerá ninguna entrada que indique que AppArmor está habilitado en los archivos de registro de StorageGRID.

Configurar la red host (Ubuntu o Debian)

Una vez finalizada la instalación de Linux en los hosts, puede que deba realizar alguna configuración adicional para preparar un conjunto de interfaces de red en cada host adecuado para la asignación a los nodos StorageGRID que se pondrá en marcha más adelante.

Antes de empezar

- Ha revisado el "Directrices para redes de StorageGRID".
- Ha revisado la información sobre "requisitos de migración de contenedores de nodos".
- Si utiliza hosts virtuales, ha leído el Consideraciones y recomendaciones para la clonación de direcciones MAC antes de configurar la red del host.

> Si utiliza equipos virtuales como hosts, debe seleccionar VMXNET 3 como adaptador de red virtual. El adaptador de red VMware E1000 ha provocado problemas de conectividad con contenedores StorageGRID puestos en marcha en ciertas distribuciones de Linux.

Acerca de esta tarea

Los nodos de grid deben poder acceder a la red de grid y, opcionalmente, a las redes de administrador y cliente. Para proporcionar este acceso, debe crear asignaciones que asocien la interfaz física del host con las interfaces virtuales para cada nodo de grid. Cuando se crean interfaces de host, se utilizan nombres descriptivos para facilitar la puesta en marcha en todos los hosts y para habilitar la migración.

La misma interfaz se puede compartir entre el host y uno o varios nodos. Por ejemplo, podría usar la misma interfaz para el acceso al host y el acceso a la red de administrador de nodo para facilitar el mantenimiento del host y del nodo. Aunque el host y los nodos individuales pueden compartir la misma interfaz, todos deben tener direcciones IP diferentes. Las direcciones IP no se pueden compartir entre nodos ni entre el host y cualquier nodo.

Puede utilizar la misma interfaz de red de host para proporcionar la interfaz de red de cuadrícula para todos los nodos StorageGRID del host; puede utilizar una interfaz de red de host diferente para cada nodo; o puede hacer algo entre ambos. Sin embargo, normalmente no debería proporcionar la misma interfaz de red host que las interfaces de red de Grid y Admin para un solo nodo, o bien como la interfaz de red de cuadrícula para un nodo y la interfaz de red de cliente para otro.

Puede completar esta tarea de muchas maneras. Por ejemplo, si los hosts son máquinas virtuales y va a implementar uno o dos nodos de StorageGRID para cada host, puede crear el número correcto de interfaces de red en el hipervisor y usar una asignación de 1 a 1. Si va a poner en marcha varios nodos en hosts con configuración básica para su uso en producción, puede aprovechar el soporte de la pila de red de Linux para VLAN y LACP para la tolerancia a fallos y el uso compartido de ancho de banda. En las siguientes secciones, se ofrecen enfoques detallados de estos dos ejemplos. No es necesario utilizar ninguno de estos ejemplos; puede utilizar cualquier enfoque que satisfaga sus necesidades.

No utilice dispositivos de enlace o puente directamente como interfaz de red de contenedor. De esta manera, se podría evitar el inicio del nodo causado por un problema de kernel con el uso de MACVLAN con dispositivos de enlace y puente en el espacio de nombres del contenedor. En su lugar, utilice un dispositivo que no sea de vínculo, como un par VLAN o Ethernet virtual (veth). Especifique este dispositivo como la interfaz de red en el archivo de configuración del nodo.

Consideraciones y recomendaciones para la clonación de direcciones MAC

La clonación de direcciones MAC hace que el contenedor utilice la dirección MAC del host y el host utilice la dirección MAC de una dirección que especifique o una generada aleatoriamente. Debe utilizar la clonación de direcciones MAC para evitar el uso de configuraciones de red en modo promiscuo.

Activación de la clonado de MAC

En algunos entornos, la seguridad se puede mejorar mediante el clonado de direcciones MAC porque permite utilizar un NIC virtual dedicado para la red de administración, la red de cuadrícula y la red de cliente. Si el contenedor utiliza la dirección MAC de la NIC dedicada en el host, podrá evitar el uso de configuraciones de red en modo promiscuo.

La clonación de direcciones MAC está pensada para utilizarse con instalaciones de servidores virtuales y puede que no funcione correctamente con todas las configuraciones de dispositivos físicos.

Si no se puede iniciar un nodo debido a que una interfaz objetivo de clonado MAC está ocupada, es posible que deba establecer el enlace a "inactivo" antes de iniciar el nodo. Además, es posible que el entorno virtual pueda evitar la clonación de MAC en una interfaz de red mientras el enlace está activo. Si un nodo no puede configurar la dirección MAC e iniciar debido a una interfaz que está ocupada, configurar el enlace a "inactivo" antes de iniciar el nodo puede solucionar el problema.

La clonación de direcciones MAC está deshabilitada de forma predeterminada y debe establecerse mediante claves de configuración de nodos. Debe habilitarla cuando instala StorageGRID.

Hay una clave para cada red:

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

Si se establece la clave en "verdadero", el contenedor utilizará la dirección MAC de la NIC del host. Además, el host utilizará la dirección MAC de la red de contenedores especificada. De forma predeterminada, la dirección del contenedor es una dirección generada aleatoriamente, pero si ha definido una utilizando la `_NETWORK_MAC` la clave de configuración del nodo, en su lugar, se usa esa dirección. El host y el contenedor siempre tendrán direcciones MAC diferentes.

Al habilitar la clonación MAC en un host virtual sin habilitar también el modo promiscuo en el hipervisor, es posible que la red de host Linux utilice la interfaz del host para dejar de funcionar.

Casos de uso de clonación DE MAC

Existen dos casos de uso a tener en cuenta con la clonación de MAC:

- Clonado DE MAC no activado: Cuando el `_CLONE_MAC` La clave del archivo de configuración del nodo no está establecida o se establece en "false", el host utilizará el NIC MAC host y el contenedor tendrá un MAC generado por StorageGRID, a menos que se especifique un MAC en el `_NETWORK_MAC` clave. Si se establece una dirección en la `_NETWORK_MAC` clave, el contenedor tendrá la dirección especificada en `_NETWORK_MAC` clave. Esta configuración de claves requiere el uso del modo promiscuo.
- Clonado DE MAC activado: Cuando la `_CLONE_MAC` La clave del archivo de configuración del nodo se establece en "true", el contenedor utiliza el NIC MAC del host y el host utiliza un MAC generado por StorageGRID, a menos que se especifique un MAC en el `_NETWORK_MAC` clave. Si se establece una dirección en la `_NETWORK_MAC` key, el host utiliza la dirección especificada en lugar de la generada. En esta configuración de claves, no debe utilizar el modo promiscuo.

> Si no desea utilizar la clonación de direcciones MAC y prefiere permitir que todas las interfaces reciban y transmitan datos para direcciones MAC distintas de las asignadas por el hipervisor, Asegúrese de que las propiedades de seguridad en los niveles de conmutador virtual y grupo de puertos estén establecidas en **Aceptar** para el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas. Los valores establecidos en el conmutador virtual pueden ser anulados por los valores en el nivel de grupo de puertos, por lo que asegúrese de que la configuración sea la misma en ambos lugares.

Para habilitar la clonación de MAC, consulte "instrucciones para crear archivos de configuración de nodo".

Ejemplo de clonación EN MAC

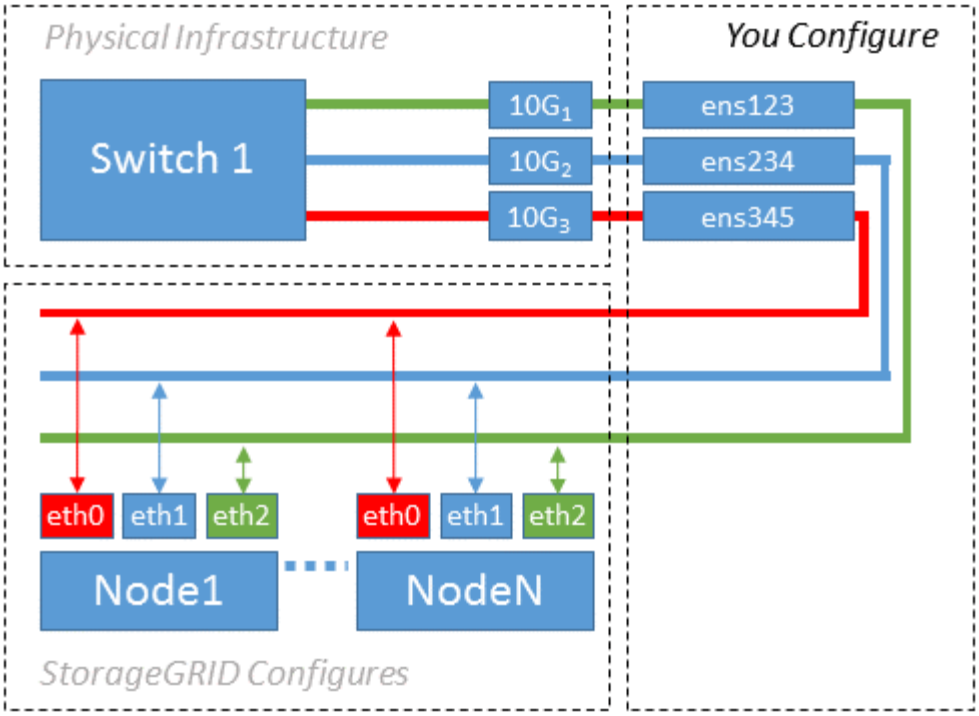
Ejemplo de clonación MAC habilitada con un host que tiene la dirección MAC 11:22:33:44:55:66 para la interfaz ens256 y las siguientes claves en el archivo de configuración del nodo:

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Resultado: El MAC host para ens256 es b2:9c:02:c2:27:10 y el MAC de la red de administración es 11:22:33:44:55:66

Ejemplo 1: Asignación de 1 a 1 a NIC físicas o virtuales

El ejemplo 1 describe una asignación sencilla de interfaz física que requiere poca o ninguna configuración en el lado del host.



El sistema operativo Linux crea las interfaces ensXYZ automáticamente durante la instalación o el arranque, o cuando las interfaces se añaden en caliente. No se necesita ninguna configuración que no sea asegurarse de que las interfaces estén configuradas para que se encuentren en funcionamiento automáticamente después del arranque. Debe determinar qué red ensXYZ corresponde a qué red StorageGRID (Grid, Admin o Cliente) para poder proporcionar las asignaciones correctas más adelante en el proceso de configuración.

Tenga en cuenta que en la figura se muestran varios nodos StorageGRID; sin embargo, normalmente usaría esta configuración para máquinas virtuales de un solo nodo.

Si el switch 1 es un switch físico, debe configurar los puertos conectados a las interfaces de 10 G_1 a 10 G_3 para el modo de acceso y colocarlos en las VLAN que corresponda.

Ejemplo 2: Enlace LACP que transporta VLAN

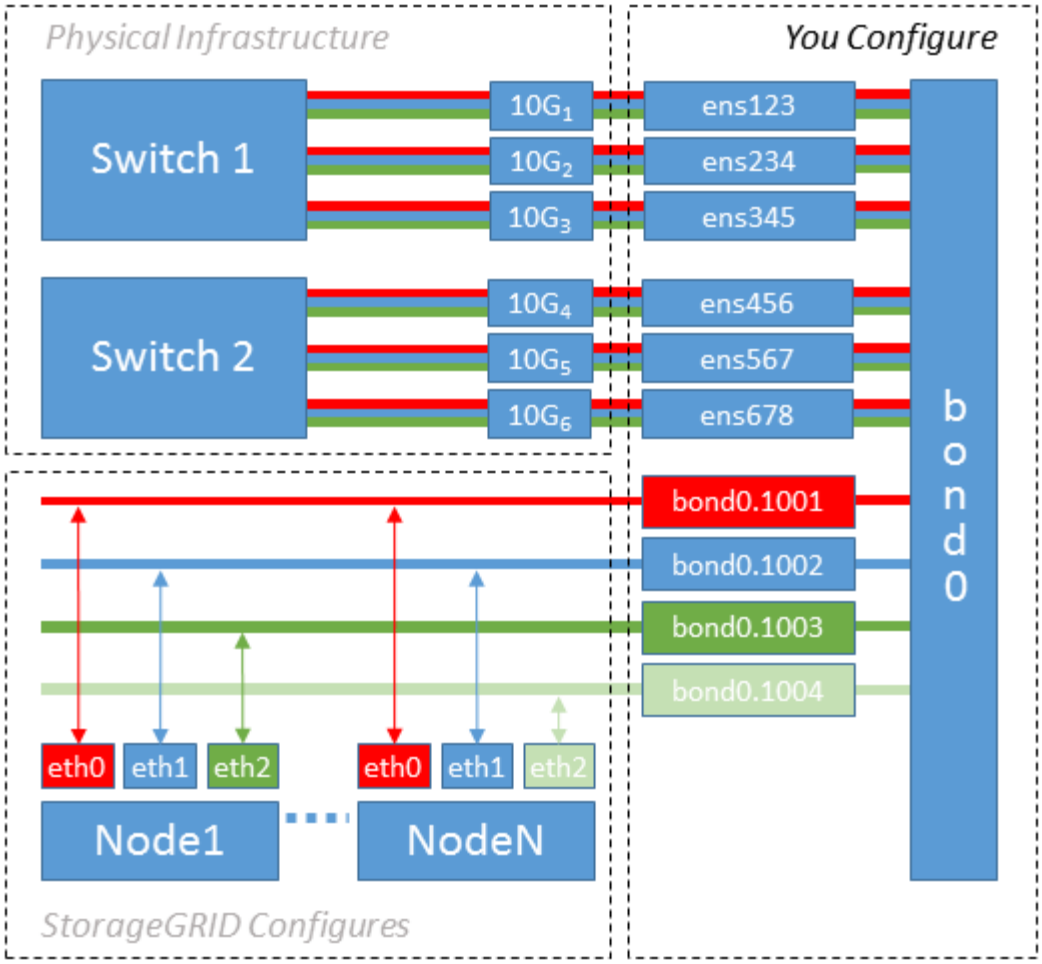
En el ejemplo 2 se supone que está familiarizado con las interfaces de red de enlace y con la creación de interfaces VLAN en la distribución Linux que está utilizando.

Acerca de esta tarea

El ejemplo 2 describe un esquema genérico, flexible y basado en VLAN que facilita el uso compartido de todo el ancho de banda de red disponible en todos los nodos de un único host. Este ejemplo se aplica especialmente a hosts con configuración básica.

Para entender este ejemplo, supongamos que tiene tres subredes distintas para las redes Grid, Admin y Client en cada centro de datos. Las subredes se encuentran en VLAN independientes (1001, 1002 y 1003) y se presentan al host en un puerto de tronco enlazado con LACP (bond0). Usted configuraría tres interfaces VLAN en el enlace: Bond0.1001, bond0.1002, y bond0.1003.

Si requiere VLAN y subredes independientes para redes de nodos en el mismo host, puede agregar interfaces VLAN en el vínculo y asignarlas al host (mostrado como bond0.1004 en la ilustración).



Pasos

1. Agregue todas las interfaces de red físicas que se utilizarán para la conectividad de red de StorageGRID en un único vínculo de LACP.

   Utilice el mismo nombre para el enlace en cada host, por ejemplo, bond0.

2. Cree interfaces VLAN que utilicen este vínculo como su «dispositivo físico» asociado mediante la convención de nomenclatura de la interfaz VLAN estándar `physdev-name.VLAN ID`.

   Tenga en cuenta que los pasos 1 y 2 requieren una configuración adecuada en los conmutadores EDGE que terminan los otros extremos de los enlaces de red. Los puertos del switch perimetral también deben agregarse a un canal de puerto LACP, donde se debe configurar como tronco y donde se puede pasar todas las VLAN requeridas.

   Se proporcionan archivos de configuración de interfaz de ejemplo para este esquema de configuración de red por host.

Información relacionada

"Ejemplo /etc/network/interfaces"

Configurar el almacenamiento del host

Se deben asignar los volúmenes de almacenamiento en bloque a cada host.

Antes de empezar

Ha revisado los siguientes temas, que le proporcionan información necesaria para realizar esta tarea:

"Los requisitos de almacenamiento y rendimiento"

"Requisitos de migración de contenedores de nodos"

Acerca de esta tarea

Cuando asigne volúmenes de almacenamiento de bloques (LUN) a hosts, utilice las tablas en «Requisitos de almacenamiento» para determinar lo siguiente:

- Número de volúmenes necesarios para cada host (según la cantidad y los tipos de nodos que se pondrán en marcha en ese host)
- Categoría de almacenamiento para cada volumen (es decir, datos del sistema o datos de objetos)
- El tamaño de cada volumen

Utilizará esta información, así como el nombre persistente asignado por Linux a cada volumen físico cuando implemente nodos StorageGRID en el host.

No es necesario crear particiones, formatear o montar ninguno de estos volúmenes; solo debe asegurarse de que sean visibles para los hosts.

Solo se requiere un LUN de datos de objetos para los nodos de almacenamiento solo de metadatos.

Evite utilizar archivos especiales de dispositivos raw (`/dev/sdb`, por ejemplo) al redactar la lista de nombres de volumen. Estos archivos pueden cambiar entre reinicios del host, lo que impacta en el funcionamiento correcto del sistema. Si utiliza LUN iSCSI y rutas múltiples de asignación de dispositivos, considere el uso de alias multivía en la `/dev/mapper` directorio, especialmente si la topología SAN incluye rutas de red redundantes al almacenamiento compartido. De forma alternativa, puede utilizar los enlaces programables creados por el sistema en `/dev/disk/by-path/` para los nombres de dispositivos persistentes.

Por ejemplo:

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Los resultados serán distintos para cada instalación.

Asigne nombres descriptivos a cada uno de estos volúmenes de almacenamiento en bloques para simplificar la instalación inicial de StorageGRID y los procedimientos de mantenimiento futuros. Si se utiliza el controlador multivía del asignador de dispositivos para acceder de forma redundante a volúmenes de almacenamiento compartido, es posible utilizar el `alias` en su `/etc/multipath.conf` archivo.

Por ejemplo:

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

Esto hará que los alias aparezcan como dispositivos de bloque en el `/dev/mapper` directorio en el host, lo que permite especificar un nombre descriptivo y de fácil validación cada vez que una operación de configuración o mantenimiento requiere especificar un volumen de almacenamiento de bloques.

> Si está configurando almacenamiento compartido para admitir la migración de nodos de StorageGRID y el uso de rutas múltiples de asignación de dispositivos, puede crear e instalar un común `/etc/multipath.conf` en todos los hosts ubicados conjuntamente. Solo hay que asegurarse de usar un volumen de almacenamiento de Docker diferente en cada host. El uso de alias e incluir el nombre de host de destino en el alias de cada LUN de volumen de almacenamiento de Docker facilitará su recordatorio y le recomienda que lo haga.

Información relacionada

"Los requisitos de almacenamiento y rendimiento"

"Requisitos de migración de contenedores de nodos"

Configure el volumen de almacenamiento de Docker

Antes de instalar Docker, es posible que tenga que formatear el volumen de almacenamiento de Docker y montarlo en `/var/lib/docker`.

Acerca de esta tarea

Puede omitir estos pasos si tiene pensado utilizar almacenamiento local para el volumen de almacenamiento de Docker y tener suficiente espacio disponible en la partición de host que contiene `/var/lib`.

Pasos

1. Cree un sistema de archivos en el volumen de almacenamiento de Docker:

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Monte el volumen de almacenamiento de Docker:

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

3. Añada una entrada para docker-Storage-volume-device a /etc/fstab.

   Este paso garantiza que el volumen de almacenamiento se vuelva a montar automáticamente después de reiniciar el host.

Instale Docker

El sistema StorageGRID se ejecuta en Linux como una colección de contenedores de Docker. Antes de instalar StorageGRID, debe instalar Docker.

Pasos

1. Siga las instrucciones para su distribución de Linux para instalar Docker.

   > Si Docker no se incluye con su distribución de Linux, puede descargarla en el sitio web de Docker.

2. Para asegurarse de que Docker se ha activado y se ha iniciado, ejecute los dos comandos siguientes:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Confirme que ha instalado la versión esperada de Docker; para ello, introduzca lo siguiente:

```
sudo docker version
```

Las versiones cliente y servidor deben ser 1.11.0 o posterior.

Información relacionada

"Configurar el almacenamiento del host"

Instale los servicios de host StorageGRID

Se utiliza el paquete StorageGRID DEB PARA instalar los servicios de host de StorageGRID.

Acerca de esta tarea

Estas instrucciones describen cómo instalar los servicios host desde los paquetes DEB. Como alternativa, puede usar los metadatos del repositorio de APT incluidos en el archivo de instalación para instalar los paquetes DEB de forma remota. Consulte las instrucciones del repositorio de APT para su sistema operativo Linux.

Pasos

1. Copie los paquetes StorageGRID DEB en cada host o déjelos disponibles en el almacenamiento compartido.

   Por ejemplo, colóquelos en el `/tmp` directory, para poder utilizar el comando de ejemplo en el paso siguiente.

2. Inicie sesión en cada host como raíz o utilice una cuenta con permiso sudo y ejecute los siguientes comandos.

   Debe instalar el `images` primero el paquete, y el `service` segundo paquete. Si colocó los paquetes en un directorio distinto de `/tmp`, modifique el comando para reflejar la ruta de acceso utilizada.

```
sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
```

> Python 2.7 ya debe estar instalado antes de poder instalar los paquetes StorageGRID. La `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` el comando fallará hasta que lo haya hecho.

Automatizar la instalación (Ubuntu o Debian)

Puede automatizar la instalación del servicio de host de StorageGRID y la configuración de los nodos de grid.

Acerca de esta tarea

La automatización de la puesta en marcha puede ser útil en cualquiera de los siguientes casos:

- Ya utiliza un marco de orquestación estándar, como Ansible, Puppet o Chef, para poner en marcha y configurar hosts físicos o virtuales.
- Tiene pensado implementar varias instancias de StorageGRID.
- Está poniendo en marcha una instancia de StorageGRID grande y compleja.

El servicio de host StorageGRID se instala mediante un paquete y está impulsado por archivos de configuración que pueden crearse de forma interactiva durante una instalación manual, o bien se pueden preparar con antelación (o mediante programación) para permitir la instalación automatizada mediante marcos de orquestación estándar. StorageGRID proporciona scripts Python opcionales para automatizar la configuración de dispositivos StorageGRID y todo el sistema StorageGRID (el «grid»). Puede utilizar estos scripts directamente o puede inspeccionarlos para obtener información sobre cómo utilizar la API REST de instalación de StorageGRID en las herramientas de configuración e implementación de grid que desarrolla usted mismo.

Automatizar la instalación y configuración del servicio de host de StorageGRID

Puede automatizar la instalación del servicio de host de StorageGRID mediante marcos de orquestación estándar como Ansible, Puppet, Chef, Fabric o SaltStack.

El servicio de host StorageGRID está empaquetado en UN DEB y está controlado por archivos de configuración que se pueden preparar con antelación (o mediante programación) para permitir la instalación automatizada. Si ya utiliza un marco de orquestación estándar para instalar y configurar Ubuntu o Debian, agregar StorageGRID a sus libros de estrategia o recetas debe ser sencillo.

Puede automatizar estas tareas:

1. Instalando Linux
2. Configurando Linux
3. Configurar interfaces de red de host para que cumplan los requisitos de StorageGRID
4. Configurar el almacenamiento del host para cumplir con los requisitos de StorageGRID
5. Instalación de Docker
6. Instalar el servicio host StorageGRID
7. Creación de archivos de configuración del nodo StorageGRID en `/etc/storagegrid/nodes`
8. Validar los archivos de configuración del nodo StorageGRID
9. Iniciar el servicio de host StorageGRID

Ejemplo de rol y libro de estrategia de Ansible

El rol y el libro de estrategia de Ansible de ejemplo se proporcionan con el archivo de instalación en `/extras` carpeta. El libro de estrategia de Ansible muestra cómo `storagegrid` El rol prepara los hosts e instala StorageGRID en los servidores de destino. Puede personalizar el rol o el libro de estrategia según sea necesario.

Automatice la configuración de StorageGRID

Después de implementar los nodos de grid, puede automatizar la configuración del sistema StorageGRID.

Antes de empezar

- Conoce la ubicación de los siguientes archivos del archivo de instalación.

Nombre de archivo	Descripción
configure-storagegrid.py	Script Python utilizado para automatizar la configuración
configure-storagegrid.sample.json	Archivo de configuración de ejemplo para utilizar con el script
configure-storagegrid.blank.json	Archivo de configuración en blanco para utilizar con el script

- Ha creado un `configure-storagegrid.json` archivo de configuración. Para crear este archivo, puede modificar el archivo de configuración de ejemplo (`configure-storagegrid.sample.json`) o el archivo de configuración en blanco (`configure-storagegrid.blank.json`).

Acerca de esta tarea

Puede utilizar el `configure-storagegrid.py` El guión de Python y el `configure-storagegrid.json` Archivo de configuración para automatizar la configuración del sistema StorageGRID.

También puede configurar el sistema mediante Grid Manager o la API de instalación.

Pasos

1. Inicie sesión en el equipo Linux que está utilizando para ejecutar el script Python.
2. Cambie al directorio en el que ha extraído el archivo de instalación.

   Por ejemplo:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   donde `platform` es `debs`, `rpms`, o. `vsphere`.

3. Ejecute el script Python y utilice el archivo de configuración que ha creado.

   Por ejemplo:

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

Resultado

Un paquete de recuperación `.zip` el archivo se genera durante el proceso de configuración y se descarga en el directorio en el que se ejecuta el proceso de instalación y configuración. Debe realizar una copia de seguridad del archivo de paquete de recuperación para poder recuperar el sistema StorageGRID si falla uno o más nodos de grid. Por ejemplo, cópielo en una ubicación de red segura y en una ubicación de almacenamiento en nube segura.

El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

Si especificó que se deben generar contraseñas aleatorias, abra el `Passwords.txt` File y busque las contraseñas que se necesitan para acceder al sistema StorageGRID.

```
#####################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip           #####
#####   Safeguard this file as it will be needed in case of a     #####
#####                 StorageGRID node recovery.                  #####
#####################################################################
```

El sistema StorageGRID se instala y configura cuando se muestra un mensaje de confirmación.

```
StorageGRID has been configured and installed.
```

Información relacionada

"Información general de la instalación de la API de REST"

Implemente nodos de grid virtual (Ubuntu o Debian)

Cree archivos de configuración de nodos para implementaciones de Ubuntu o Debian

Los archivos de configuración de los nodos son archivos de texto pequeños que proporcionan la información que el servicio de host StorageGRID necesita para iniciar un nodo y conectarlo a la red adecuada y bloquear recursos de almacenamiento. Los archivos de configuración de nodos se usan para los nodos virtuales y no se usan para los nodos del dispositivo.

Ubicación de los archivos de configuración del nodo

Coloque el archivo de configuración de cada nodo StorageGRID en el `/etc/storagegrid/nodes` directorio en el host donde se ejecutará el nodo. Por ejemplo, si planea ejecutar un nodo de administración, un nodo de puerta de enlace y un nodo de almacenamiento en Hosta, debe colocar tres archivos de configuración de nodo en `/etc/storagegrid/nodes` En Hosta.

Puede crear los archivos de configuración directamente en cada host mediante un editor de texto, como vim o nano, o bien puede crearlos en otro lugar y moverlos a cada host.

Nomenclatura de los archivos de configuración de nodos

Los nombres de los archivos de configuración son significativos. El formato es `node-name.conf`, donde `node-name` es un nombre que asigna al nodo. Este nombre aparece en el instalador de StorageGRID y se utiliza para operaciones de mantenimiento de nodos, como la migración de nodos.

Los nombres de los nodos deben seguir estas reglas:

- Debe ser único
- Debe comenzar por una letra

- Puede contener los caracteres De La A a la Z y de la a a la Z.
- Puede contener los números del 0 al 9
- Puede contener uno o varios guiones (-)
- No debe tener más de 32 caracteres, sin incluir el `.conf` extensión

Todos los archivos incluidos `/etc/storagegrid/nodes` que no sigan estas convenciones de nomenclatura no serán analizadas por el servicio de host.

Si tiene una topología de varios sitios planificada para la cuadrícula, un esquema típico de nomenclatura de nodos podría ser:

```
site-nodetype-nodenumber.conf
```

Por ejemplo, podría utilizar `dc1-adm1.conf` Para el primer nodo de administrador en el centro de datos 1, y. `dc2-sn3.conf` Para el tercer nodo de almacenamiento en el centro de datos 2. Sin embargo, puede utilizar cualquier esquema que desee, siempre que todos los nombres de nodo sigan las reglas de nomenclatura.

Contenido de un archivo de configuración de nodo

Un archivo de configuración contiene pares clave/valor, con una clave y un valor por línea. Para cada par clave/valor, siga estas reglas:

- La clave y el valor deben estar separados por un signo igual (=) y espacios en blanco opcionales.
- Las teclas no pueden contener espacios.
- Los valores pueden contener espacios incrustados.
- Se ignora cualquier espacio en blanco inicial o final.

La siguiente tabla define los valores de todas las claves admitidas. Cada clave tiene una de las siguientes designaciones:

- **Requerido**: Requerido para cada nodo o para los tipos de nodo especificados
- **Mejor práctica**: Opcional, aunque recomendado
- **Opcional**: Opcional para todos los nodos

Claves de red de administración

IP_ADMINISTRADOR

Valor	Designación
La dirección IPv4 de red de grid del nodo de administrador principal para la cuadrícula a la que pertenece este nodo. Utilice el mismo valor especificado para GRID_NETWORK_IP para el nodo de grid con NODE_TYPE = VM_Admin_Node y ADMIN_ROLE = Primary. Si omite este parámetro, el nodo intenta detectar un nodo de administración principal con mDNS. "La forma en que los nodos de grid detectan el nodo de administrador principal" **Nota**: Este valor se ignora, y podría estar prohibido, en el nodo de administración principal.	Mejor práctica

ADMIN_NETWORK_CONFIG

Valor	Designación
DHCP, ESTÁTICO O DESHABILITADO	Opcional

ADMIN_NETWORK_ESL

Valor	Designación
Lista separada por comas de subredes en notación CIDR a la que este nodo debe comunicarse mediante la puerta de enlace de la red de administración. Ejemplo: `172.16.0.0/21,172.17.0.0/21`	Opcional

ADMIN_NETWORK_GATEWAY

Valor	Designación

La dirección IPv4 de la puerta de enlace de red de administrador local para este nodo. Debe estar en la subred definida por ADMIN_NETWORK_IP y ADMIN_NETWORK_MASK. Este valor se omite para redes configuradas con DHCP.
 	
Ejemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Obligatorio si `ADMIN_NETWORK_ESL` se especifica. Opcional de lo contrario.

IP_RED_ADMIN

Valor	Designación

La dirección IPv4 de este nodo en la red administrativa. Esta clave solo es necesaria cuando ADMIN_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
 	
Ejemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necesario cuando ADMIN_NETWORK_CONFIG = STATIC.
	
	Opcional de lo contrario.

ADMIN_NETWORK_MAC

Valor	Designación
La dirección MAC de la interfaz de red de administración en el contenedor. Este campo es opcional. Si se omite, se generará automáticamente una dirección MAC. Debe tener 6 pares de dígitos hexadecimales separados por dos puntos. Ejemplo: `b2:9c:02:c2:27:10`	Opcional

ADMIN_NETWORK_MASK

Valor	Designación

La máscara de red IPv4 para este nodo, en la red de administrador. Especifique esta clave cuando ADMIN_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
 	
Ejemplos:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necesario si se especifica ADMIN_NETWORK_IP y ADMIN_NETWORK_CONFIG = STATIC.
	
	Opcional de lo contrario.

MTU_RED_ADMIN

Valor	Designación

La unidad de transmisión máxima (MTU) para este nodo en la red de administración. No especifique si ADMIN_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se utiliza 1500.
 	
Si desea utilizar tramas gigantes, establezca el MTU en un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado.
 	
IMPORTANTE: El valor MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, pueden ocurrir problemas de rendimiento de red o pérdida de paquetes.
 	
Ejemplos:
 	
`1500`
 	
`8192`
	Opcional

ADMIN_NETWORK_TARGET

Valor	Designación

Nombre del dispositivo host que utilizará para el acceso a la red de administración mediante el nodo StorageGRID. Solo se admiten nombres de interfaces de red. Normalmente, se utiliza un nombre de interfaz diferente al especificado para GRID_NETWORK_TARGET o CLIENT_NETWORK_TARGET.
 	
Nota: No utilice dispositivos de enlace o puente como objetivo de red. Configure una VLAN (u otra interfaz virtual) en la parte superior del dispositivo de enlace o utilice un puente y un par Ethernet virtual (veth).
 	
Mejor práctica:especifique un valor aunque este nodo no tenga inicialmente una dirección IP de red de administración. Después, puede añadir una dirección IP de red de administrador más adelante, sin tener que volver a configurar el nodo en el host.
 	
Ejemplos:
 	
`bond0.1002`
 	
`ens256`
	Mejor práctica

ADMIN_NETWORK_TARGET_TYPE

Valor	Designación

Interfaz (este es el único valor admitido.)	Opcional

ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Designación
Verdadero o Falso Establezca la clave en "TRUE" para que el contenedor StorageGRID use la dirección MAC de la interfaz de destino del host en la red de administración. **Mejor práctica:** en redes donde se requiera el modo promiscuo, utilice la clave ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC en su lugar. Para obtener más información sobre la clonación de MAC: • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Red Hat Enterprise Linux)" • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)"	Mejor práctica

ADMIN_ROLE

Valor	Designación
Primario o no primario Esta clave solo es necesaria cuando NODE_TYPE = VM_ADMIN_Node; no la especifique para otros tipos de nodos.	Necesario cuando NODE_TYPE = VM_ADMIN_Node Opcional de lo contrario.

Bloquear las teclas del dispositivo

BLOCK_DEVICE_AUDIT_LOGS

Valor	Designación

La ruta y el nombre del archivo especial del dispositivo de bloque que este nodo utilizará para el almacenamiento persistente de los registros de auditoría.
 	
Ejemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-audit-logs`
	Necesario para nodos con NODE_TYPE = VM_ADMIN_Node. No lo especifique para otros tipos de nodo.

BLOQUE_DISPOSITIVO_RANGEDB_NNNN

Valor	Designación

Ruta y nombre del archivo especial del dispositivo de bloque que este nodo utilizará para el almacenamiento de objetos persistente. Esta clave solo es necesaria para los nodos con NODE_TYPE = VM_Storage_Node; no la especifique para otros tipos de nodos.
 	
Sólo SE requiere BLOCK_DEVICE_RANGEDB_000; el resto es opcional. El dispositivo de bloque especificado para BLOCK_DEVICE_RANGEDB_000 debe tener al menos 4 TB; los demás pueden ser más pequeños.
 	
No deje espacios vacíos. Si especifica BLOCK_DEVICE_RANGEDB_005, también debe especificar BLOCK_DEVICE_RANGEDB_004.
 	
Nota: Para la compatibilidad con las implementaciones existentes, las claves de dos dígitos son compatibles con los nodos actualizados.
 	
Ejemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-rangedb-000`
	Obligatorio:
	
	BLOQUE_DISPOSITIVO_RANGEDB_000
	
	Opcional:
	
	BLOQUE_DISPOSITIVO_RANGEDB_001
	
	BLOQUE_DISPOSITIVO_RANGEDB_002
	
	BLOQUE_DISPOSITIVO_RANGEDB_003
	
	BLOQUE_DISPOSITIVO_RANGEDB_004
	
	BLOQUE_DISPOSITIVO_RANGEDB_005
	
	BLOQUE_DISPOSITIVO_RANGEDB_006
	
	BLOQUE_DISPOSITIVO_RANGEDB_007
	
	BLOQUE_DISPOSITIVO_RANGEDB_008
	
	BLOQUE_DISPOSITIVO_RANGEDB_009
	
	BLOQUE_DISPOSITIVO_RANGEDB_010
	
	BLOQUE_DISPOSITIVO_RANGEDB_011
	
	BLOQUE_DISPOSITIVO_RANGEDB_012
	
	BLOQUE_DISPOSITIVO_RANGEDB_013
	
	BLOQUE_DISPOSITIVO_RANGEDB_014
	
	BLOQUE_DISPOSITIVO_RANGEDB_015

BLOCK_DEVICE_TABLES

Valor	Designación

Ruta y nombre del archivo especial del dispositivo de bloque que este nodo utilizará para el almacenamiento persistente de tablas de bases de datos. Esta clave solo es necesaria para los nodos con NODE_TYPE = VM_ADMIN_Node; no la especifique para otros tipos de nodos.
 	
Ejemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-adm1-tables`
	Obligatorio

BLOCK_DEVICE_VAR_LOCAL

Valor	Designación

Ruta de acceso y nombre del archivo especial del dispositivo de bloque que este nodo utilizará para su `/var/local` almacenamiento persistente.
 	
Ejemplos:
 	
`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
 	
`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
 	
`/dev/mapper/sgws-sn1-var-local`
	Obligatorio

Claves de red cliente

CLIENT_NETWORK_CONFIG

Valor	Designación
DHCP, ESTÁTICO O DESHABILITADO	Opcional

PUERTA_DE_ENLACE_RED_CLIENTE

Valor	Designación

Dirección IPv4 de la puerta de enlace de red de cliente local para este nodo, que debe estar en la subred definida por CLIENT_NETWORK_IP y CLIENT_NETWORK_MASK. Este valor se omite para redes configuradas con DHCP.
 	
Ejemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Opcional

IP_RED_CLIENTE

Valor	Designación

La dirección IPv4 de este nodo en la red cliente.
 	
Esta clave solo es necesaria cuando CLIENT_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
 	
Ejemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necesario cuando CLIENT_NETWORK_CONFIG = ESTÁTICO
	
	Opcional de lo contrario.

MAC_RED_CLIENTE

Valor	Designación
La dirección MAC de la interfaz de red de cliente en el contenedor. Este campo es opcional. Si se omite, se generará automáticamente una dirección MAC. Debe tener 6 pares de dígitos hexadecimales separados por dos puntos. Ejemplo: `b2:9c:02:c2:27:20`	Opcional

MÁSCARA_RED_CLIENTE

Valor	Designación

La máscara de red IPv4 para este nodo en la red de cliente.
 	
Especifique esta clave cuando CLIENT_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
 	
Ejemplos:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necesario si se especifica CLIENT_NETWORK_ip y CLIENT_NETWORK_CONFIG = ESTÁTICO
	
	Opcional de lo contrario.

MTU_RED_CLIENTE

Valor	Designación

La unidad de transmisión máxima (MTU) para este nodo en la red cliente. No especifique si CLIENT_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se utiliza 1500.
 	
Si desea utilizar tramas gigantes, establezca el MTU en un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado.
 	
IMPORTANTE: El valor MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, pueden ocurrir problemas de rendimiento de red o pérdida de paquetes.
 	
Ejemplos:
 	
`1500`
 	
`8192`
	Opcional

DESTINO_RED_CLIENTE

Valor	Designación

Nombre del dispositivo host que utilizará para el acceso a la red de cliente mediante el nodo StorageGRID. Solo se admiten nombres de interfaces de red. Normalmente, se utiliza un nombre de interfaz diferente al especificado para GRID_NETWORK_TARGET o ADMIN_NETWORK_TARGET.
 	
Nota: No utilice dispositivos de enlace o puente como objetivo de red. Configure una VLAN (u otra interfaz virtual) en la parte superior del dispositivo de enlace o utilice un puente y un par Ethernet virtual (veth).
 	
Mejor práctica: especifique un valor aunque este nodo no tenga inicialmente una dirección IP de red de cliente. Después puede añadir una dirección IP de red de cliente más tarde, sin tener que volver a configurar el nodo en el host.
 	
Ejemplos:
 	
`bond0.1003`
 	
`ens423`
	Mejor práctica

CLIENT_NETWORK_TARGET_TYPE

Valor	Designación
Interfaz (solo se admite este valor.)	Opcional

CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Designación
Verdadero o Falso Establezca la clave en "true" para hacer que el contenedor StorageGRID utilice la dirección MAC de la interfaz de destino del host en la red cliente. **Mejor práctica:** en redes donde se requiera el modo promiscuo, utilice la clave CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC en su lugar. Para obtener más información sobre la clonación de MAC: • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Red Hat Enterprise Linux)" • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)"	Mejor práctica

Claves de red de cuadrícula

GRID_NETWORK_CONFIG

Valor	Designación
ESTÁTICO o DHCP El valor por defecto es ESTÁTICO si no se especifica.	Mejor práctica

PUERTA_DE_ENLACE_RED_GRID

Valor	Designación
Dirección IPv4 de la puerta de enlace de red local para este nodo, que debe estar en la subred definida por GRID_NETWORK_IP y GRID_NETWORK_MASK. Este valor se omite para redes configuradas con DHCP. Si la red de red es una subred única sin puerta de enlace, utilice la dirección de puerta de enlace estándar de la subred (X.30 Z.1) o el valor DE GRID_NETWORK_IP de este nodo; cualquiera de los dos valores simplificará las posibles futuras expansiones de red de cuadrícula.	Obligatorio

IP_RED_GRID

Valor	Designación

Dirección IPv4 de este nodo en la red de cuadrícula. Esta clave solo es necesaria cuando GRID_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
 	
Ejemplos:
 	
`1.1.1.1`
 	
`10.224.4.81`
	Necesario cuando GRID_NETWORK_CONFIG = ESTÁTICO
	
	Opcional de lo contrario.

MAC_RED_GRID

Valor	Designación

La dirección MAC de la interfaz de red de red del contenedor. Debe tener 6 pares de dígitos hexadecimales separados por dos puntos. Ejemplo: `b2:9c:02:c2:27:30`	Opcional Si se omite, se generará automáticamente una dirección MAC.

GRID_NETWORK_MASK

Valor	Designación

Máscara de red IPv4 para este nodo en la red de cuadrícula. Especifique esta clave cuando GRID_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
 	
Ejemplos:
 	
`255.255.255.0`
 	
`255.255.248.0`
	Necesario cuando se especifica GRID_NETWORK_ip y GRID_NETWORK_CONFIG = ESTÁTICO.
	
	Opcional de lo contrario.

MTU_RED_GRID

Valor	Designación

La unidad de transmisión máxima (MTU) para este nodo en la red Grid. No especifique si GRID_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se utiliza 1500.
 	
Si desea utilizar tramas gigantes, establezca el MTU en un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado.
 	
IMPORTANTE: El valor MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, pueden ocurrir problemas de rendimiento de red o pérdida de paquetes.
 	
IMPORTANTE: Para obtener el mejor rendimiento de red, todos los nodos deben configurarse con valores MTU similares en sus interfaces de red Grid. 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.
 	
Ejemplos:
 	
`1500`
 	
`8192`
	Opcional

GRID_NETWORK_TARGET

Valor	Designación

Nombre del dispositivo host que utilizará para el acceso a la red de cuadrícula mediante el nodo StorageGRID. Solo se admiten nombres de interfaces de red. Normalmente, se utiliza un nombre de interfaz diferente al especificado para ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET.
 	
Nota: No utilice dispositivos de enlace o puente como objetivo de red. Configure una VLAN (u otra interfaz virtual) en la parte superior del dispositivo de enlace o utilice un puente y un par Ethernet virtual (veth).
 	
Ejemplos:
 	
`bond0.1001`
 	
`ens192`
	Obligatorio

GRID_NETWORK_TARGET_TYPE

Valor	Designación

Interfaz (este es el único valor admitido.)	Opcional

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Designación
Verdadero o Falso Establezca el valor de la clave en "verdadero" para que el contenedor StorageGRID utilice la dirección MAC de la interfaz de destino del host en la red de red. **Mejor práctica:** en redes donde se requiera el modo promiscuo, utilice la clave GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC en su lugar. Para obtener más información sobre la clonación de MAC: • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Red Hat Enterprise Linux)" • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)"	Mejor práctica

Clave de interfaces

INTERFAZ_DESTINO_nnnn

Valor	Designación
Nombre y descripción opcional para una interfaz adicional que se desea añadir a este nodo. Puede añadir varias interfaces adicionales a cada nodo. Para *nnnn*, especifique un número único para cada entrada de INTERFAZ_DESTINO que agregue. Para el valor, especifique el nombre de la interfaz física en el host de configuración básica. A continuación, de manera opcional, añada una coma y proporcione una descripción de la interfaz, que se muestra en la página interfaces VLAN y en la página grupos de alta disponibilidad. Ejemplo: `INTERFACE_TARGET_0001=ens256, Trunk` Si añade una interfaz troncal, debe configurar una interfaz VLAN en StorageGRID. Si agrega una interfaz de acceso, puede añadir la interfaz directamente a un grupo de alta disponibilidad; no es necesario configurar una interfaz de VLAN.	Opcional

Clave RAM máxima

RAM_MÁXIMA

Valor	Designación

La cantidad máxima de RAM que se permite que este nodo consuma. Si se omite esta clave, el nodo no tiene restricciones de memoria. Al establecer este campo para un nodo de nivel de producción, especifique un valor que sea al menos 24 GB y 16 a 32 GB menor que la RAM total del sistema.
 	
Nota: El valor de la RAM afecta al espacio reservado real de metadatos de un nodo. Consulte "Descripción del espacio reservado de metadatos".
 	
El formato de este campo es *`numberunit`*, donde *`unit`* puede ser `b`, `k`, `m`, o. `g`.
 	
Ejemplos:
 	
`24g`
 	
`38654705664b`
 	
Nota: Si desea utilizar esta opción, debe activar el soporte de núcleo para grupos de memoria.
	Opcional

Clave de tipo de nodo

TIPO_NODO

Valor	Designación
Tipo de nodo: VM_Admin_Node VM_Storage_Node VM_Archive_Node Puerta de enlace_API_VM	Obligatorio

Claves de reasignación de puertos

REASIGNAR_PUERTO

Valor	Designación

Reasigna cualquier puerto que usa un nodo para las comunicaciones internas del nodo de grid o las comunicaciones externas. La reasignación de puertos es necesaria si las políticas de red de la empresa restringen uno o más puertos utilizados por StorageGRID, como se describe en "Comunicaciones internas de los nodos de grid" o. "Comunicaciones externas". **IMPORTANTE**: No reasigne los puertos que planea usar para configurar los puntos finales del equilibrador de carga. **Nota**: Si sólo SE establece PORT_REMAPP, la asignación que especifique se utiliza tanto para comunicaciones entrantes como salientes. Si TAMBIÉN se especifica PORT_REMAPP_INBOUND, PORT_REMAPP sólo se aplica a las comunicaciones salientes. El formato utilizado es: *`network type/protocol/default port used by grid node/new port`*, donde *`network type`* es grid, administrador o cliente, y. *`protocol`* es tcp o udp. Ejemplo: `PORT_REMAP = client/tcp/18082/443`	Opcional

PORT_REMAPP_INBOUND

Valor	Designación
Reasigna las comunicaciones entrantes al puerto especificado. Si especifica PORT_REMAP_INBOUND pero no especifica un valor para PORT_REMAP, las comunicaciones salientes para el puerto no cambian. **IMPORTANTE**: No reasigne los puertos que planea usar para configurar los puntos finales del equilibrador de carga. El formato utilizado es: *`network type/protocol/remapped port /default port used by grid node`*, donde *`network type`* es grid, administrador o cliente, y. *`protocol`* es tcp o udp. Ejemplo: `PORT_REMAP_INBOUND = grid/tcp/3022/22`	Opcional

La forma en que los nodos de grid detectan el nodo de administrador principal

Los nodos de grid se comunican con el nodo de administrador principal para realizar tareas de configuración y gestión. Cada nodo de grid debe conocer la dirección IP del nodo de administrador principal en la red de grid.

Para garantizar que un nodo de grid pueda acceder al nodo de administrador principal, puede realizar cualquiera de las siguientes acciones al implementar el nodo:

- Puede usar el parámetro ADMIN_IP para introducir la dirección IP del nodo administrador primario manualmente.

- Puede omitir el parámetro ADMIN_IP para que el nodo del grid detecte el valor automáticamente. La detección automática es especialmente útil cuando la red de cuadrícula utiliza DHCP para asignar la dirección IP al nodo de administración principal.

La detección automática del nodo de administración principal se realiza mediante un sistema de nombres de dominio de multidifusión (mDNS). Cuando se inicia por primera vez el nodo de administración principal, publica su dirección IP mediante mDNS. A continuación, otros nodos de la misma subred pueden consultar la dirección IP y adquirirla automáticamente. Sin embargo, debido a que el tráfico IP de multidifusión no se puede enrutar en subredes, los nodos de otras subredes no pueden adquirir directamente la dirección IP del nodo de administración principal.

Si utiliza la detección automática:

- Debe incluir la configuración ADMIN_IP para al menos un nodo de grid en las subredes a las que no está conectado directamente el nodo de administración principal. A continuación, este nodo de cuadrícula publicará la dirección IP del nodo de administración principal para otros nodos de la subred a fin de detectar con mDNS.
- Asegúrese de que la infraestructura de red admite la transferencia de tráfico IP multifundido dentro de una subred.

Archivos de configuración del nodo de ejemplo

Puede usar los archivos de configuración del nodo de ejemplo para ayudar a configurar los archivos de configuración del nodo para el sistema StorageGRID. Los ejemplos muestran archivos de configuración de nodo para todos los tipos de nodos de cuadrícula.

En la mayoría de los nodos, puede agregar información de direccionamiento de red de administrador y cliente (IP, máscara, puerta de enlace, etc.) al configurar la cuadrícula mediante Grid Manager o la API de instalación. La excepción es el nodo de administrador principal. Si desea examinar la dirección IP de red de administrador del nodo de administración principal para completar la configuración de grid (porque la red de grid no se enrutó, por ejemplo), debe configurar la conexión de red de administración para el nodo de administración principal en su archivo de configuración de nodo. Esto se muestra en el ejemplo.

En los ejemplos, el destino de red de cliente se ha configurado como práctica recomendada, aunque la red de cliente esté deshabilitada de forma predeterminada.

Ejemplo de nodo de administración primario

Ejemplo de nombre de archivo: `/etc/storagegrid/nodes/dc1-adm1.conf`

Ejemplo del contenido del archivo:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Ejemplo para Storage Node

Ejemplo de nombre de archivo: `/etc/storagegrid/nodes/dc1-sn1.conf`

Ejemplo del contenido del archivo:

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Ejemplo para nodo de archivado

Ejemplo de nombre de archivo: `/etc/storagegrid/nodes/dc1-arc1.conf`

Ejemplo del contenido del archivo:

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Ejemplo para Gateway Node

Ejemplo de nombre de archivo: `/etc/storagegrid/nodes/dc1-gw1.conf`

Ejemplo del contenido del archivo:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Ejemplo de un nodo de administrador que no es primario

Ejemplo de nombre de archivo: `/etc/storagegrid/nodes/dc1-adm2.conf`

Ejemplo del contenido del archivo:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Validar la configuración de StorageGRID

Después de crear archivos de configuración en `/etc/storagegrid/nodes` Debe validar el contenido de cada uno de los nodos StorageGRID.

Para validar el contenido de los archivos de configuración, ejecute el siguiente comando en cada host:

```
sudo storagegrid node validate all
```

Si los archivos son correctos, el resultado muestra **PASADO** para cada archivo de configuración, como se muestra en el ejemplo.

Cuando se usa solo una LUN en los nodos de solo metadatos, puede recibir un mensaje de advertencia que se puede ignorar.

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

Para una instalación automatizada, puede suprimir este resultado utilizando `-q` o. `--quiet` de la `storagegrid` (por ejemplo, `storagegrid --quiet…`). Si suprime el resultado, el comando tendrá un valor de salida que no es cero si se detectan advertencias o errores de configuración.

Si los archivos de configuración son incorrectos, los problemas se muestran como **ADVERTENCIA** y **ERROR**, como se muestra en el ejemplo. Si se encuentra algún error de configuración, debe corregirlo antes de

continuar con la instalación.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Inicie el servicio de host StorageGRID

Para iniciar los nodos de StorageGRID y asegurarse de que reinicien después del reinicio de un host, debe habilitar e iniciar el servicio de host StorageGRID.

Pasos

1. Ejecute los siguientes comandos en cada host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Ejecute el siguiente comando para asegurarse de que se sigue la implementación:

```
sudo storagegrid node status node-name
```

3. Si alguno de los nodos devuelve el estado «Sin ejecución» o «Detenido», ejecute el siguiente comando:

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

4. Si anteriormente habilitó e inició el servicio de host de StorageGRID (o si no está seguro de si el servicio se ha habilitado e iniciado), también debe ejecutar el siguiente comando:

```
sudo systemctl reload-or-restart storagegrid
```

Configurar la cuadrícula y completar la instalación (Ubuntu o Debian)

Desplácese hasta Grid Manager

El Gestor de cuadrícula se utiliza para definir toda la información necesaria para configurar el sistema StorageGRID.

Antes de empezar

El nodo de administración principal debe estar implementado y haber completado la secuencia de inicio inicial.

Pasos

1. Abra el explorador web y desplácese hasta una de las siguientes direcciones:

   `https://primary_admin_node_ip`

   `client_network_ip`

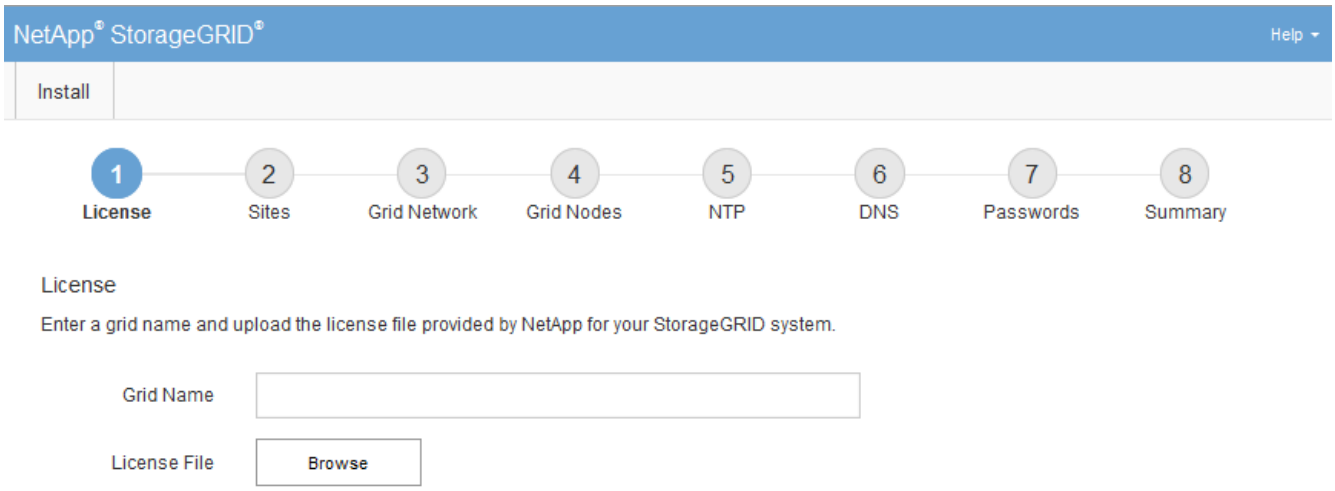
   También puede acceder a Grid Manager en el puerto 8443:

   `https://primary_admin_node_ip:8443`

   > Puede usar la dirección IP para la IP del nodo de administración principal en la red de grid o en la red de administración, según corresponda a su configuración de red.

2. Selecciona **Instalar un sistema StorageGRID**.

   Se muestra la página que se utiliza para configurar un sistema StorageGRID.



Especifique la información de licencia de StorageGRID

Debe especificar el nombre del sistema StorageGRID y cargar el archivo de licencia proporcionado por NetApp.

Pasos

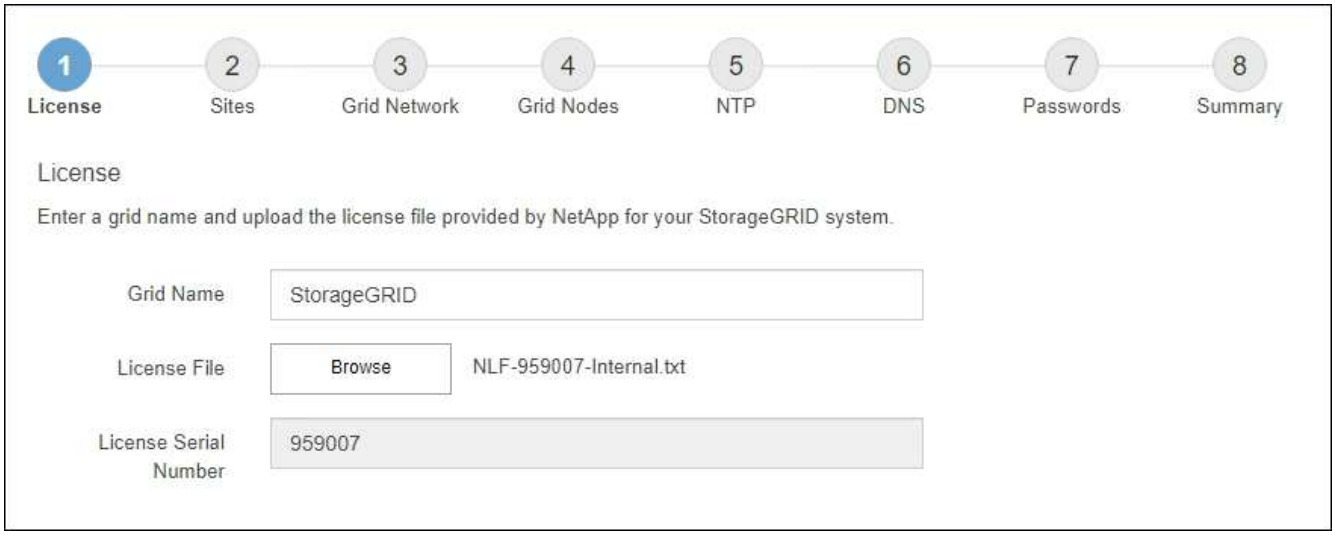
1. En la página Licencia, introduzca un nombre significativo para su sistema StorageGRID en el campo **Nombre de cuadrícula**.

   Tras la instalación, el nombre se muestra en la parte superior del menú nodos.

2. Seleccione **Examinar** y busque el archivo de licencia de NetApp (`NLF-unique-id.txt`) Y seleccione **Abrir**.

   El archivo de licencia se valida y se muestra el número de serie.

   > El archivo de instalación de StorageGRID incluye una licencia gratuita que no proporciona ningún derecho de soporte para el producto. Puede actualizar a una licencia que ofrezca soporte tras la instalación.



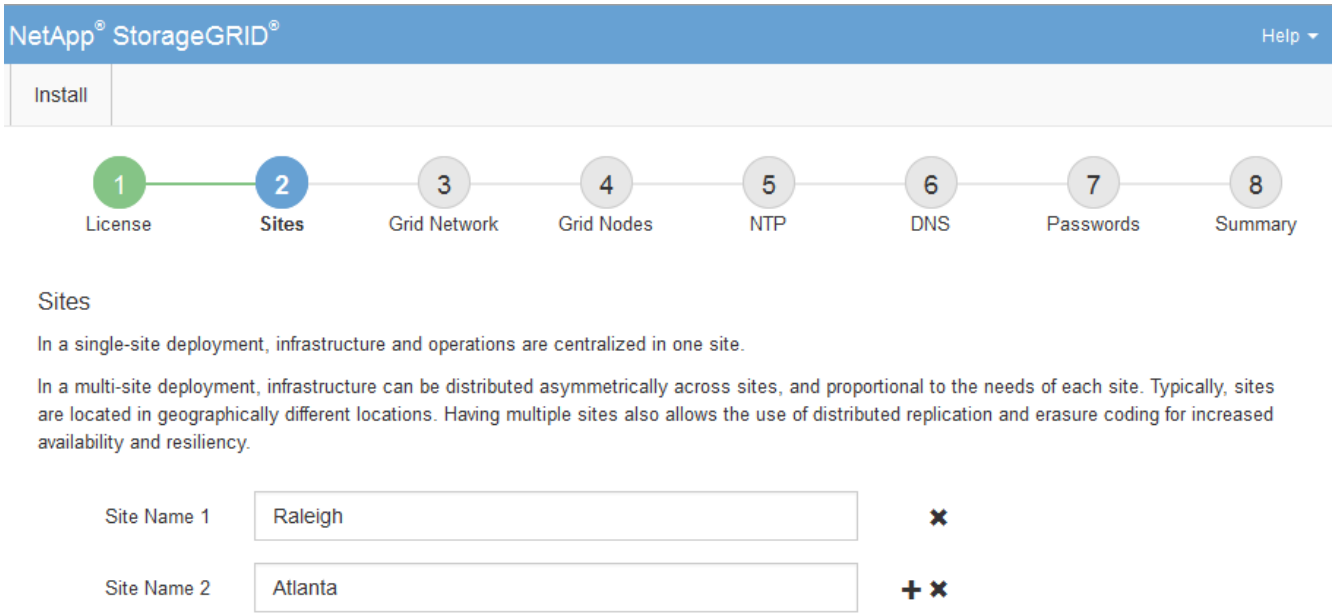
3. Seleccione **Siguiente**.

Agregar sitios

Debe crear al menos un sitio cuando instale StorageGRID. Puede crear sitios adicionales para aumentar la fiabilidad y la capacidad de almacenamiento de su sistema StorageGRID.

1. En la página Sitios, introduzca el **Nombre del sitio**.
2. Para agregar sitios adicionales, haga clic en el signo más situado junto a la última entrada del sitio e introduzca el nombre en el nuevo cuadro de texto **Nombre del sitio**.

   Agregue tantos sitios adicionales como sea necesario para la topología de la cuadrícula. Puede agregar hasta 16 sitios.



3. Haga clic en **Siguiente**.

Especifique las subredes de red de red

Debe especificar las subredes que se utilizan en la red de cuadrícula.

Acerca de esta tarea

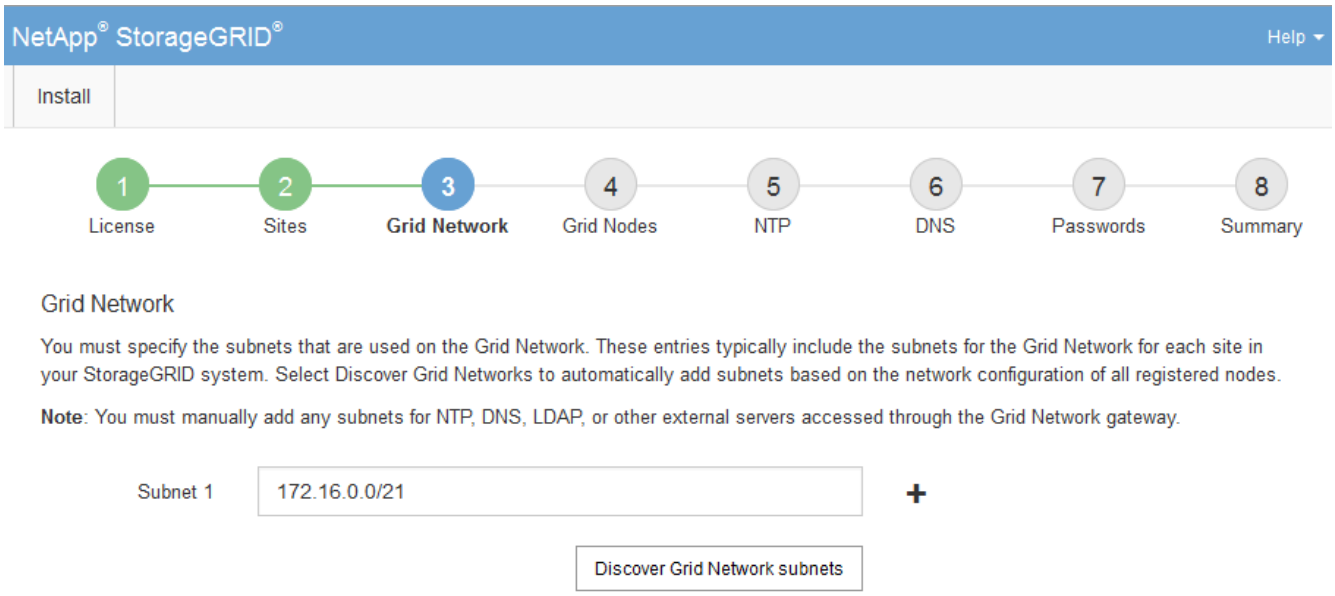
Las entradas de subred incluyen las subredes de la red de grid para cada sitio del sistema de StorageGRID, junto con las subredes a las que sea necesario acceder a través de la red de grid.

Si tiene varias subredes de cuadrícula, se requiere la puerta de enlace de red de cuadrícula. Todas las subredes de la cuadrícula especificadas deben ser accesibles a través de esta puerta de enlace.

Pasos

1. Especifique la dirección de red CIDR para al menos una red de cuadrícula en el cuadro de texto **Subnet 1**.
2. Haga clic en el signo más situado junto a la última entrada para añadir una entrada de red adicional.

   Si ya ha implementado al menos un nodo, haga clic en **detectar subredes** de redes de cuadrícula para rellenar automáticamente la Lista de subredes de red de cuadrícula con las subredes notificadas por los nodos de cuadrícula que se han registrado en el Gestor de cuadrícula.



3. Haga clic en **Siguiente**.

Aprobar los nodos de cuadrícula pendientes

Debe aprobar cada nodo de cuadrícula para poder unirse al sistema StorageGRID.

Antes de empezar

Ha puesto en marcha todos los nodos de grid de dispositivos virtuales y StorageGRID.

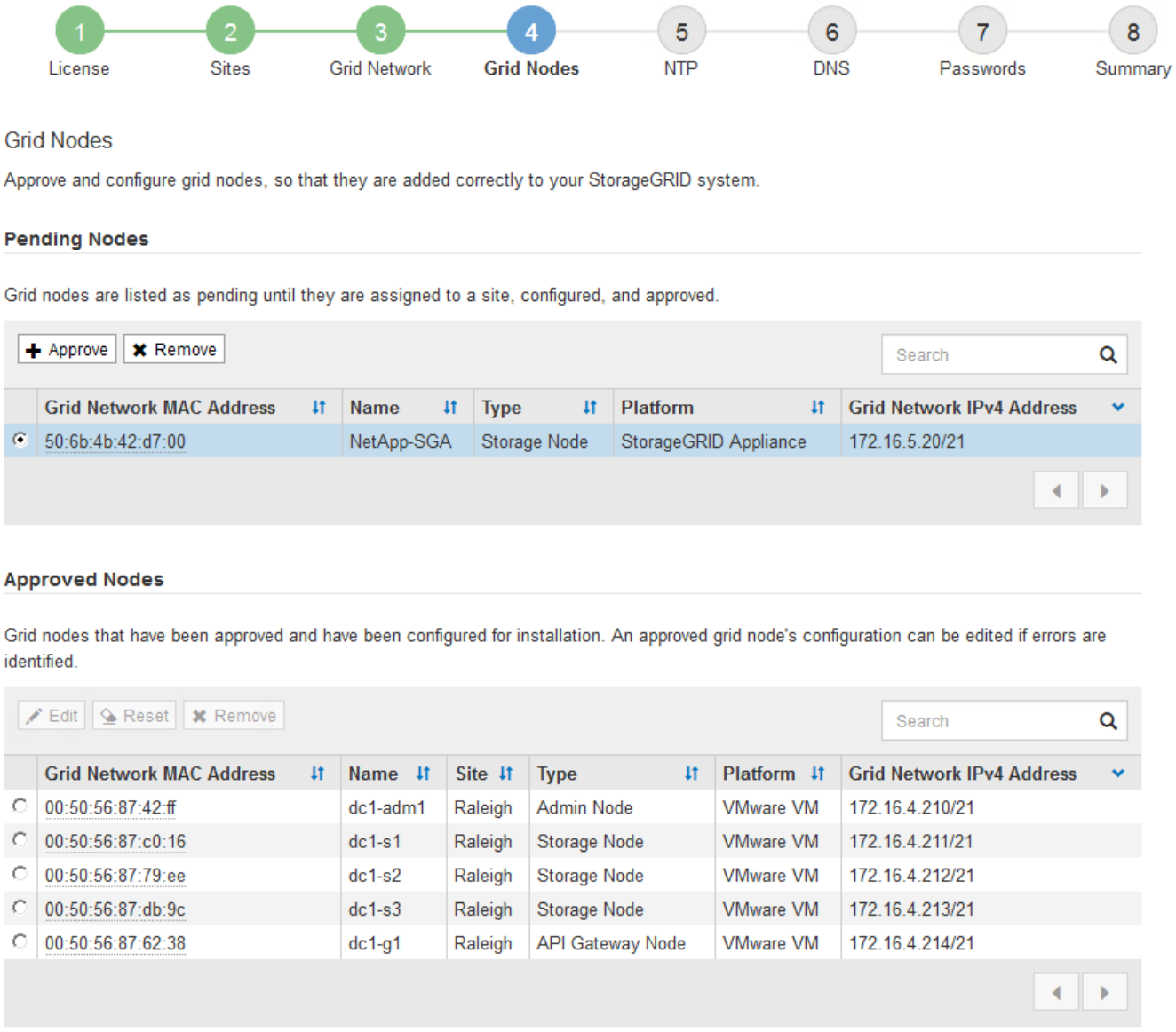
> Es más eficiente realizar una instalación única de todos los nodos, en lugar de instalar algunos ahora y algunos nodos más adelante.

Pasos

1. Revise la lista Pending Nodes y confirme que se muestran todos los nodos de grid que ha implementado.

> Si falta un nodo de cuadrícula, confirme que se ha implementado correctamente.

2. Seleccione el botón de opción situado junto al nodo pendiente que desea aprobar.



3. Haga clic en **aprobar**.
4. En Configuración general, modifique la configuración de las siguientes propiedades según sea necesario:
   - **Sitio**: El nombre del sistema del sitio para este nodo de cuadrícula.
   - **Nombre**: El nombre del sistema para el nodo. El nombre predeterminado es el nombre que especifique cuando configure el nodo.

     Los nombres de sistema son necesarios para las operaciones internas de StorageGRID y no se pueden cambiar después de completar la instalación. Sin embargo, durante este paso del proceso de instalación, puede cambiar los nombres del sistema según sea necesario.

   - **Función NTP**: La función de Protocolo de hora de red (NTP) del nodo de red. Las opciones son **automático**, **primario** y **Cliente**. Al seleccionar **automático**, se asigna la función principal a los nodos de administración, los nodos de almacenamiento con servicios ADC, los nodos de puerta de enlace y cualquier nodo de cuadrícula que tenga direcciones IP no estáticas. Al resto de los nodos de grid se le asigna el rol de cliente.

Asegúrese de que al menos dos nodos de cada sitio puedan acceder a al menos cuatro fuentes de NTP externas. Si solo un nodo de un sitio puede acceder a los orígenes NTP, se producirán problemas de tiempo si ese nodo falla. Además, designar dos nodos por sitio como orígenes NTP primarios garantiza una sincronización precisa si un sitio está aislado del resto de la cuadrícula.

- **Tipo de almacenamiento** (solo nodos de almacenamiento): Especifique que un nuevo nodo de almacenamiento se utilice exclusivamente para metadatos. Las opciones son **Objetos y metadatos** y **Solo metadatos**. Consulte "Tipos de nodos de almacenamiento" Para obtener más información sobre nodos de almacenamiento solo de metadatos.

  Cuando se instala un grid con nodos solo metadatos, este también debe contener un número mínimo de nodos para el almacenamiento de objetos. Para un grid de sitio único, hay al menos dos nodos de almacenamiento configurados para objetos y metadatos. Para un grid de varios sitios, al menos un nodo de almacenamiento por sitio está configurado para objetos y metadatos.

- **Servicio ADC** (sólo nodos de almacenamiento): Seleccione **automático** para que el sistema determine si el nodo requiere el servicio controlador de dominio administrativo (ADC). El servicio ADC realiza un seguimiento de la ubicación y disponibilidad de los servicios de red. Al menos tres nodos de almacenamiento en cada sitio deben incluir el servicio ADC. No puede agregar el servicio ADC a un nodo después de que se haya desplegado.

5. En Red de cuadrícula, modifique la configuración de las siguientes propiedades según sea necesario:

   - **Dirección IPv4 (CIDR)**: La dirección de red CIDR para la interfaz de red Grid (eth0 dentro del contenedor). Por ejemplo: 192.168.1.234/21
   - **Gateway**: El gateway de red de red de red de red de red de red de Por ejemplo: 192.168.0.1

     La puerta de enlace es necesaria si hay varias subredes de la cuadrícula.

   Si seleccionó DHCP para la configuración de red de cuadrícula y cambia el valor aquí, el nuevo valor se configurará como dirección estática en el nodo. Debe asegurarse de que la dirección IP resultante no esté dentro del pool de direcciones de DHCP.

6. Si desea configurar la red administrativa para el nodo de grid, añada o actualice los ajustes en la sección Admin Network, según sea necesario.

   Introduzca las subredes de destino de las rutas fuera de esta interfaz en el cuadro de texto **subredes (CIDR)**. Si hay varias subredes de administración, se requiere la puerta de enlace de administración.

   Si seleccionó DHCP para la configuración de red del administrador y cambia el valor aquí, el nuevo valor se configurará como dirección estática en el nodo. Debe asegurarse de que la dirección IP resultante no esté dentro del pool de direcciones de DHCP.

   Dispositivos: Para un dispositivo StorageGRID, si la red de administración no se configuró durante la instalación inicial mediante el instalador de dispositivos StorageGRID, no se puede configurar en este cuadro de diálogo Administrador de grid. En su lugar, debe seguir estos pasos:

   a. Reinicie el dispositivo: En el instalador del equipo, seleccione **Avanzado** > **Reiniciar**.

      El reinicio puede tardar varios minutos.

b. Seleccione **Configurar redes** > **Configuración de enlaces** y active las redes apropiadas.
c. Seleccione **Configurar redes** > **Configuración IP** y configure las redes habilitadas.
d. Vuelva a la página de inicio y haga clic en **Iniciar instalación**.
e. En Grid Manager: Si el nodo aparece en la tabla Nodos aprobados, elimine el nodo.
f. Quite el nodo de la tabla Pending Nodes.
g. Espere a que el nodo vuelva a aparecer en la lista Pending Nodes.
h. Confirme que puede configurar las redes adecuadas. Ya deben rellenarse con la información proporcionada en la página de configuración de IP del instalador de dispositivos.

   Para obtener más información, consulte "Inicio rápido para la instalación de hardware" para localizar las instrucciones del aparato.

7. Si desea configurar la Red cliente para el nodo de cuadrícula, agregue o actualice los ajustes en la sección Red cliente según sea necesario. Si se configura la red de cliente, se requiere la puerta de enlace y se convierte en la puerta de enlace predeterminada del nodo después de la instalación.

   > Si seleccionó DHCP para la configuración de red de cliente y cambia el valor aquí, el nuevo valor se configurará como dirección estática en el nodo. Debe asegurarse de que la dirección IP resultante no esté dentro del pool de direcciones de DHCP.

   Electrodomésticos: Para un dispositivo StorageGRID, si la red cliente no se configuró durante la instalación inicial mediante el instalador de dispositivos StorageGRID, no se puede configurar en este cuadro de diálogo Administrador de grid. En su lugar, debe seguir estos pasos:

   a. Reinicie el dispositivo: En el instalador del equipo, seleccione **Avanzado** > **Reiniciar**.

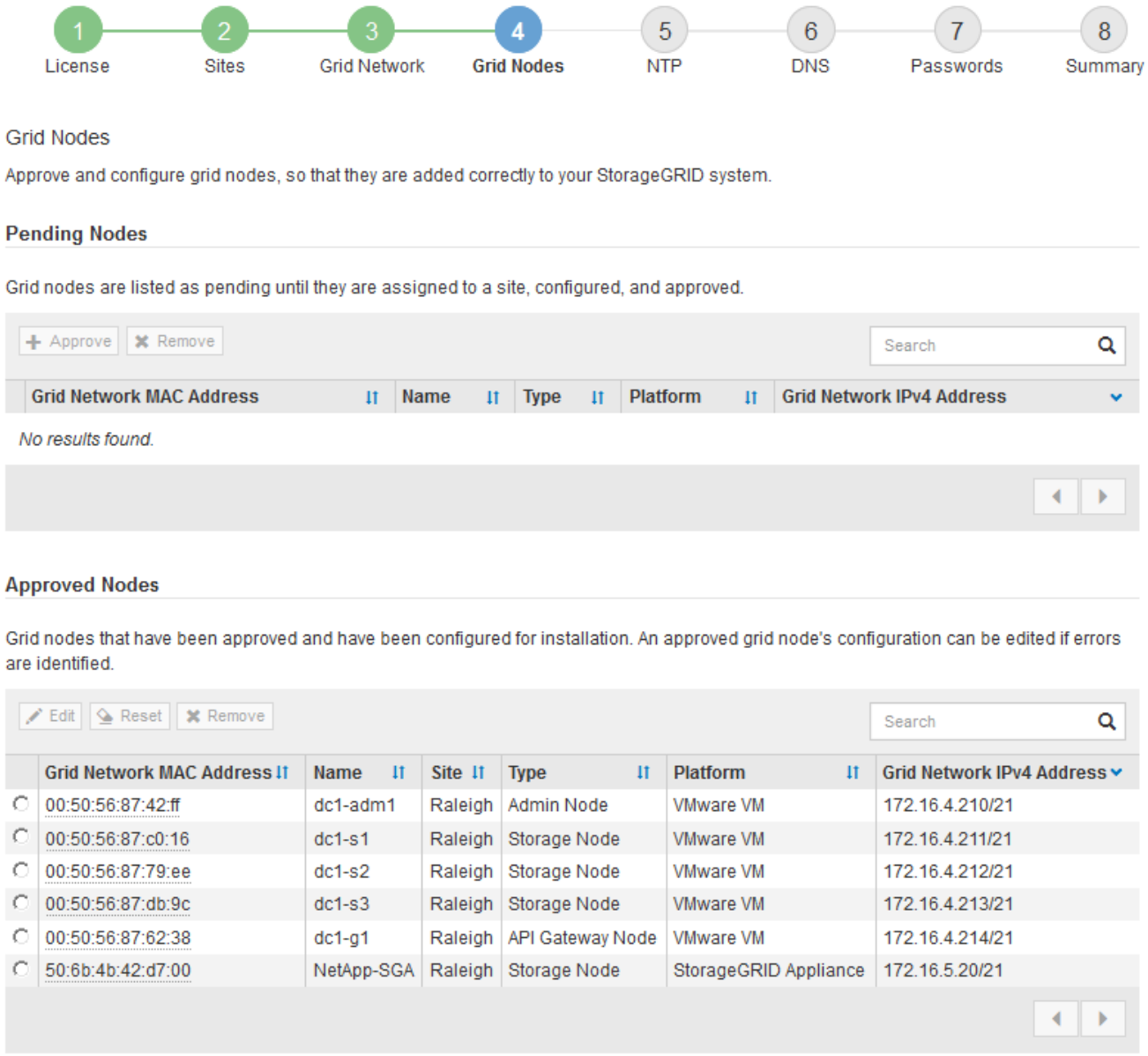
      El reinicio puede tardar varios minutos.

   b. Seleccione **Configurar redes** > **Configuración de enlaces** y active las redes apropiadas.
   c. Seleccione **Configurar redes** > **Configuración IP** y configure las redes habilitadas.
   d. Vuelva a la página de inicio y haga clic en **Iniciar instalación**.
   e. En Grid Manager: Si el nodo aparece en la tabla Nodos aprobados, elimine el nodo.
   f. Quite el nodo de la tabla Pending Nodes.
   g. Espere a que el nodo vuelva a aparecer en la lista Pending Nodes.
   h. Confirme que puede configurar las redes adecuadas. Ya deben rellenarse con la información proporcionada en la página de configuración de IP del instalador de dispositivos.

      Para saber cómo instalar dispositivos StorageGRID, consulte "Inicio rápido para la instalación de hardware" para localizar las instrucciones del aparato.

8. Haga clic en **Guardar**.

   La entrada del nodo de grid se mueve a la lista de nodos aprobados.



9. Repita estos pasos para cada nodo de cuadrícula pendiente que desee aprobar.

   Debe aprobar todos los nodos que desee de la cuadrícula. Sin embargo, puede volver a esta página en cualquier momento antes de hacer clic en **instalar** en la página Resumen. Puede modificar las propiedades de un nodo de cuadrícula aprobado seleccionando su botón de opción y haciendo clic en **Editar**.

10. Cuando haya terminado de aprobar nodos de cuadrícula, haga clic en **Siguiente**.

Especifique la información del servidor de protocolo de tiempo de redes

Es necesario especificar la información de configuración del protocolo de tiempo de redes (NTP) para el sistema StorageGRID, de manera que se puedan mantener sincronizadas las operaciones realizadas en servidores independientes.

Acerca de esta tarea

Debe especificar las direcciones IPv4 para los servidores NTP.

Debe especificar servidores NTP externos. Los servidores NTP especificados deben usar el protocolo NTP.

Debe especificar cuatro referencias de servidor NTP de estrato 3 o superior para evitar problemas con la desviación del tiempo.

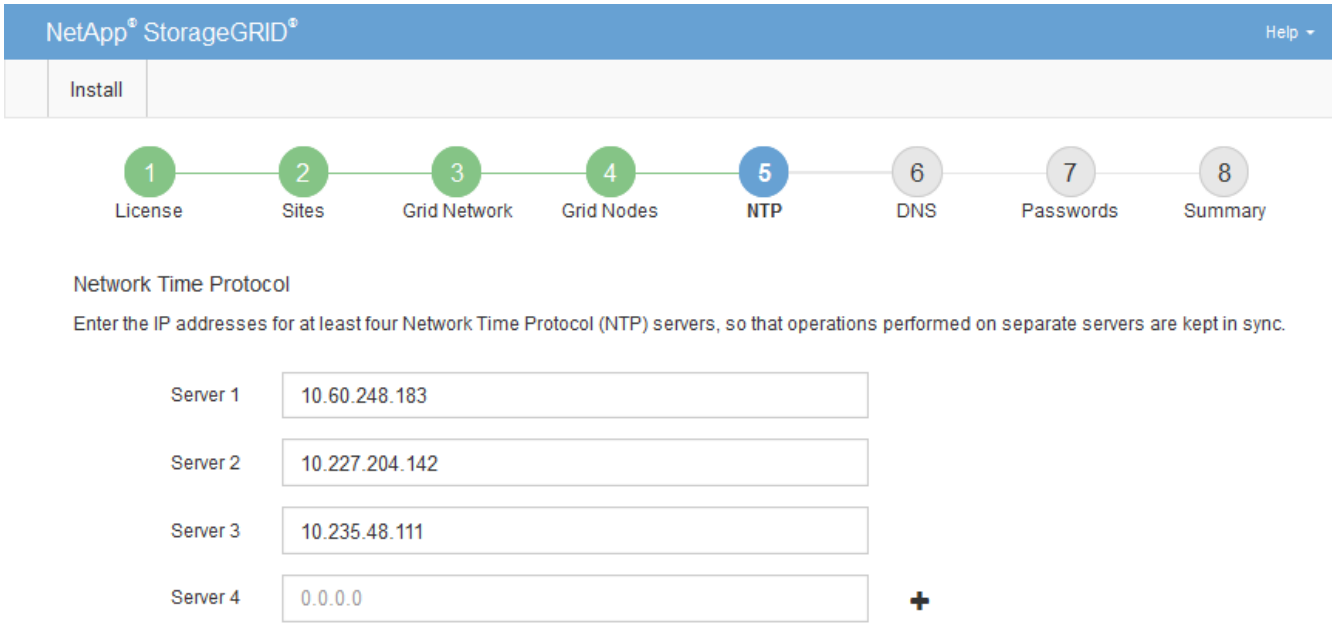
> Al especificar el origen NTP externo para una instalación de StorageGRID en el nivel de producción, no use el servicio Windows Time (W32Time) en una versión de Windows anterior a Windows Server 2016. El servicio de tiempo en versiones anteriores de Windows no es lo suficientemente preciso y no es compatible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

Los nodos a los que asignó previamente roles NTP primarios utilizan los servidores NTP externos.

> Asegúrese de que al menos dos nodos de cada sitio puedan acceder a al menos cuatro fuentes de NTP externas. Si solo un nodo de un sitio puede acceder a los orígenes NTP, se producirán problemas de tiempo si ese nodo falla. Además, designar dos nodos por sitio como orígenes NTP primarios garantiza una sincronización precisa si un sitio está aislado del resto de la cuadrícula.

Pasos

1. Especifique las direcciones IPv4 para al menos cuatro servidores NTP en los cuadros de texto **servidor 1** a **servidor 4** .
2. Si es necesario, seleccione el signo más junto a la última entrada para agregar entradas adicionales del servidor.



3. Seleccione **Siguiente**.

Información relacionada

"Directrices sobre redes"

Especifique la información del servidor DNS

Debe especificar la información DNS del sistema StorageGRID, de modo que pueda acceder a los servidores externos con nombres de host en lugar de direcciones IP.

Acerca de esta tarea

Especificando "Información del servidor DNS" Permite usar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP para notificaciones por correo electrónico y AutoSupport.

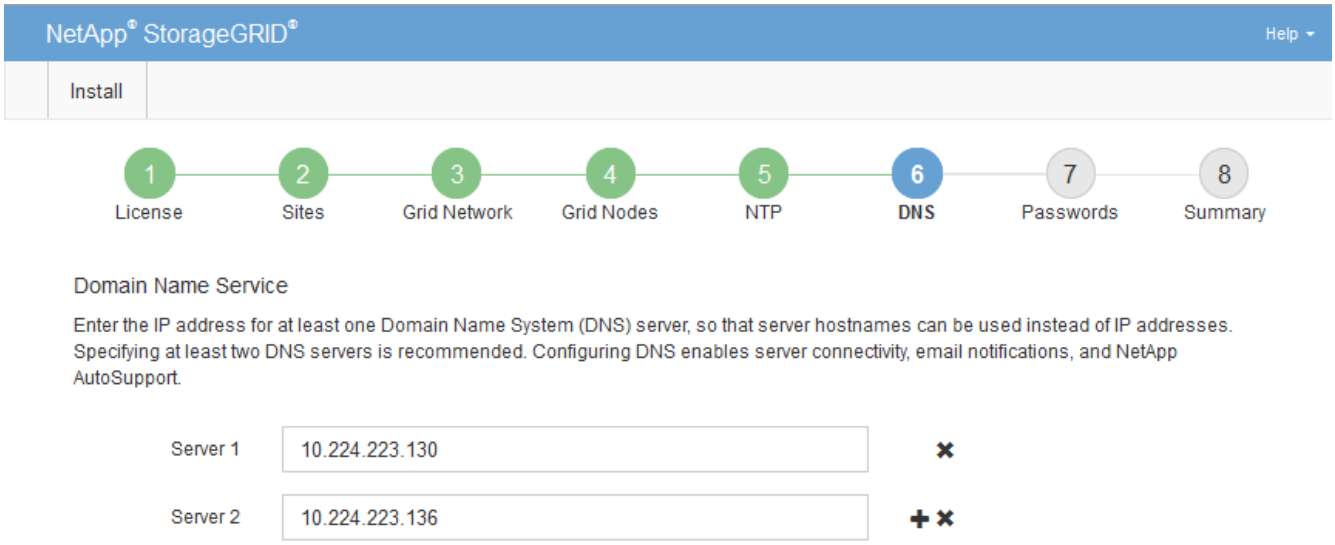
Para garantizar que el funcionamiento sea correcto, especifique dos o tres servidores DNS. Si especifica más de tres, es posible que solo se utilicen tres debido a las limitaciones conocidas del sistema operativo en algunas plataformas. Si tiene restricciones de enrutamiento en su entorno, puede "Personalice la lista de servidores DNS" Para nodos individuales (normalmente todos los nodos en un sitio) para usar un conjunto diferente de hasta tres servidores DNS.

Si es posible, utilice servidores DNS a los que cada sitio puede acceder localmente para asegurarse de que un sitio islandn pueda resolver los FQDN para destinos externos.

Si se omite o se configura incorrectamente la información del servidor DNS, se activa una alarma DNST en el servicio SSM de cada nodo de cuadrícula. La alarma se borra cuando DNS está configurado correctamente y la nueva información del servidor ha llegado a todos los nodos de la cuadrícula.

Pasos

1. Especifique la dirección IPv4 para al menos un servidor DNS en el cuadro de texto **servidor 1**.
2. Si es necesario, seleccione el signo más junto a la última entrada para agregar entradas adicionales del servidor.



   La práctica recomendada es especificar al menos dos servidores DNS. Puede especificar hasta seis servidores DNS.

3. Seleccione **Siguiente**.

Especifique las contraseñas del sistema StorageGRID

Como parte de la instalación del sistema StorageGRID, debe introducir las contraseñas que se utilizarán para proteger el sistema y realizar tareas de mantenimiento.

Acerca de esta tarea

Utilice la página instalar contraseñas para especificar la contraseña de acceso de aprovisionamiento y la contraseña de usuario raíz de administración de grid.

- La clave de acceso de aprovisionamiento se usa como clave de cifrado y el sistema StorageGRID no la almacena.
- Debe disponer de la clave de acceso de aprovisionamiento para los procedimientos de instalación, ampliación y mantenimiento, incluida la descarga del paquete de recuperación. Por lo tanto, es importante almacenar la frase de contraseña de aprovisionamiento en una ubicación segura.
- Puede cambiar la frase de acceso de aprovisionamiento desde Grid Manager si tiene la actual.
- La contraseña de usuario raíz de gestión de grid se puede cambiar mediante Grid Manager.
- Las contraseñas de SSH y la consola de línea de comandos generadas aleatoriamente se almacenan en la `Passwords.txt` En el paquete de recuperación.

Pasos

1. En **frase de paso de aprovisionamiento**, introduzca la contraseña de provisión que será necesaria para realizar cambios en la topología de la red del sistema StorageGRID.

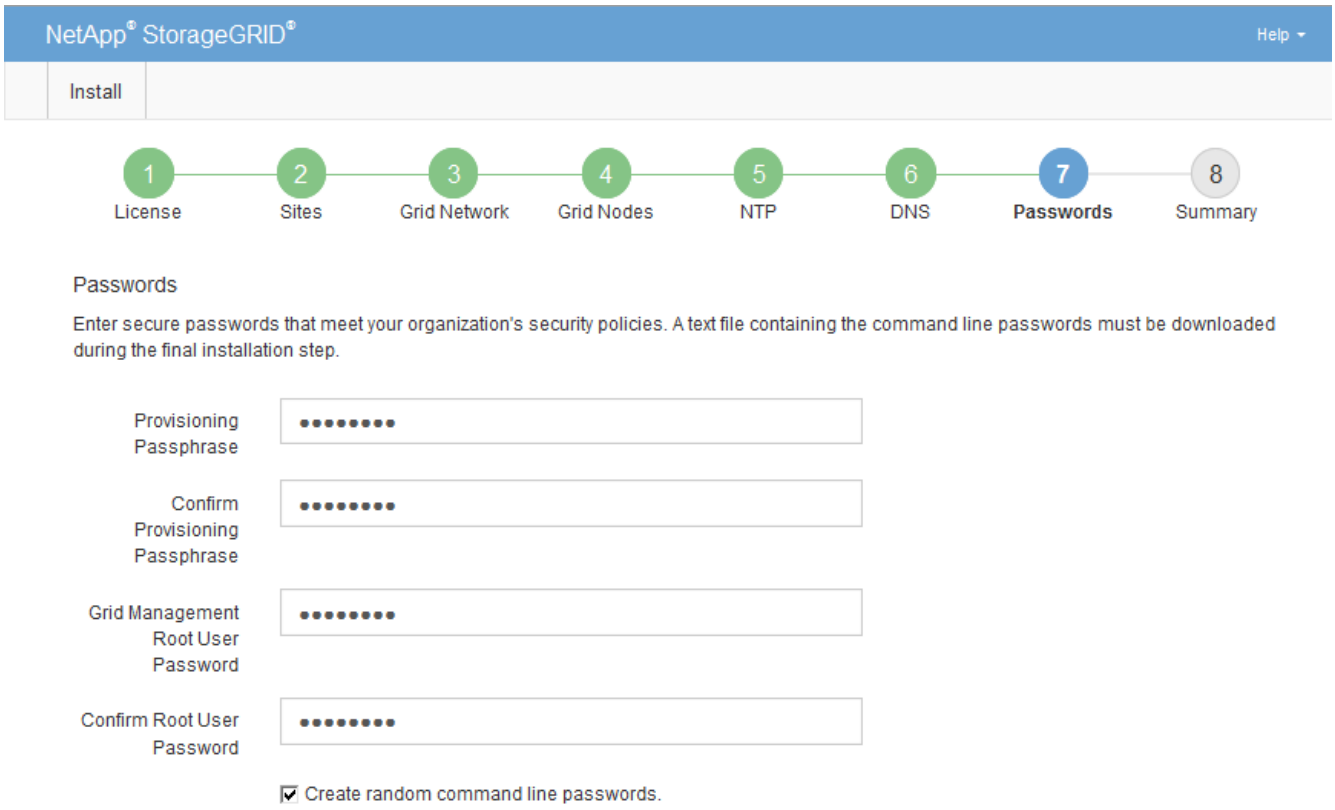
   Almacenar la clave de acceso de aprovisionamiento en un lugar seguro.

   > Si después de la instalación ha finalizado y desea cambiar la contraseña de acceso de aprovisionamiento más tarde, puede utilizar Grid Manager. Seleccione **CONFIGURACIÓN** > **Control de acceso**> **contraseñas de cuadrícula**.

2. En **Confirmar la frase de paso de aprovisionamiento**, vuelva a introducir la contraseña de aprovisionamiento para confirmarla.
3. En **Grid Management Root User Password**, introduzca la contraseña que se utilizará para acceder a Grid Manager como usuario “root”.

   Guarde la contraseña en un lugar seguro.

4. En **Confirmar contraseña de usuario raíz**, vuelva a introducir la contraseña de Grid Manager para confirmarla.



5. Si va a instalar una cuadrícula con fines de prueba de concepto o demostración, opcionalmente desactive la casilla de verificación **Crear contraseñas de línea de comandos aleatorias**.

   En las implementaciones de producción, las contraseñas aleatorias deben utilizarse siempre por motivos de seguridad. Borrar **Crear contraseñas de línea de comandos aleatorias** solo para las cuadrículas de demostración si desea utilizar contraseñas predeterminadas para acceder a los nodos de la cuadrícula desde la línea de comandos usando la cuenta “root” o “admin”.

   > Se le solicitará que descargue el archivo del paquete de recuperación (`sgws-recovery-package-id-revision.zip`) Después de hacer clic en **instalar** en la página Resumen. Debe "descargue este archivo" para completar la instalación. Las contraseñas que se necesitan para acceder al sistema se almacenan en la `Passwords.txt` Archivo, incluido en el archivo del paquete de recuperación.

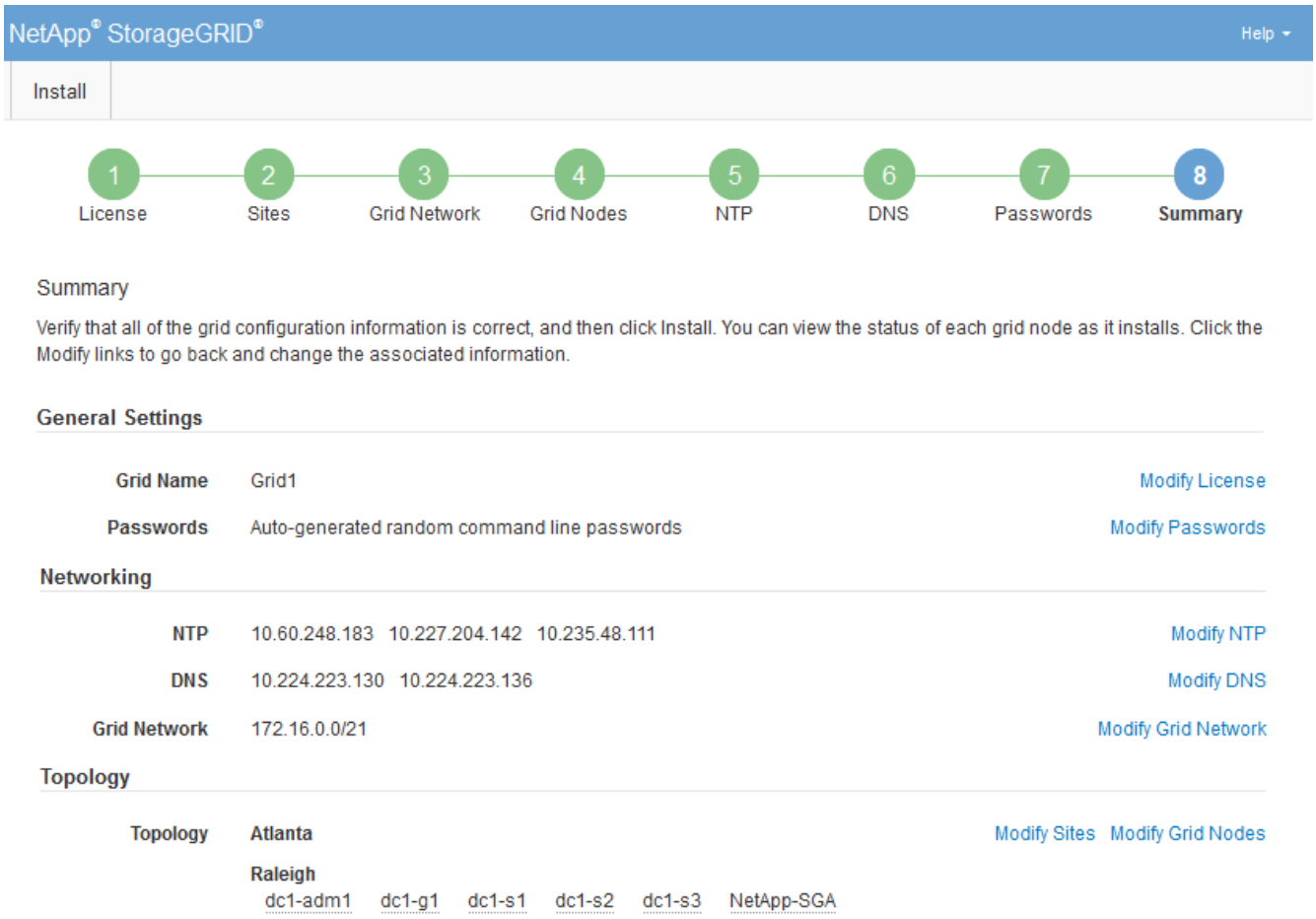
6. Haga clic en **Siguiente**.

Revise la configuración y complete la instalación

Debe revisar con cuidado la información de configuración que ha introducido para asegurarse de que la instalación se complete correctamente.

Pasos

1. Abra la página **Resumen**.



2. Verifique que toda la información de configuración de la cuadrícula sea correcta. Utilice los enlaces Modify de la página Summary para volver atrás y corregir los errores.
3. Haga clic en **instalar**.

> Si un nodo está configurado para utilizar la red de cliente, la puerta de enlace predeterminada para ese nodo cambia de la red de cuadrícula a la red de cliente cuando hace clic en **instalar**. Si se pierde la conectividad, debe asegurarse de acceder al nodo de administración principal a través de una subred accesible. Consulte "Directrices sobre redes" para obtener más detalles.

4. Haga clic en **Descargar paquete de recuperación**.

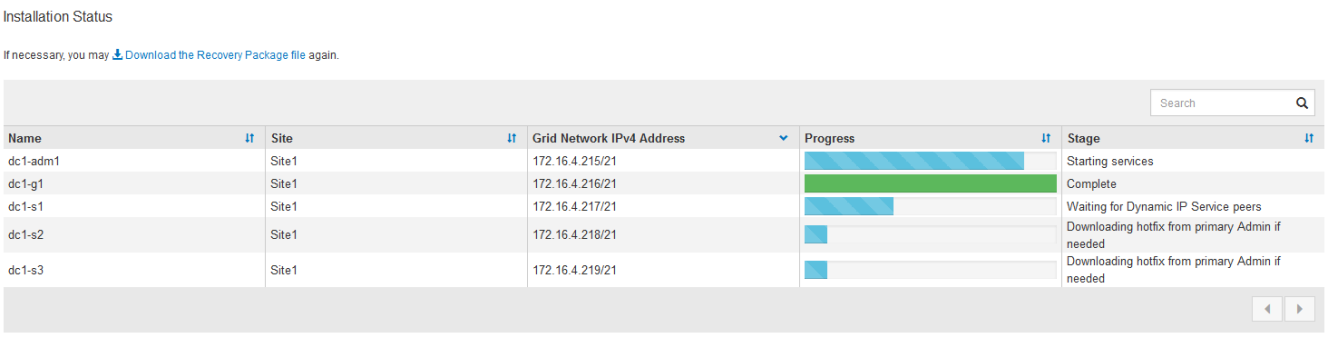
   Cuando la instalación avance hasta el punto en el que se define la topología de la cuadrícula, se le pedirá que descargue el archivo del paquete de recuperación (`.zip`), y confirme que puede obtener acceso al contenido de este archivo. Debe descargar el archivo de paquete de recuperación para que pueda recuperar el sistema StorageGRID si falla uno o más nodos de grid. La instalación continúa en segundo plano, pero no es posible completar la instalación y acceder al sistema StorageGRID hasta que se descargue y verifique este archivo.

5. Compruebe que puede extraer el contenido del `.zip` archivar y, a continuación, guardarlo en dos ubicaciones seguras, seguras e independientes.

> El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

6. Seleccione la casilla de verificación **He descargado y verificado correctamente el archivo del paquete de recuperación** y haga clic en **Siguiente**.

   Si la instalación sigue en curso, aparece la página de estado. Esta página indica el progreso de la instalación para cada nodo de cuadrícula.



   Cuando se llega a la fase completa de todos los nodos de cuadrícula, aparece la página de inicio de sesión de Grid Manager.

7. Inicie sesión en Grid Manager con el usuario "root" y la contraseña que especificó durante la instalación.

Directrices posteriores a la instalación

Después de completar la implementación y la configuración de un nodo de grid, siga estas directrices para el direccionamiento DHCP y los cambios de configuración de red.

- Si se utilizó DHCP para asignar direcciones IP, configure una reserva DHCP para cada dirección IP en las redes que se estén utilizando.

  DHCP solo puede configurarse durante la fase de implementación. No puede configurar DHCP durante la configuración.

  > Los nodos se reinician cuando cambian sus direcciones IP, lo que puede provocar interrupciones de servicio si un cambio de dirección DHCP afecta a varios nodos al mismo tiempo.

- Debe usar los procedimientos de cambio IP si desea cambiar direcciones IP, máscaras de subred y puertas de enlace predeterminadas para un nodo de grid. Consulte "Configurar las direcciones IP".
- Si realiza cambios de configuración de redes, incluidos los cambios de enrutamiento y puerta de enlace, es posible que se pierda la conectividad de cliente al nodo de administración principal y a otros nodos de grid. En función de los cambios de red aplicados, es posible que deba restablecer estas conexiones.

Información general de la instalación de la API de REST

StorageGRID proporciona la API de instalación de StorageGRID para realizar tareas de instalación.

La API utiliza la plataforma API de código abierto de Swagger para proporcionar la documentación de API. Swagger permite que tanto desarrolladores como no desarrolladores interactúen con la API en una interfaz de usuario que ilustra cómo responde la API a los parámetros y las opciones. En esta documentación se asume que está familiarizado con las tecnologías web estándar y el formato de datos JSON.

Cualquier operación de API que realice mediante la página web de documentos de API es una operación en directo. Tenga cuidado de no crear, actualizar o eliminar datos de configuración u otros datos por error.

Cada comando de API REST incluye la URL de la API, una acción HTTP, los parámetros de URL necesarios o opcionales y una respuesta de API esperada.

API de instalación de StorageGRID

La API de instalación de StorageGRID solo está disponible cuando está configurando inicialmente el sistema StorageGRID y si necesita realizar una recuperación de nodo de administración principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de la API, vaya a la página web de instalación en el nodo de administración principal y seleccione **Ayuda** > **Documentación de la API** en la barra de menús.

La API de instalación de StorageGRID incluye las siguientes secciones:

- **Config** — Operaciones relacionadas con la versión del producto y las versiones de la API. Puede mostrar la versión de la versión del producto y las versiones principales de la API que admite esa versión.
- **Grid** — Operaciones de configuración a nivel de cuadrícula. Puede obtener y actualizar la configuración de la cuadrícula, incluidos los detalles de la cuadrícula, las subredes de la red de cuadrícula, las contraseñas de la cuadrícula y las direcciones IP del servidor NTP y DNS.
- **Nodes** — Operaciones de configuración a nivel de nodo. Puede recuperar una lista de nodos de cuadrícula, eliminar un nodo de cuadrícula, configurar un nodo de cuadrícula, ver un nodo de cuadrícula y restablecer la configuración de un nodo de cuadrícula.
- **Aprovisionamiento** — Operaciones de aprovisionamiento. Puede iniciar la operación de aprovisionamiento y ver el estado de la operación de aprovisionamiento.
- **Recuperación** — Operaciones de recuperación del nodo de administración principal. Puede restablecer la información, cargar el paquete de recuperación, iniciar la recuperación y ver el estado de la operación de recuperación.
- **Paquete de recuperación** — Operaciones para descargar el paquete de recuperación.
- **Esquemas** — esquemas API para implementaciones avanzadas
- **Sites** — Operaciones de configuración a nivel de sitio. Puede crear, ver, eliminar y modificar un sitio.

Información relacionada

"Automatización de la instalación"

A continuación, ¿dónde ir

Después de completar una instalación, realice las tareas de integración y configuración necesarias. Puede realizar las tareas opcionales según sea necesario.

Tareas requeridas

- "Cree una cuenta de inquilino" Para cada protocolo de cliente (Swift o S3) que se utilizará para almacenar objetos en el sistema StorageGRID.
- "Acceso al sistema de control" mediante la configuración de grupos y cuentas de usuario. Opcionalmente, puede hacerlo "configurar un origen de identidad federado" (Como Active Directory u OpenLDAP), para

que pueda importar grupos y usuarios de administración. O bien, puede hacerlo "crear usuarios y grupos locales".

- Integre y pruebe el "S3 API" o. "API Swift" Aplicaciones cliente que utilizará para cargar objetos en el sistema StorageGRID.
- "Configure las reglas de gestión de la vida útil de la información (ILM) y la política de ILM" se desea utilizar para proteger los datos de objetos.
- Si la instalación incluye nodos de almacenamiento del dispositivo, utilice el sistema operativo SANtricity para realizar las siguientes tareas:
  - Conéctese a cada dispositivo StorageGRID.
  - Comprobar recepción de datos AutoSupport.

  Consulte "Configure el hardware".
- Revise y siga el "Directrices de fortalecimiento del sistema StorageGRID" eliminar los riesgos de seguridad.
- "Configure las notificaciones por correo electrónico para las alertas del sistema".
- Si el sistema StorageGRID incluye algún nodo de archivado (obsoleto), configure la conexión del nodo de archivado al sistema de almacenamiento de archivado externo de destino.

Tareas opcionales

- "Actualice las direcciones IP del nodo de grid" Si han cambiado desde que planificó el despliegue y generó el paquete de recuperación.
- "Configurar el cifrado del almacenamiento", si es necesario.
- "Configurar la compresión del almacenamiento" para reducir el tamaño de los objetos almacenados, si es necesario.

Solucionar problemas de instalación

Si se produce algún problema durante la instalación del sistema StorageGRID, puede acceder a los archivos de registro de la instalación. Es posible que el soporte técnico también deba utilizar los archivos de registro de instalación para resolver problemas.

Los siguientes archivos de registro de instalación están disponibles en el contenedor que ejecuta cada nodo:

- `/var/local/log/install.log` (se encuentra en todos los nodos de grid)
- `/var/local/log/gdu-server.log` (Encontrado en el nodo de administración principal)

Los siguientes archivos de registro de instalación están disponibles en el host:

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/<node-name>.log`

Para obtener información sobre cómo acceder a los archivos de registro, consulte "Recopilar archivos de registro y datos del sistema".

Información relacionada

"Solucionar los problemas de un sistema StorageGRID"

Ejemplo /etc/network/interfaces

La `/etc/network/interfaces` File incluye tres secciones, que definen las interfaces físicas, la interfaz de enlace y las interfaces VLAN. Puede combinar las tres secciones de ejemplo en un solo archivo, que agregará cuatro interfaces físicas de Linux en un único enlace LACP y establecerá tres interfaces de VLAN que tendencia al vínculo para su uso como interfaces de grid, administrador y red de cliente de StorageGRID.

Interfaces físicas

Tenga en cuenta que los switches de los otros extremos de los enlaces también deben tratar los cuatro puertos como un único enlace troncal o canal de puerto LACP y deben pasar, al menos, las tres VLAN de referencia con etiquetas.

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

Interfaz de vínculo

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

Interfaces de VLAN

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

Instale StorageGRID en VMware

Inicio rápido para instalar StorageGRID en VMware

Siga estos pasos generales para instalar un nodo VMware StorageGRID.

1 **Preparación**

- Descubra "Arquitectura de StorageGRID y topología de red".
- Conozca los aspectos específicos de "Redes StorageGRID".
- Reúna y prepare el "Información y materiales requeridos".
- Instalar y configurar "VMware vSphere Hypervisor, vCenter y los hosts ESX".
- Prepare lo necesario "CPU y RAM".
- Prevea "requisitos de rendimiento y almacenamiento".

2 **Puesta en marcha**

Despliegar nodos de grid. Cuando se implementan nodos de grid, se crean como parte del sistema

StorageGRID y se conectan a una o varias redes.

- Utilice VMware vSphere Web Client, un archivo .vmdk y un conjunto de plantillas de archivos .ovf a. "Ponga en marcha los nodos basados en software como máquinas virtuales" en los servidores que preparó en el paso 1.
- Para poner en marcha los nodos de dispositivos StorageGRID, siga el "Inicio rápido para la instalación de hardware".

Configuración

Cuando se hayan desplegado todos los nodos, utilice Grid Manager a. "configure la cuadrícula y complete la instalación".

Automatizar la instalación

Para ahorrar tiempo y garantizar la coherencia, puede automatizar la implementación y la configuración de los nodos de grid, así como la configuración del sistema StorageGRID.

- "Automatice la puesta en marcha de nodos de grid mediante VMware vSphere".
- Después de implementar los nodos de grid, "Automatice la configuración del sistema StorageGRID" Usando el script de configuración de Python proporcionado en el archivo de instalación.
- "Automatice la instalación y la configuración de los nodos de grid de dispositivos"
- Si es un desarrollador avanzado de implementaciones de StorageGRID, automatice la instalación de los nodos de grid mediante el "Instalación de la API de REST".

Planificar y preparar la instalación en VMware

Información y materiales requeridos

Antes de instalar StorageGRID, recopile y prepare la información y los materiales necesarios.

Información obligatoria

Plan de red

Qué redes pretende conectar a cada nodo StorageGRID. StorageGRID admite múltiples redes para la separación del tráfico, la seguridad y la conveniencia administrativa.

Consulte StorageGRID "Directrices sobre redes".

Información de red

A menos que se utilice DHCP, las direcciones IP para asignar a cada nodo de grid y las direcciones IP de los servidores DNS y NTP.

Servidores para nodos de grid

Identificar un conjunto de servidores (físicos, virtuales o ambos) que, agregado, proporcione los recursos suficientes para respaldar el número y el tipo de nodos de StorageGRID que va a implementar.

Si la instalación de StorageGRID no utilizará nodos de almacenamiento del dispositivo StorageGRID (hardware), debe usar almacenamiento RAID de hardware con caché de escritura respaldada por batería (BBWC). StorageGRID no admite el uso de redes de área de almacenamiento virtuales (VSAN), RAID de software ni ninguna protección RAID.

Migración de nodos (si es necesario)

Comprenda el "requisitos para la migración de nodos", si desea realizar el mantenimiento programado en hosts físicos sin ninguna interrupción del servicio.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Materiales requeridos

Licencia de StorageGRID de NetApp

Debe tener una licencia de NetApp válida y con firma digital.

En el archivo de instalación de StorageGRID se incluye una licencia que no sea de producción, y que se puede utilizar para pruebas y entornos Grid de prueba de concepto.

Archivo de instalación de StorageGRID

"Descargue el archivo de instalación de StorageGRID y extraiga los archivos".

Portátil de servicio

El sistema StorageGRID se instala a través de un ordenador portátil de servicio.

El portátil de servicio debe tener:

- Puerto de red
- Cliente SSH (por ejemplo, PuTTY)
- "Navegador web compatible"

Documentación de StorageGRID

- "Notas de la versión"
- "Instrucciones para administrar StorageGRID"

Descargue y extraiga los archivos de instalación de StorageGRID

Debe descargar los archivos de instalación de StorageGRID y extraer los archivos.

Pasos

1. Vaya a la "Página de descargas de NetApp para StorageGRID".
2. Seleccione el botón para descargar la última versión, o seleccione otra versión en el menú desplegable y seleccione **Ir**.
3. Inicie sesión con el nombre de usuario y la contraseña de su cuenta de NetApp.
4. Si aparece una declaración Precaution/MustRead, léala y seleccione la casilla de verificación.

Debe aplicar cualquier revisión requerida después de instalar la versión de StorageGRID. Para obtener más información, consulte "procedimiento de revisión en las instrucciones de recuperación y mantenimiento"

5. Lea el Contrato de licencia de usuario final, seleccione la casilla de verificación y, a continuación, seleccione * Aceptar y continuar *.
6. En la columna **instalar StorageGRID**, seleccione el archivo .tgz o .zip para VMware.

   Utilice la `.zip` Archivo si está ejecutando Windows en el portátil de servicio.

7. Guarde y extraiga el archivo de archivado.
8. Elija los archivos que necesite en la siguiente lista.

   Los archivos que necesite dependen de la topología de cuadrícula planificada y de cómo implementar el sistema StorageGRID.

Las rutas enumeradas en la tabla son relativas al directorio de nivel superior instalado por el archivo de instalación extraído.

Ruta y nombre de archivo	Descripción
	Archivo de texto que describe todos los archivos contenidos en el archivo de descarga de StorageGRID.
	Una licencia gratuita que no proporciona ningún derecho de soporte para el producto.
	El archivo de disco de máquina virtual que se usa como plantilla para crear máquinas virtuales del nodo de grid.
	El archivo de plantilla Abrir formato de virtualización (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar el nodo de administración principal.
	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de administración no primarios.
	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de archivado.
	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de puerta de enlace.

Ruta y nombre de archivo	Descripción
	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de almacenamiento basados en máquinas virtuales.
Herramienta de secuencia de comandos de la implementación	Descripción
	Una secuencia de comandos de shell Bash que se utiliza para automatizar la implementación de nodos de cuadrícula virtual.
	Ejemplo de archivo de configuración para utilizar con `deploy-vsphere-ovftool.sh` guión.
	Script Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Una secuencia de comandos Python que se utiliza para automatizar la configuración de los dispositivos StorageGRID.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de grid cuando se activa el inicio de sesión único (SSO). También puede utilizar este script para ping federate.
	Ejemplo de archivo de configuración para utilizar con `configure-storagegrid.py` guión.
	Un archivo de configuración en blanco para usar con el `configure-storagegrid.py` guión.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de grid cuando se activa el inicio de sesión único (SSO) mediante Active Directory o ping federate.
	Un guion de ayuda llamado por el compañero `storagegrid-ssoauth-azure.py` Script de Python para realizar interacciones SSO con Azure.

Ruta y nombre de archivo	Descripción
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno StorageGRID que no sea de producción para probar la compatibilidad de la actualización.

Requisitos de software para VMware

Es posible usar una máquina virtual para alojar cualquier tipo de nodo StorageGRID. Se necesita una máquina virtual para cada nodo de grid.

Hipervisor de VMware vSphere

Debe instalar VMware vSphere Hypervisor en un servidor físico preparado. El hardware debe estar configurado correctamente (incluidas las versiones del firmware y la configuración del BIOS) antes de instalar el software VMware.

- Configure las redes en el hipervisor según sea necesario para admitir la conexión a redes del sistema StorageGRID que está instalando.

  "Directrices sobre redes"

- Asegúrese de que el almacén de datos sea lo suficientemente grande para las máquinas virtuales y los discos virtuales necesarios para alojar los nodos de grid.
- Si crea más de un almacén de datos, asigne un nombre a cada almacén de datos para poder identificar fácilmente qué almacén de datos se debe usar para cada nodo de grid al crear máquinas virtuales.

Requisitos de configuración del host ESX

Debe configurar correctamente el protocolo de hora de red (NTP) en cada host ESX. Si el tiempo del host es incorrecto, podrían producirse efectos negativos, incluso la pérdida de datos.

Requisitos de configuración de VMware

Debe instalar y configurar VMware vSphere y vCenter antes de implementar los nodos de StorageGRID.

Para obtener información sobre las versiones compatibles del hipervisor de VMware vSphere y el software VMware vCenter Server, consulte la "Herramienta de matriz de interoperabilidad de NetApp".

Para conocer los pasos necesarios para instalar estos productos de VMware, consulte la documentación de VMware.

Otro software necesario

Para instalar StorageGRID en VMware, debe instalar algunos paquetes de software de terceros. Algunas distribuciones de Linux soportadas no contienen estos paquetes por defecto. Las versiones del paquete de software en las que se han probado las instalaciones de StorageGRID incluyen las que se indican en esta

página.

> Si selecciona una opción de instalación en tiempo de ejecución de contenedor y distribución de Linux que requiera alguno de estos paquetes y la distribución de Linux no los instala automáticamente, instale una de las versiones que se enumeran aquí, si está disponible en su proveedor o en el proveedor de soporte para su distribución de Linux. De lo contrario, utilice las versiones de paquete predeterminadas disponibles en su proveedor.

> Todas las opciones de instalación requieren Podman o Docker. No instale ambos paquetes. Instale solo el paquete requerido por su opción de instalación.

Versiones de Python probadas

- 3,5.2-2
- 3,6.8-2
- 3,6.8-38
- 3,6.9-1
- 3,7.3-1
- 3,8.10-0
- 3,9.2-1
- 3,9.10-2
- 3,9.16-1
- 3.10.6-1
- 3.11.2-6

Versiones de Podman probadas

- 3,2.3-0
- 3,4.4+ds1
- 4,1.1-7
- 4,2.0-11
- 4,3.1+ds1-8+b1
- 4,4.1-8
- 4,4.1-12

Versiones de Docker probadas

> La compatibilidad de Docker está obsoleta y se eliminará en un lanzamiento futuro.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23,0.6-1
- Docker-CE 24,0.2-1

- Docker-CE 24,0.4-1
- Docker-CE 24,0.5-1
- Docker-CE 24,0.7-1
- 1.5-2

Requisitos de CPU y RAM

Antes de instalar el software StorageGRID, verifique y configure el hardware de manera que esté listo para admitir el sistema StorageGRID.

Cada nodo StorageGRID requiere los siguientes recursos mínimos:

- Núcleos de CPU: 8 por nodo
- RAM: Al menos 24 GB por nodo y de 2 a 16 GB menos que la RAM total del sistema, en función de la RAM total disponible y la cantidad de software que no sea StorageGRID que se ejecute en el sistema

Asegúrese de que el número de nodos StorageGRID que tiene previsto ejecutar en cada host físico o virtual no supere el número de núcleos de CPU o la RAM física disponible. Si los hosts no están dedicados a ejecutar StorageGRID (no se recomienda), asegúrese de tener en cuenta los requisitos de recursos de las otras aplicaciones.

> Supervise el uso de la CPU y la memoria de forma regular para garantizar que estos recursos siguen teniendo la capacidad de adaptarse a su carga de trabajo. Por ejemplo, si se dobla la asignación de RAM y CPU de los nodos de almacenamiento virtual, se proporcionarán recursos similares a los que se proporcionan para los nodos de dispositivos StorageGRID. Además, si la cantidad de metadatos por nodo supera los 500 GB, puede aumentar la memoria RAM por nodo a 48 GB o más. Para obtener información sobre la gestión del almacenamiento de metadatos de objetos, el aumento del valor de Espacio Reservado de Metadatos y la supervisión del uso de CPU y memoria, consulte las instrucciones para "administración", "Supervisión", y. "actualizar" StorageGRID

Si la tecnología de subprocesos múltiples está habilitada en los hosts físicos subyacentes, puede proporcionar 8 núcleos virtuales (4 núcleos físicos) por nodo. Si el subprocesamiento no está habilitado en los hosts físicos subyacentes, debe proporcionar 8 núcleos físicos por nodo.

Si utiliza máquinas virtuales como hosts y tiene control del tamaño y el número de máquinas virtuales, debe utilizar una única máquina virtual para cada nodo StorageGRID y ajustar el tamaño de la máquina virtual según corresponda.

Para implementaciones de producción, no debe ejecutar varios nodos de almacenamiento en el mismo hardware de almacenamiento físico o host virtual. Cada nodo de almacenamiento de una única puesta en marcha de StorageGRID debe tener su propio dominio de fallos aislado. Puede maximizar la durabilidad y disponibilidad de los datos de objetos si se asegura de que un único error de hardware solo pueda afectar a un único nodo de almacenamiento.

Consulte también "Los requisitos de almacenamiento y rendimiento".

Los requisitos de almacenamiento y rendimiento

Debe comprender los requisitos de rendimiento y almacenamiento de los nodos StorageGRID alojados en las máquinas virtuales, de modo que puede proporcionar el

espacio suficiente para respaldar la configuración inicial y la expansión futura del almacenamiento.

Requisitos de rendimiento

El rendimiento del volumen del SO y del primer volumen de almacenamiento afecta significativamente el rendimiento general del sistema. Asegúrese de que proporcionan un rendimiento de disco adecuado en términos de latencia, operaciones de entrada/salida por segundo (IOPS) y rendimiento.

Todos los nodos StorageGRID requieren que la unidad de sistema operativo y todos los volúmenes de almacenamiento tengan el almacenamiento en caché de devolución de escritura habilitado. La caché debe estar en un medio protegido o persistente.

Requisitos de las máquinas virtuales que usan almacenamiento de NetApp ONTAP

Si desea implementar un nodo de StorageGRID como máquina virtual con almacenamiento asignado desde un sistema NetApp ONTAP, se ha confirmado que el volumen no tiene una política de organización en niveles de FabricPool habilitada. Por ejemplo, si un nodo StorageGRID se ejecuta como máquina virtual en un host VMware, asegúrese de que el volumen que realiza el backup del almacén de datos del nodo no tenga habilitada una política de organización en niveles de FabricPool. Al deshabilitar el almacenamiento en niveles de FabricPool para los volúmenes que se usan con los nodos StorageGRID, se simplifica la solución de problemas y las operaciones de almacenamiento.

> No utilice nunca FabricPool para colocar en niveles datos relacionados con StorageGRID en el propio StorageGRID. La organización en niveles de los datos de StorageGRID en StorageGRID aumenta la solución de problemas y la complejidad operativa.

Cantidad de máquinas virtuales necesarias

Cada sitio StorageGRID requiere como mínimo tres nodos de almacenamiento.

> En una puesta en marcha de producción, no ejecute más de un nodo de almacenamiento en un único servidor de máquina virtual. Al utilizar un host de máquina virtual dedicado para cada nodo de almacenamiento se proporciona un dominio de fallo aislado.

Se pueden implementar otros tipos de nodos, como los nodos de administrador o los nodos de pasarela, en el mismo host de máquina virtual o en sus propios hosts de máquina virtual dedicada, según sea necesario. Sin embargo, si tiene varios nodos del mismo tipo (dos nodos de Gateway, por ejemplo), no instale todas las instancias en el mismo host de máquina virtual.

Requisitos de almacenamiento por tipo de nodo

En un entorno de producción, las máquinas virtuales para nodos de StorageGRID deben cumplir diferentes requisitos, en función de los tipos de nodos.

> Las instantáneas de disco no se pueden utilizar para restaurar los nodos de grid. En su lugar, consulte "recuperación de nodo de grid" procedimientos para cada tipo de nodo.

Tipo de nodo	Reducida
Nodo de administración	LUN DE 100 GB PARA SO LUN de 200 GB para las tablas de nodos de administración LUN de 200 GB para el registro de auditoría del nodo de administración
Nodo de almacenamiento	LUN DE 100 GB PARA SO 3 LUN para cada nodo de almacenamiento en este host **Nota**: Un nodo de almacenamiento puede tener de 1 a 16 LUN de almacenamiento; se recomiendan al menos 3 LUN de almacenamiento. Tamaño mínimo por LUN: 4 TB Tamaño máximo de LUN probado: 39 TB.
Nodo de almacenamiento (solo metadatos)	1 LUN Tamaño mínimo por LUN: 4 TB **Nota**: No hay un tamaño máximo para la única LUN. Se guardará el exceso de capacidad para usarlo más adelante. **Nota**: Solo se requiere un rangedb para los nodos de almacenamiento solo de metadatos.
Nodo de puerta de enlace	LUN DE 100 GB PARA SO
Nodo de archivado	LUN DE 100 GB PARA SO

En función del nivel de auditoría configurado, el tamaño de las entradas de usuario, como el nombre de clave de objeto S3, Y cuántos datos de registro de auditoría debe conservar, es posible que necesite aumentar el tamaño del LUN del registro de auditoría en cada nodo de administración.Por lo general, un grid genera aproximadamente 1 KB de datos de auditoría por operación de S3. Lo que significaría que un LUN de 200 GB admitiría 70 millones de operaciones al día o 800 operaciones por segundo durante dos o tres días.

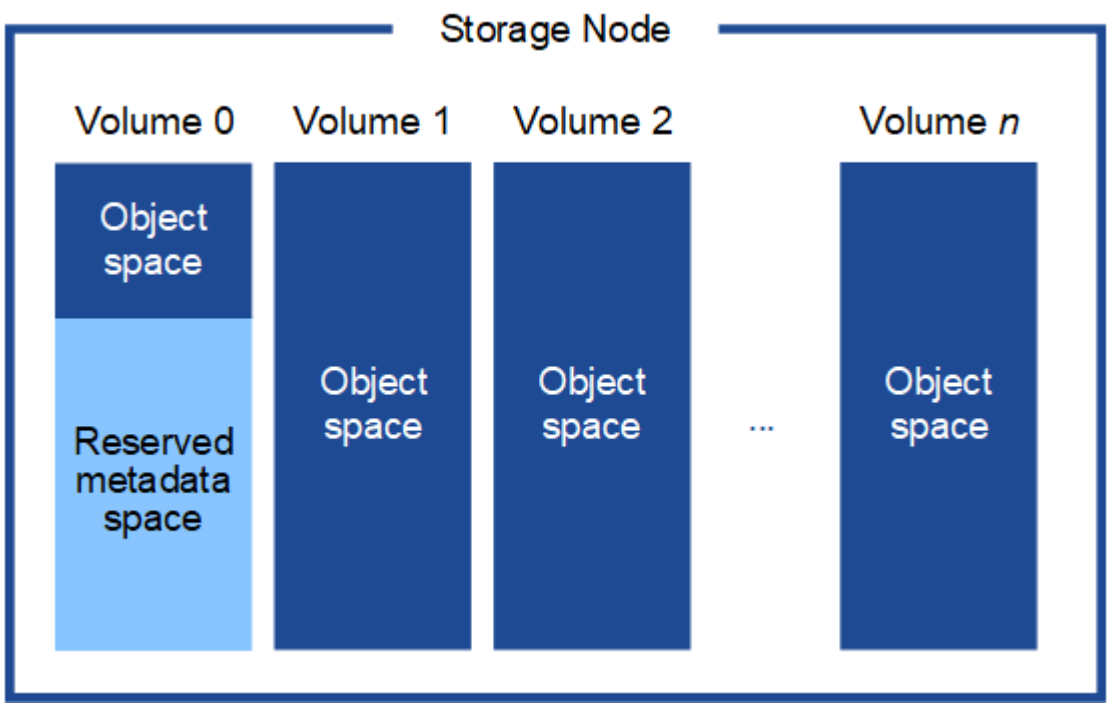
Requisitos de almacenamiento para nodos de almacenamiento

Un nodo de almacenamiento basado en software puede tener de 1 a 16 volúmenes de almacenamiento: Se recomiendan -3 o más volúmenes de almacenamiento. Cada volumen de almacenamiento debe ser 4 TB o mayor.

Un nodo de almacenamiento de dispositivo puede tener hasta 48 volúmenes de almacenamiento.

Como se muestra en la figura, StorageGRID reserva espacio para los metadatos del objeto en el volumen de almacenamiento 0 de cada nodo de almacenamiento. Cualquier espacio restante en el volumen de almacenamiento 0 y cualquier otro volumen de almacenamiento en el nodo de almacenamiento se utilizan

exclusivamente para los datos de objetos.



Para proporcionar redundancia y proteger los metadatos de objetos de la pérdida, StorageGRID almacena tres copias de los metadatos para todos los objetos del sistema en cada sitio. Las tres copias de metadatos de objetos se distribuyen uniformemente por todos los nodos de almacenamiento de cada sitio.

Cuando se instala un grid con nodos de almacenamiento solo de metadatos, el grid también debe contener un número mínimo de nodos para el almacenamiento de objetos. Consulte "Tipos de nodos de almacenamiento" Para obtener más información sobre nodos de almacenamiento solo de metadatos.

- Para un grid de sitio único, hay al menos dos nodos de almacenamiento configurados para objetos y metadatos.
- Para un grid de varios sitios, al menos un nodo de almacenamiento por sitio está configurado para objetos y metadatos.

Cuando se asigna espacio al volumen 0 de un nuevo nodo de almacenamiento, se debe garantizar que haya espacio suficiente para la porción de ese nodo de todos los metadatos de objetos.

- Como mínimo, debe asignar al menos 4 TB al volumen 0.

> Si solo se utiliza un volumen de almacenamiento para un nodo de almacenamiento y se asignan 4 TB o menos al volumen, es posible que el nodo de almacenamiento introduzca el estado de solo lectura de almacenamiento al inicio y almacene solo metadatos de objetos.

> Si se asigna menos de 500 GB al volumen 0 (solo para uso no en producción), el 10 % de la capacidad del volumen de almacenamiento se reserva para metadatos.

- Si va a instalar un nuevo sistema (StorageGRID 11,6 o superior) y cada nodo de almacenamiento tiene 128 GB o más de RAM, asigne 8 TB o más al volumen 0. Al usar un valor mayor para el volumen 0, se puede aumentar el espacio permitido para los metadatos en cada nodo de almacenamiento.
- Al configurar nodos de almacenamiento diferentes para un sitio, utilice el mismo ajuste para el volumen 0 si es posible. Si un sitio contiene nodos de almacenamiento de distintos tamaños, el nodo de

almacenamiento con el volumen más pequeño 0 determinará la capacidad de metadatos de ese sitio.

Para obtener más información, vaya a. "Gestione el almacenamiento de metadatos de objetos".

Automatización de la instalación (VMware)

Puede usar VMware vSphere para automatizar la implementación de los nodos de grid. También puede automatizar la configuración de StorageGRID.

Automatice la puesta en marcha del nodo de grid

Utilice VMware vSphere para automatizar la puesta en marcha de nodos de grid.

Antes de empezar

- Usted tiene acceso a un sistema Linux/Unix con Bash 3.2 o posterior.
- Tiene instalada y configurada correctamente la herramienta OVF de VMware 4.1.
- Conoce el nombre de usuario y la contraseña necesarios para acceder a VMware vSphere con la herramienta OVF.
- Conoce la URL de infraestructura virtual (VI) para la ubicación en vSphere donde desea implementar las máquinas virtuales de StorageGRID. Esta URL será normalmente un vApp o un grupo de recursos. Por ejemplo: `vi://vcenter.example.com/vi/sgws`

> Puede utilizar VMware `ovftool` utilidad para determinar este valor (consulte `ovftool` documentación para obtener más detalles).

> Si va a implementar en un vApp, los equipos virtuales no se iniciarán automáticamente la primera vez y deberá conectarlos manualmente.

- Recogió toda la información necesaria para el archivo de configuración. Consulte "Recopile información sobre el entorno de implementación" para obtener más información.
- Tiene acceso a los siguientes archivos desde el archivo de instalación de VMware para StorageGRID:

Nombre de archivo	Descripción
NetApp-SG-versión-SHA.vmdk	El archivo de disco de máquina virtual que se usa como plantilla para crear máquinas virtuales del nodo de grid. **Nota:** este archivo debe estar en la misma carpeta que el `.ovf` y.. `.mf` archivos.
vsphere-primary-admin.ovf vsphere-primary-admin.mf	El archivo de plantilla Abrir formato de virtualización (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar el nodo de administración principal.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de administración no primarios.

Nombre de archivo	Descripción
vsphere-archive.ovf vsphere-archive.mf	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de archivado.
vsphere-gateway.ovf vsphere-gateway.mf	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de puerta de enlace.
vsphere-storage.ovf vsphere-storage.mf	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de almacenamiento basados en máquinas virtuales.
deploy-vsphere-ovftool.sh	La secuencia de comandos de shell Bash utilizada para automatizar la implementación de nodos de cuadrícula virtual.
deploy-vsphere-ovftool-sample.ini	El archivo de configuración de ejemplo para utilizar con `deploy-vsphere-ovftool.sh` guión.

Defina el archivo de configuración para la implementación

Especifique la información necesaria para implementar nodos de grid virtual para StorageGRID en un archivo de configuración, que utiliza el `deploy-vsphere-ovftool.sh` Guión de bash. Puede modificar un archivo de configuración de ejemplo para que no tenga que crear el archivo desde cero.

Pasos

1. Realice una copia del archivo de configuración de ejemplo (`deploy-vsphere-ovftool.sample.ini`). Guarde el nuevo archivo como `deploy-vsphere-ovftool.ini` en el mismo directorio que `deploy-vsphere-ovftool.sh`.
2. Abierto `deploy-vsphere-ovftool.ini`.
3. Especifique toda la información necesaria para poner en marcha los nodos de grid virtual de VMware.

   Consulte Ajustes del archivo de configuración para obtener más información.

4. Cuando haya introducido y verificado toda la información necesaria, guarde y cierre el archivo.

Ajustes del archivo de configuración

La `deploy-vsphere-ovftool.ini` el archivo de configuración contiene la configuración necesaria para poner en marcha los nodos de grid virtual.

En primer lugar, el archivo de configuración enumera los parámetros globales y, a continuación, enumera los parámetros específicos del nodo en las secciones definidas por el nombre del nodo. Cuando se utilice el archivo:

- *Parámetros globales* se aplican a todos los nodos de cuadrícula.
- *Parámetros específicos del nodo* anulan los parámetros globales.

Parámetros globales

Los parámetros globales se aplican a todos los nodos de cuadrícula, a menos que se anulen por la configuración de secciones individuales. Coloque los parámetros que se aplican a varios nodos en la sección global Parameter y, a continuación, anule estos ajustes según sea necesario en las secciones de nodos individuales.

- **OVFTOOL_ARGUMENTS**: Puede especificar OVFTOOL_ARGUMENTS como configuración global o puede aplicar argumentos individualmente a nodos específicos. Por ejemplo:

```
OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
--datastore='datastore_name'
```

  Puede utilizar el `--powerOffTarget` y.. `--overwrite` opciones para apagar y sustituir las máquinas virtuales existentes.

  > Debe implementar nodos en almacenes de datos diferentes y especificar OVFTOOL_ARGUMENTS para cada nodo, en lugar de globalmente.

- **FUENTE**: La ruta a la plantilla de máquina virtual StorageGRID (`.vmdk`) y el `.ovf` y.. `.mf` archivos para nodos de grid individuales. De forma predeterminada, se utiliza el directorio actual.

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- **TARGET**: La URL de la infraestructura virtual (vi) de VMware vSphere para la ubicación en la que se va a implementar StorageGRID. Por ejemplo:

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- **GRID_NETWORK_CONFIG**: Método utilizado para adquirir direcciones IP, TANTO ESTÁTICAS como DHCP. El valor predeterminado es STATIC. Si todos o la mayoría de los nodos utilizan el mismo método para adquirir direcciones IP, puede especificar ese método aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
GRID_NETWORK_CONFIG = DHCP
```

- **GRID_NETWORK_TARGET**: El nombre de una red VMware existente que se utilizará para la red Grid. Si todos los nodos utilizan el mismo nombre de red, o la mayoría de ellos, puede especificarlo aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
GRID_NETWORK_TARGET = SG-Admin-Network
```

- **GRID_NETWORK_MASK**: La máscara de red para la red Grid. Si todos los nodos o la mayoría de ellos utilizan la misma máscara de red, puede especificarla aquí. A continuación, puede anular la configuración

global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_NETWORK_GATEWAY**: El gateway de red para la red Grid. Si todos o la mayoría de los nodos utilizan la misma puerta de enlace de red, puede especificarla aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- * GRID_NETWORK_MTU*: OPCIONAL. La unidad de transmisión máxima (MTU) en la red de red. Si se especifica, el valor debe estar entre 1280 y 9216. Por ejemplo:

```
GRID_NETWORK_MTU = 8192
```

  Si se omite, se usa 1400.

  Si desea utilizar tramas gigantes, establezca el MTU en un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado.

  > El valor de MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, pueden ocurrir problemas de rendimiento de red o pérdida de paquetes.

  > 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.

- **ADMIN_NETWORK_CONFIG**: El método utilizado para adquirir direcciones IP, YA SEA DESACTIVADAS, ESTÁTICAS o DHCP. El valor predeterminado es DISABLED. Si todos o la mayoría de los nodos utilizan el mismo método para adquirir direcciones IP, puede especificar ese método aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_CONFIG = STATIC
```

- **ADMIN_NETWORK_TARGET**: El nombre de una red VMware existente que se utilizará para la red de administración. Esta configuración es necesaria a menos que la red de administración esté deshabilitada. Si todos los nodos utilizan el mismo nombre de red, o la mayoría de ellos, puede especificarlo aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_TARGET = SG-Admin-Network
```

- **ADMIN_NETWORK_MASK**: La máscara DE red para la red de administración. Este ajuste es obligatorio si se utiliza una dirección IP estática. Si todos los nodos o la mayoría de ellos utilizan la misma máscara de red, puede especificarla aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_NETWORK_GATEWAY**: La puerta de enlace DE red para la red de administración. Esta configuración es necesaria si está utilizando direcciones IP estáticas y especifica subredes externas en la configuración ADMIN_NETWORK_ESL. (Es decir, no es necesario si ADMIN_NETWORK_ESL está vacío.) Si todos o la mayoría de los nodos utilizan la misma puerta de enlace de red, puede especificarla aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL**: La lista de subredes externas (rutas) para la Red Admin, especificada como una lista separada por comas de destinos de rutas CIDR. Si todos o la mayoría de los nodos utilizan la misma lista de subredes externas, puede especificarlo aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- **ADMIN_NETWORK_MTU**: OPCIONAL. La unidad de transmisión máxima (MTU) en la red de administración. No especifique si ADMIN_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se usa 1400. Si desea utilizar tramas gigantes, establezca el MTU en un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado. Si todos los nodos, o la mayoría, utilizan el mismo MTU para la red administrativa, puede especificarlo aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG**: Método utilizado para adquirir direcciones IP, YA SEA DESACTIVADAS, ESTÁTICAS o DHCP. El valor predeterminado es DISABLED. Si todos o la mayoría de los nodos utilizan el mismo método para adquirir direcciones IP, puede especificar ese método aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_CONFIG = STATIC
```

- **CLIENT_NETWORK_TARGET**: El nombre de una red VMware existente que se utilizará para la red cliente. Esta configuración es necesaria a menos que la red de cliente esté deshabilitada. Si todos los nodos utilizan el mismo nombre de red, o la mayoría de ellos, puede especificarlo aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_TARGET = SG-Client-Network
```

- **CLIENT_NETWORK_MASK**: La máscara de red para la red cliente. Este ajuste es obligatorio si se utiliza una dirección IP estática. Si todos los nodos o la mayoría de ellos utilizan la misma máscara de red, puede especificarla aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_NETWORK_GATEWAY**: La puerta de enlace de red para la red cliente. Este ajuste es obligatorio si se utiliza una dirección IP estática. Si todos o la mayoría de los nodos utilizan la misma puerta de enlace de red, puede especificarla aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **MTU_CLIENTE**: OPCIONAL. La unidad de transmisión máxima (MTU) en la red de cliente. No especifique si CLIENT_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se usa 1400. Si desea utilizar tramas gigantes, establezca el MTU en un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado. Si todos o la mayoría de los nodos utilizan el mismo MTU para la red de cliente, puede especificarlo aquí. A continuación, puede anular la configuración global especificando diferentes opciones para uno o varios nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAPP**: Reasigna cualquier puerto utilizado por un nodo para comunicaciones internas de nodo de red o comunicaciones externas. Es necesario volver a asignar puertos si las políticas de red de la empresa restringen uno o varios puertos utilizados por StorageGRID. Para obtener una lista de puertos que utiliza StorageGRID, consulte Comunicaciones internas de los nodos de grid y comunicaciones externas en "Directrices sobre redes".

  > No vuelva a asignar los puertos que está planeando utilizar para configurar los puntos finales del equilibrador de carga.

  > Si sólo SE establece PORT_REMAPP, la asignación que especifique se utilizará para las comunicaciones entrantes y salientes. Si TAMBIÉN se especifica PORT_REMAPP_INBOUND, PORT_REMAPP sólo se aplica a las comunicaciones salientes.

  El formato utilizado es: *`network type/protocol/default port used by grid node/new port`*, donde tipo de red es grid, administrador o cliente y protocolo es tcp o udp.

  Por ejemplo:

```
PORT_REMAP = client/tcp/18082/443
```

Si se utiliza solo, este ejemplo establece una asignación simétrica de las comunicaciones entrantes y salientes del nodo de cuadrícula desde el puerto 18082 al puerto 443. Si se utiliza junto con PORT_REMAPP_INBOUND, este ejemplo asigna las comunicaciones salientes del puerto 18082 al puerto 443.

- **PORT_REMAPP_INBOUND**: Reasigna las comunicaciones entrantes para el puerto especificado. Si especifica PORT_REMAP_INBOUND pero no especifica un valor para PORT_REMAP, las comunicaciones salientes para el puerto no cambian.

> No vuelva a asignar los puertos que está planeando utilizar para configurar los puntos finales del equilibrador de carga.

El formato utilizado es: *`network type/protocol/_default port used by grid node/new port`*, donde tipo de red es grid, administrador o cliente y protocolo es tcp o udp.

Por ejemplo:

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

En este ejemplo se toma el tráfico que se envía al puerto 443 para pasar un firewall interno y lo dirige al puerto 18082, donde el nodo de grid está escuchando las solicitudes de S3.

- **TEMPORARY_PASSWORD_TYPE**: Tipo de contraseña de instalación temporal que se utilizará al acceder a la consola de VM o al usar SSH antes de que el nodo se una a la cuadrícula.

> Si todos o la mayoría de los nodos utilizan el mismo tipo de contraseña de instalación temporal, especifique el tipo en la sección de parámetros globales. A continuación, de manera opcional, utilice un valor diferente para un nodo individual. Por ejemplo, si selecciona **Usar contraseña personalizada** globalmente, puede usar **CUSTOM_TEMPORARY_PASSWORD=<password>** para establecer la contraseña para cada nodo.

TEMPORARY_PASSWORD_TYPE puede ser uno de los siguientes:

  - **Usar nombre de nodo**: El nombre de nodo se utiliza como contraseña de instalación temporal.
  - **Deshabilitar contraseña**: No se utilizará ninguna contraseña de instalación temporal. Si necesita acceder a la máquina virtual para depurar los problemas de instalación, consulte "Solucionar problemas de instalación".
  - **Usar contraseña personalizada**: El valor proporcionado con **CUSTOM_TEMPORARY_PASSWORD=<password>** se utiliza como contraseña de instalación temporal.

> Opcionalmente, puede omitir el parámetro **TEMPORARY_PASSWORD_TYPE** y especificar únicamente **CUSTOM_TEMPORARY_PASSWORD=<password>**.

- **CUSTOM_TEMPORARY_PASSWORD=<password>**

Opcional. La contraseña temporal que se debe utilizar al acceder a esta máquina virtual y utilizar SSH durante la instalación. Se ignora si **TEMPORARY_PASSWORD_TYPE** está establecido en **Usar nombre de nodo** o **Desactivar contraseña**.

Parámetros específicos del nodo

Cada nodo se encuentra en su propia sección del archivo de configuración. Cada nodo requiere la siguiente configuración:

- El encabezado de sección define el nombre del nodo que se mostrará en el Gestor de cuadrícula. Puede anular este valor especificando el parámetro opcional NODE_NAME para el nodo.
- **NODE_TYPE**: VM_Admin_Node, VM_Storage_Node, VM_Archive_Node o VM_API_Gateway_Node
- **GRID_NETWORK_IP**: La dirección IP del nodo en la red de cuadrícula.
- **ADMIN_NETWORK_IP**: La dirección IP del nodo en la red de administración. Solo es obligatorio si el nodo está conectado a la red Admin y ADMIN_NETWORK_CONFIG se establece en STATIC.
- **IP_RED_CLIENTE**: La dirección IP del nodo en la red cliente. Es obligatorio sólo si el nodo está conectado a la red cliente y CLIENT_NETWORK_CONFIG para este nodo se establece en ESTÁTICO.
- **ADMIN_IP**: La dirección IP del nodo Admin primario de la red Grid. Utilice el valor especificado como GRID_NETWORK_IP para el nodo de administración principal. Si omite este parámetro, el nodo intenta detectar la IP del nodo de administración principal mediante mDNS. Para obtener más información, consulte "La forma en que los nodos de grid detectan el nodo de administrador principal".

  > El parámetro ADMIN_IP se omite para el nodo de administración principal.

- Todos los parámetros que no se establecieron globalmente. Por ejemplo, si un nodo está conectado a la red de administrador y no especificó parámetros DE RED_ADMIN en todo el mundo, debe especificarlos para el nodo.

Nodo de administrador principal

Se necesitan las siguientes configuraciones adicionales para el nodo de administración principal:

- **NODE_TYPE**: VM_Admin_Node
- **ROL_ADMINISTRADOR**: Primario

Esta entrada de ejemplo es para un nodo de administrador principal que está en las tres redes:

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_IP = 10.1.0.2
  ADMIN_NETWORK_IP = 10.3.0.2
  CLIENT_NETWORK_IP = 10.4.0.2
```

La siguiente configuración adicional es opcional para el nodo de administración principal:

- **DISCO**: De forma predeterminada, a los nodos de administración se les asignan dos discos duros adicionales de 200 GB para la auditoría y el uso de bases de datos. Es posible aumentar esta configuración con el parámetro DISK. Por ejemplo:

```
DISK = INSTANCES=2, CAPACITY=300
```

Para los nodos de administrador, LAS INSTANCIAS siempre deben ser iguales 2.

Nodo de almacenamiento

Se requiere la siguiente configuración adicional para los nodos de almacenamiento:

- **NODE_TYPE**: VM_Storage_Node

  Esta entrada de ejemplo es para un nodo de almacenamiento que se encuentra en las redes Grid y Admin, pero no en la red cliente. Este nodo utiliza LA configuración ADMIN_IP para especificar la dirección IP del nodo de administración principal en la red de grid.

```
[DC1-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.0.3
  ADMIN_NETWORK_IP = 10.3.0.3

  ADMIN_IP = 10.1.0.2
```

  Esta segunda entrada de ejemplo es para un nodo de almacenamiento en una red cliente donde la política de red empresarial del cliente establece que una aplicación cliente S3 sólo puede acceder al nodo de almacenamiento mediante el puerto 80 o 443. El archivo de configuración de ejemplo utiliza PORT_REMAP para habilitar el nodo de almacenamiento para enviar y recibir mensajes S3 en el puerto 443.

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

  El último ejemplo crea una reasignación simétrica para el tráfico ssh del puerto 22 al puerto 3022, pero establece explícitamente los valores para el tráfico entrante y saliente.

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

La siguiente configuración adicional es opcional para nodos de almacenamiento:

- **DISCO**: De forma predeterminada, a los nodos de almacenamiento se les asignan tres discos de 4 TB para el uso de RangeDB. Esta configuración se puede aumentar con el parámetro DISK. Por ejemplo:

```
DISK = INSTANCES=16, CAPACITY=4096
```

Nodo de archivado

Se requiere la siguiente configuración adicional para los nodos de archivado:

- **NODE_TYPE**: VM_Archive_Node

Esta entrada de ejemplo es para un nodo de archivado que se encuentra en las redes Grid y Admin, pero no en la red cliente.

```
[DC1-ARC1]
  NODE_TYPE = VM_Archive_Node

  GRID_NETWORK_IP = 10.1.0.4
  ADMIN_NETWORK_IP = 10.3.0.4

  ADMIN_IP = 10.1.0.2
```

Nodo de puerta de enlace

Para los nodos de puerta de enlace se requiere la siguiente configuración adicional:

- **NODE_TYPE**: VM_API_GATEWAY

Esta entrada de ejemplo es para un nodo de puerta de enlace de ejemplo en las tres redes. En este ejemplo, no se especificó ningún parámetro de red de cliente en la sección global del archivo de configuración, por lo que se deben especificar para el nodo:

```
[DC1-G1]
  NODE_TYPE = VM_API_Gateway

  GRID_NETWORK_IP = 10.1.0.5
  ADMIN_NETWORK_IP = 10.3.0.5

  CLIENT_NETWORK_CONFIG = STATIC
  CLIENT_NETWORK_TARGET = SG-Client-Network
  CLIENT_NETWORK_MASK = 255.255.255.0
  CLIENT_NETWORK_GATEWAY = 10.4.0.1
  CLIENT_NETWORK_IP = 10.4.0.5

  ADMIN_IP = 10.1.0.2
```

Nodo de administrador no primario

Se requieren los siguientes ajustes adicionales para los nodos del administrador que no son primarios:

- **NODE_TYPE**: VM_Admin_Node
- **ROL_ADMIN**: No primario

Esta entrada de ejemplo es para un nodo de administración no primario que no está en la red de cliente:

```
[DC2-ADM1]
  ADMIN_ROLE = Non-Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_TARGET = SG-Grid-Network
  GRID_NETWORK_IP = 10.1.0.6
  ADMIN_NETWORK_IP = 10.3.0.6

  ADMIN_IP = 10.1.0.2
```

La siguiente configuración adicional es opcional para los nodos de administrador que no son primarios:

- **DISCO**: De forma predeterminada, a los nodos de administración se les asignan dos discos duros adicionales de 200 GB para la auditoría y el uso de bases de datos. Es posible aumentar esta configuración con el parámetro DISK. Por ejemplo:

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  Para los nodos de administrador, LAS INSTANCIAS siempre deben ser iguales 2.

Ejecute el script Bash

Puede utilizar el `deploy-vsphere-ovftool.sh` El script bash y el archivo de configuración deploy-vsphere-ovftool.ini que modificó para automatizar la implementación de los nodos de StorageGRID en VMware vSphere.

Antes de empezar

- Ha creado un archivo de configuración deploy-vsphere-ovftool.ini para el entorno.

Puede utilizar la ayuda disponible con el script Bash introduciendo los comandos de ayuda (`-h/--help`). Por ejemplo:

```
./deploy-vsphere-ovftool.sh -h
```

o.

```
./deploy-vsphere-ovftool.sh --help
```

Pasos

1. Inicie sesión en el equipo Linux que está utilizando para ejecutar el script Bash.
2. Cambie al directorio en el que ha extraído el archivo de instalación.

   Por ejemplo:

   ```
   cd StorageGRID-Webscale-version/vsphere
   ```

3. Para desplegar todos los nodos de cuadrícula, ejecute la secuencia de comandos Bash con las opciones adecuadas para su entorno.

   Por ejemplo:

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-
   vsphere-ovftool.ini
   ```

4. Si un nodo de cuadrícula no se pudo implementar debido a un error, resuelva el error y vuelva a ejecutar el script Bash sólo para ese nodo.

   Por ejemplo:

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd --single
   -node="DC1-S3" ./deploy-vsphere-ovftool.ini
   ```

La implementación se completa cuando se pasa el estado de cada nodo.

```
Deployment Summary
+-----------------------------+----------+----------------------+
| node                        | attempts | status               |
+-----------------------------+----------+----------------------+
| DC1-ADM1                    |        1 | Passed               |
| DC1-G1                      |        1 | Passed               |
| DC1-S1                      |        1 | Passed               |
| DC1-S2                      |        1 | Passed               |
| DC1-S3                      |        1 | Passed               |
+-----------------------------+----------+----------------------+
```

Automatice la configuración de StorageGRID

Después de implementar los nodos de grid, puede automatizar la configuración del sistema StorageGRID.

Antes de empezar

- Conoce la ubicación de los siguientes archivos del archivo de instalación.

Nombre de archivo	Descripción
configure-storagegrid.py	Script Python utilizado para automatizar la configuración
configure-storagegrid.sample.json	Archivo de configuración de ejemplo para utilizar con el script
configure-storagegrid.blank.json	Archivo de configuración en blanco para utilizar con el script

- Ha creado un `configure-storagegrid.json` archivo de configuración. Para crear este archivo, puede modificar el archivo de configuración de ejemplo (`configure-storagegrid.sample.json`) o el archivo de configuración en blanco (`configure-storagegrid.blank.json`).

Puede utilizar el `configure-storagegrid.py` El guión de Python y el `configure-storagegrid.json` Archivo de configuración para automatizar la configuración del sistema StorageGRID.

También puede configurar el sistema mediante Grid Manager o la API de instalación.

Pasos

1. Inicie sesión en el equipo Linux que está utilizando para ejecutar el script Python.
2. Cambie al directorio en el que ha extraído el archivo de instalación.

   Por ejemplo:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

donde `platform` es debs, rpms o vsphere.

3. Ejecute el script Python y utilice el archivo de configuración que ha creado.

   Por ejemplo:

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

Resultado

Un paquete de recuperación `.zip` el archivo se genera durante el proceso de configuración y se descarga en el directorio en el que se ejecuta el proceso de instalación y configuración. Debe realizar una copia de seguridad del archivo de paquete de recuperación para poder recuperar el sistema StorageGRID si falla uno o más nodos de grid. Por ejemplo, cópielo en una ubicación de red segura y en una ubicación de almacenamiento en nube segura.

> El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

Si especificó que se deben generar contraseñas aleatorias, abra el `Passwords.txt` File y busque las contraseñas que se necesitan para acceder al sistema StorageGRID.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

El sistema StorageGRID se instala y configura cuando se muestra un mensaje de confirmación.

```
StorageGRID has been configured and installed.
```

Información relacionada

"Desplácese hasta Grid Manager"

"Información general de la instalación de la API de REST"

Poner en marcha nodos de grid de máquina virtual (VMware)

Recopile información sobre el entorno de implementación

Antes de implementar nodos de grid, debe recopilar información acerca de la configuración de red y el entorno de VMware.

Es más eficiente realizar una instalación única de todos los nodos, en lugar de instalar algunos ahora y algunos nodos más adelante.

Información sobre VMware

Debe acceder al entorno de implementación y recopilar información sobre el entorno de VMware, las redes que se crearon para las redes de grid, administrador y cliente, y los tipos de volúmenes de almacenamiento que se usarán para los nodos de almacenamiento.

Debe recopilar información sobre el entorno de VMware, incluidos los siguientes:

- El nombre de usuario y la contraseña de una cuenta de VMware vSphere que tenga los permisos adecuados para completar la implementación.
- Información de configuración de red, host y almacén de datos para cada máquina virtual de nodo StorageGRID.

VMware Live vMotion hace que salte el tiempo del reloj de la máquina virtual y no es compatible con los nodos de grid de ningún tipo. Aunque es poco frecuente, las horas de reloj incorrectas pueden provocar la pérdida de datos o actualizaciones de configuración.

Información de red de cuadrícula

Debe recopilar información sobre la red de VMware que se creó para la red de grid de StorageGRID (obligatoria), incluidos los siguientes elementos:

- El nombre de la red.
- El método que se utiliza para asignar direcciones IP, ya sea estáticas o DHCP.
  - Si utiliza direcciones IP estáticas, los detalles de redes necesarios para cada nodo de grid (dirección IP, puerta de enlace, máscara de red).
  - Si utiliza DHCP, la dirección IP del nodo de administración principal en la red de grid. Consulte "La forma en que los nodos de grid detectan el nodo de administrador principal" si quiere más información.

Información de la red de administrador

Para los nodos que se conectarán a la red de administrador de StorageGRID opcional, deberá recopilar información acerca de la red de VMware creada para esta red, incluidos los siguientes:

- El nombre de la red.
- El método que se utiliza para asignar direcciones IP, ya sea estáticas o DHCP.
  - Si utiliza direcciones IP estáticas, los detalles de redes necesarios para cada nodo de grid (dirección IP, puerta de enlace, máscara de red).
  - Si utiliza DHCP, la dirección IP del nodo de administración principal en la red de grid. Consulte "La forma en que los nodos de grid detectan el nodo de administrador principal" si quiere más información.
- Lista de subredes externas (ESL) para la red de administración.

Información de la red de clientes

Para los nodos que se conectarán a la red de cliente de StorageGRID opcional, deberá recopilar información acerca de la red de VMware creada para esta red, incluidos los siguientes:

- El nombre de la red.
- El método que se utiliza para asignar direcciones IP, ya sea estáticas o DHCP.
- Si utiliza direcciones IP estáticas, los detalles de redes necesarios para cada nodo de grid (dirección IP, puerta de enlace, máscara de red).

Información sobre interfaces adicionales

De manera opcional, puede añadir enlaces o interfaces de acceso a la máquina virtual en vCenter después de instalar el nodo. Por ejemplo, es posible que desee agregar una interfaz troncal a un nodo de administración o puerta de enlace, de modo que pueda utilizar interfaces VLAN para separar el tráfico que pertenece a diferentes aplicaciones o inquilinos. O bien, es posible que desee añadir una interfaz de acceso para utilizarla en un grupo de alta disponibilidad (ha).

Las interfaces que agregue se muestran en la página interfaces VLAN y en la página grupos ha de Grid Manager.

- Si agrega una interfaz troncal, configure una o varias interfaces VLAN para cada nueva interfaz principal. Consulte "Configure las interfaces VLAN".
- Si agrega una interfaz de acceso, debe añadirla directamente a los grupos de alta disponibilidad. Consulte "configuración de grupos de alta disponibilidad".

Volúmenes de almacenamiento para nodos de almacenamiento virtual

Debe recopilar la siguiente información para los nodos de almacenamiento basados en máquinas virtuales:

- El número y el tamaño de los volúmenes de almacenamiento (LUN de almacenamiento) que planea agregar. Consulte "Los requisitos de almacenamiento y rendimiento"."

Información sobre la configuración de grid

Debe recopilar información para configurar la cuadrícula:

- Licencia de Grid
- Direcciones IP del servidor del protocolo de tiempo de redes (NTP)
- Direcciones IP del servidor DNS

La forma en que los nodos de grid detectan el nodo de administrador principal

Los nodos de grid se comunican con el nodo de administrador principal para realizar tareas de configuración y gestión. Cada nodo de grid debe conocer la dirección IP del nodo de administrador principal en la red de grid.

Para garantizar que un nodo de grid pueda acceder al nodo de administrador principal, puede realizar cualquiera de las siguientes acciones al implementar el nodo:

- Puede usar el parámetro ADMIN_IP para introducir la dirección IP del nodo administrador primario manualmente.
- Puede omitir el parámetro ADMIN_IP para que el nodo del grid detecte el valor automáticamente. La detección automática es especialmente útil cuando la red de cuadrícula utiliza DHCP para asignar la dirección IP al nodo de administración principal.

La detección automática del nodo de administración principal se realiza mediante un sistema de nombres de

dominio de multidifusión (mDNS). Cuando se inicia por primera vez el nodo de administración principal, publica su dirección IP mediante mDNS. A continuación, otros nodos de la misma subred pueden consultar la dirección IP y adquirirla automáticamente. Sin embargo, debido a que el tráfico IP de multidifusión no se puede enrutar en subredes, los nodos de otras subredes no pueden adquirir directamente la dirección IP del nodo de administración principal.

Si utiliza la detección automática:

- Debe incluir la configuración ADMIN_IP para al menos un nodo de grid en las subredes a las que no está conectado directamente el nodo de administración principal. A continuación, este nodo de cuadrícula publicará la dirección IP del nodo de administración principal para otros nodos de la subred a fin de detectar con mDNS.
- Asegúrese de que la infraestructura de red admite la transferencia de tráfico IP multifundido dentro de una subred.

Ponga en marcha un nodo de StorageGRID como máquina virtual

VMware vSphere Web Client se utiliza para implementar cada nodo de grid como máquina virtual. Durante la implementación, se crea cada nodo de grid y se conecta a una o varias redes StorageGRID.

Si necesita poner en marcha algún nodo de almacenamiento con dispositivos StorageGRID, consulte "Ponga en marcha el nodo de almacenamiento del dispositivo".

Opcionalmente, puede reasignar puertos de nodo o aumentar la configuración de CPU o memoria del nodo antes de encenderlo.

Antes de empezar

- Usted ha revisado cómo "planificación y preparación de la instalación", Y comprende los requisitos de software, CPU y RAM, y almacenamiento y rendimiento.
- Ya está familiarizado con el hipervisor de VMware vSphere y tendrá experiencia en la puesta en marcha de máquinas virtuales en este entorno.

La `open-vm-tools` El paquete, una implementación de código abierto similar a las herramientas VMware, se incluye con la máquina virtual de StorageGRID. No es necesario instalar VMware Tools manualmente.

- Ha descargado y extraído la versión correcta del archivo de instalación de StorageGRID para VMware.

Si desea implementar el nuevo nodo como parte de una operación de ampliación o recuperación, debe utilizar la versión de StorageGRID que se está ejecutando en el grid.

- Tiene el disco de máquina virtual de StorageGRID (`.vmdk`) archivo:

```
NetApp-SG-version-SHA.vmdk
```

- Usted tiene la `.ovf` y.. `.mf` archivos para cada tipo de nodo de cuadrícula que esté implementando:

Nombre de archivo	Descripción
vsphere-primary-admin.ovf vsphere-primary-admin.mf	El archivo de plantilla y el archivo de manifiesto para el nodo de administración principal.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	El archivo de plantilla y el archivo de manifiesto para un nodo de administración no primario.
vsphere-storage.ovf vsphere-storage.mf	El archivo de plantilla y el archivo de manifiesto para un nodo de almacenamiento.
vsphere-gateway.ovf vsphere-gateway.mf	El archivo de plantilla y el archivo de manifiesto para un nodo de puerta de enlace.
vsphere-archive.ovf vsphere-archive.mf	El archivo de plantilla y el archivo de manifiesto para un nodo de archivado.

- La `.vdmk`, `.ovf`, y. `.mf` todos los archivos están en el mismo directorio.
- Tiene pensado minimizar los dominios de fallos. Por ejemplo, no debe implementar todos los nodos de puerta de enlace en un único servidor de máquina virtual.

> En una puesta en marcha de producción, no ejecute más de un nodo de almacenamiento en un único servidor de máquina virtual. Al utilizar un host de máquina virtual dedicado para cada nodo de almacenamiento se proporciona un dominio de fallo aislado.

- Si va a implementar un nodo como parte de una operación de expansión o recuperación, tiene el "Instrucciones para ampliar un sistema StorageGRID" o la "instrucciones de recuperación y mantenimiento".
- Si desea implementar un nodo de StorageGRID como máquina virtual con almacenamiento asignado desde un sistema NetApp ONTAP, se ha confirmado que el volumen no tiene una política de organización en niveles de FabricPool habilitada. Por ejemplo, si un nodo StorageGRID se ejecuta como máquina virtual en un host VMware, asegúrese de que el volumen que realiza el backup del almacén de datos del nodo no tenga habilitada una política de organización en niveles de FabricPool. Al deshabilitar el almacenamiento en niveles de FabricPool para los volúmenes que se usan con los nodos StorageGRID, se simplifica la solución de problemas y las operaciones de almacenamiento.

> No utilice nunca FabricPool para colocar en niveles datos relacionados con StorageGRID en el propio StorageGRID. La organización en niveles de los datos de StorageGRID en StorageGRID aumenta la solución de problemas y la complejidad operativa.

Acerca de esta tarea

Siga estas instrucciones para poner en marcha inicialmente nodos de VMware, añadir un nuevo nodo de VMware en una ampliación o reemplazar un nodo de VMware como parte de una operación de recuperación. Excepto que se indica en los pasos, el procedimiento de puesta en marcha de nodos es el mismo para todos

los tipos de nodos, incluidos los nodos de administración, los nodos de almacenamiento, los nodos de puerta de enlace y los nodos de archivado.

Si está instalando un nuevo sistema StorageGRID:

- Debe implementar el nodo de administrador principal antes de implementar cualquier otro nodo de grid.
- Debe asegurarse de que cada máquina virtual se pueda conectar al nodo de administración principal a través de la red de grid.
- Debe implementar todos los nodos de grid antes de configurar el grid.

Si va a realizar una operación de expansión o recuperación:

- Debe asegurarse de que la nueva máquina virtual pueda conectarse al nodo de administración principal a través de la red de grid.

Si necesita volver a asignar alguno de los puertos del nodo, no encienda el nodo nuevo hasta que se complete la configuración de reasignación de puerto.

Pasos

1. Con vCenter, implemente una plantilla OVF.

   Si especifica una dirección URL, elija una carpeta que contenga los siguientes archivos. De lo contrario, seleccione cada uno de estos archivos de un directorio local.

   ```
   NetApp-SG-version-SHA.vmdk
   vsphere-node.ovf
   vsphere-node.mf
   ```

   Por ejemplo, si este es el primer nodo que va a implementar, utilice estos archivos para implementar el nodo de administrador principal para el sistema StorageGRID:

   ```
   NetApp-SG-version-SHA.vmdk
   vsphere-primary-admin.ovf
   vsphere-primary-admin.mf
   ```

2. Escriba un nombre para la máquina virtual.

   La práctica estándar consiste en usar el mismo nombre tanto para la máquina virtual como para el nodo de grid.

3. Coloque la máquina virtual en el grupo de recursos o vApp apropiado.
4. Si va a implementar el nodo de administración principal, lea y acepte el Contrato de licencia para el usuario final.

   Según la versión de vCenter, el orden de los pasos variará para aceptar el acuerdo de licencia del usuario final, especificar el nombre de la máquina virtual y seleccionar un almacén de datos.

5. Seleccione el almacenamiento para la máquina virtual.

   Si desea implementar un nodo como parte de la operación de recuperación, siga las instrucciones que se

indican en paso de recuperación de almacenamiento para agregar nuevos discos virtuales, vuelva a conectar discos duros virtuales desde el nodo de cuadrícula con error, o ambos.

Al poner en marcha un nodo de almacenamiento, use 3 o más volúmenes de almacenamiento, donde cada volumen de almacenamiento es de 4 TB o más. Debe asignar al menos 4 TB al volumen 0.

> El archivo .ovf del nodo de almacenamiento define varios VMDK para el almacenamiento. A menos que estos VMDK cumplan con sus requisitos de almacenamiento, debe quitarlos y asignar los VMDK o RDM apropiados para el almacenamiento antes de encender el nodo. Los VMDK se utilizan más comúnmente en los entornos de VMware y son más fáciles de gestionar, mientras que RDM puede proporcionar un mejor rendimiento a las cargas de trabajo que utilizan tamaños de objeto más grandes (por ejemplo, mayores de 100 MB).

> Algunas instalaciones de StorageGRID pueden utilizar volúmenes de almacenamiento más grandes y activos que las cargas de trabajo virtualizadas típicas. Es posible que deba ajustar algunos parámetros de hipervisor, como `MaxAddressableSpaceTB`, para lograr un rendimiento óptimo. Si encuentra un bajo rendimiento, póngase en contacto con el recurso de soporte de virtualización para determinar si su entorno podría beneficiarse del ajuste de configuración específico de cada carga de trabajo.

6. Seleccione redes.

   Determine qué redes StorageGRID utilizará el nodo seleccionando una red de destino para cada red de origen.

   - Se requiere la red de red. Debe seleccionar una red de destino en el entorno de vSphere.
   - Si utiliza Admin Network, seleccione una red de destino diferente en el entorno de vSphere. Si no utiliza la red de administración, seleccione el mismo destino que seleccionó para la red de grid.
   - Si utiliza Client Network, seleccione una red de destino diferente en el entorno de vSphere. Si no utiliza la red cliente, seleccione el mismo destino que seleccionó para la red de grid.

7. Para **Personalizar plantilla**, configure las propiedades de nodo StorageGRID necesarias.

   a. Introduzca el **Nombre de nodo**.

   > Si va a recuperar un nodo de grid, debe introducir el nombre del nodo que se está recuperando.

   b. Utilice el menú desplegable **Contraseña de instalación temporal** para especificar una contraseña de instalación temporal, de modo que pueda acceder a la consola de VM o usar SSH antes de que el nuevo nodo se una a la cuadrícula.

   > La contraseña de instalación temporal solo se usa durante la instalación del nodo. Tras agregar un nodo a la cuadrícula, podrá acceder a él mediante la "contraseña de la consola del nodo", que aparece en la `Passwords.txt` En el paquete de recuperación.

   - **Usar nombre de nodo**: El valor que proporcionó para el campo **Nombre de nodo** se utiliza como contraseña de instalación temporal.
   - **Usar contraseña personalizada**: Se utiliza una contraseña personalizada como contraseña de instalación temporal.
   - **Deshabilitar contraseña**: No se utilizará ninguna contraseña de instalación temporal. Si necesita

acceder a la máquina virtual para depurar los problemas de instalación, consulte "Solucionar problemas de instalación".

c. Si seleccionó **Usar contraseña personalizada**, especifique la contraseña de instalación temporal que desea usar en el campo **Contraseña personalizada**.

d. En la sección **Red de cuadrícula (eth0)**, seleccione STATIC o DHCP para la **Configuración IP de red de cuadrícula**.

- Si selecciona STATIC, introduzca **Grid network IP**, **Grid network mask**, **Grid network gateway** y **Red red MTU**.
- Si selecciona DHCP, se asignan automáticamente los **Grid network IP**, **Grid network mask** y **Grid network Gateway**.

e. En el campo **IP de administración principal**, introduzca la dirección IP del nodo de administración principal para la red de red.

> Este paso no aplica si el nodo que va a implementar es el nodo de administración principal.

Si omite la dirección IP del nodo de administración principal, la dirección IP se detecta automáticamente si el nodo de administración principal o al menos otro nodo de grid con ADMIN_IP configurado, está presente en la misma subred. Sin embargo, se recomienda establecer aquí la dirección IP del nodo de administración principal.

a. En la sección **Red de administración (eth1)**, seleccione STATIC, DHCP o DISABLED para la **Configuración de IP de red de administración**.

- Si no desea utilizar la red de administración, seleccione DESACTIVADA e introduzca **0,0.0,0** para la IP de la red de administración. Puede dejar los otros campos en blanco.
- Si selecciona ESTÁTICO, introduzca **IP de red de administración**, **máscara de red de administración**, **gateway de red de administración** y **MTU de red de administración**.
- Si selecciona STATIC, introduzca la lista de subredes externas de **Admin network**. También debe configurar una puerta de enlace.
- Si selecciona DHCP, se asignan automáticamente los **IP de red de administración**, **máscara de red de administración** y **gateway de red de administración**.

b. En la sección **Red cliente (eth2)**, seleccione STATIC, DHCP o DISABLED para la configuración **IP de red cliente**.

- Si no desea utilizar la red cliente, seleccione DESACTIVADO e introduzca **0,0.0,0** para la IP de red cliente. Puede dejar los otros campos en blanco.
- Si selecciona STATIC, introduzca **IP de red de cliente**, **máscara de red de cliente**, **gateway de red de cliente** y **MTU de red de cliente**.
- Si selecciona DHCP, se asignan automáticamente **IP de red de cliente**, **máscara de red de cliente** y **Puerta de enlace de red de cliente**.

8. Revise la configuración de la máquina virtual y realice los cambios necesarios.
9. Cuando esté listo para completar, seleccione **Finalizar** para iniciar la carga de la máquina virtual.
10. Si implementó este nodo como parte de la operación de recuperación y no se trata de una recuperación de nodo completo, realice estos pasos una vez completada la implementación:

a. Haga clic con el botón derecho del ratón en la máquina virtual y seleccione **Editar configuración**.

b. Seleccione cada disco duro virtual predeterminado que se haya designado para almacenamiento y seleccione **Quitar**.

c. En función de las circunstancias de recuperación de datos, añada nuevos discos virtuales de acuerdo con sus requisitos de almacenamiento, vuelva a conectar cualquier disco duro virtual conservado del nodo de cuadrícula con error que se ha eliminado anteriormente, o ambos.

   Tenga en cuenta las siguientes directrices importantes:

   - Si va a añadir nuevos discos, debe utilizar el mismo tipo de dispositivo de almacenamiento que estaba en uso antes de la recuperación de nodos.
   - El archivo .ovf del nodo de almacenamiento define varios VMDK para el almacenamiento. A menos que estos VMDK cumplan con sus requisitos de almacenamiento, debe quitarlos y asignar los VMDK o RDM apropiados para el almacenamiento antes de encender el nodo. Los VMDK se utilizan más comúnmente en los entornos de VMware y son más fáciles de gestionar, mientras que RDM puede proporcionar un mejor rendimiento a las cargas de trabajo que utilizan tamaños de objeto más grandes (por ejemplo, mayores de 100 MB).

11. Si tiene que reasignar los puertos utilizados por este nodo, siga estos pasos.

    Es posible que deba reasignar un puerto si las políticas de red de su empresa restringen el acceso a uno o varios puertos utilizados por StorageGRID. Consulte "directrices sobre redes" Para los puertos que utiliza StorageGRID.

    > No vuelva a asignar los puertos utilizados en los extremos del equilibrador de carga.

    a. Seleccione la nueva máquina virtual.
    b. En la ficha Configurar, seleccione **Configuración** > **opciones de vApp**. La ubicación de **vApp Options** depende de la versión de vCenter.
    c. En la tabla **Propiedades**, busque PORT_REMAPP_INBOUND y PORT_REMAPP.
    d. Para asignar de forma simétrica las comunicaciones entrantes y salientes de un puerto, seleccione **PORT_REMAPP**.

       > Si sólo SE establece PORT_REMAPP, la asignación que especifique se aplicará tanto a las comunicaciones entrantes como a las salientes. Si TAMBIÉN se especifica PORT_REMAPP_INBOUND, PORT_REMAPP sólo se aplica a las comunicaciones salientes.

       i. Desplácese hacia atrás hasta la parte superior de la tabla y seleccione **Editar**.
       ii. En la ficha Tipo, seleccione **configurable por el usuario** y seleccione **Guardar**.
       iii. Seleccione **establecer valor**.
       iv. Introduzca la asignación de puertos:

           `<network type>/<protocol>/<default port used by grid node>/<new port>`

           `<network type>` es grid, administrador o cliente, y. `<protocol>` es tcp o udp.

           Por ejemplo, para reasignar el tráfico ssh del puerto 22 al puerto 3022, introduzca:

       ```
       client/tcp/22/3022
       ```

       i. Seleccione **OK**.
    e. Para especificar el puerto utilizado para las comunicaciones entrantes al nodo, seleccione

PORT_REMAPP_INBOUND.

> Si especifica PORT_REMAP_INBOUND y no especifica un valor para PORT_REMAP, las comunicaciones salientes para el puerto no cambian.

i. Desplácese hacia atrás hasta la parte superior de la tabla y seleccione **Editar**.

ii. En la ficha Tipo, seleccione **configurable por el usuario** y seleccione **Guardar**.

iii. Seleccione **establecer valor**.

iv. Introduzca la asignación de puertos:

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port
used by grid node>
```

`<network type>` es grid, administrador o cliente, y. `<protocol>` es tcp o udp.

Por ejemplo, para reasignar el tráfico SSH entrante que se envía al puerto 3022 de manera que el nodo de grid lo reciba en el puerto 22:

```
client/tcp/3022/22
```

i. Selecciona **OK**

12. Si desea aumentar la CPU o la memoria del nodo a partir de las opciones predeterminadas:
    a. Haga clic con el botón derecho del ratón en la máquina virtual y seleccione **Editar configuración**.
    b. Cambie el número de CPU o la cantidad de memoria según sea necesario.

       Establezca **Reserva de memoria** en el mismo tamaño que **memoria** asignada a la máquina virtual.

    c. Seleccione **OK**.
13. Encienda la máquina virtual.

Después de terminar

Si ha implementado este nodo como parte de un procedimiento de expansión o recuperación, vuelva a esas instrucciones para completar el procedimiento.

Configurar el grid y completar la instalación (VMware)

Desplácese hasta Grid Manager

El Gestor de cuadrícula se utiliza para definir toda la información necesaria para configurar el sistema StorageGRID.

Antes de empezar

El nodo de administración principal debe estar implementado y haber completado la secuencia de inicio inicial.

Pasos

1. Abra el explorador web y desplácese hasta una de las siguientes direcciones:

```
https://primary_admin_node_ip
```

`https://client_network_ip`

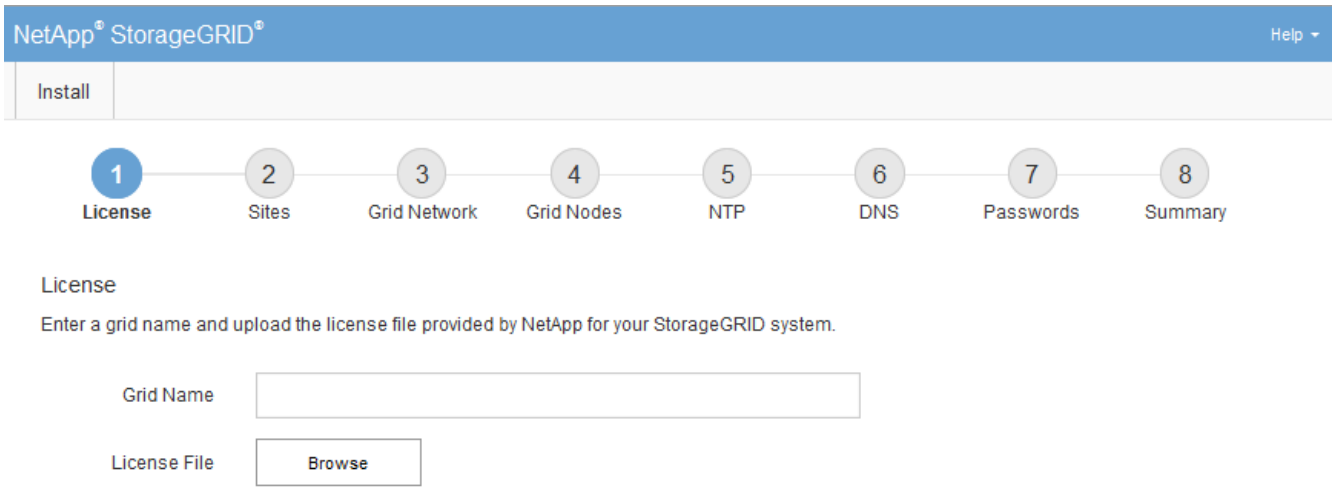
También puede acceder a Grid Manager en el puerto 8443:

`https://primary_admin_node_ip:8443`

> Puede usar la dirección IP para la IP del nodo de administración principal en la red de grid o en la red de administración, según corresponda a su configuración de red. Es posible que deba utilizar la opción security/advanced del explorador para navegar a un certificado que no es de confianza.

2. Selecciona **Instalar un sistema StorageGRID**.

   Aparece la página utilizada para configurar una cuadrícula StorageGRID.



Especifique la información de licencia de StorageGRID

Debe especificar el nombre del sistema StorageGRID y cargar el archivo de licencia proporcionado por NetApp.

Pasos

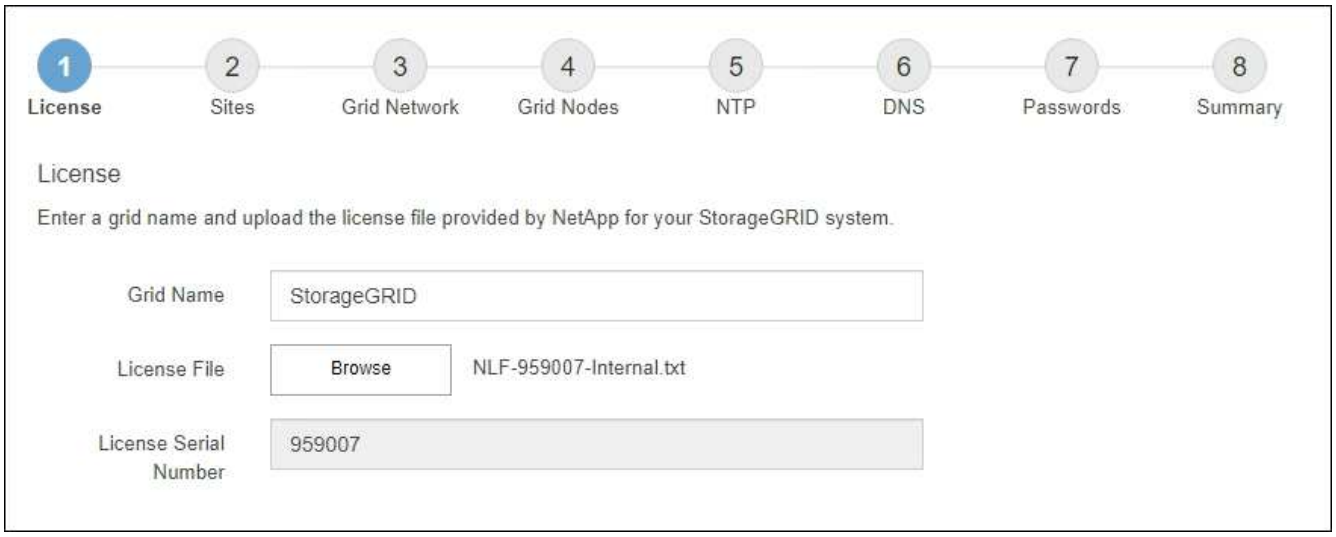
1. En la página Licencia, introduzca un nombre significativo para su sistema StorageGRID en el campo **Nombre de cuadrícula**.

   Tras la instalación, el nombre se muestra en la parte superior del menú nodos.

2. Seleccione **Examinar** y busque el archivo de licencia de NetApp (`NLF-unique-id.txt`) Y seleccione **Abrir**.

   El archivo de licencia se valida y se muestra el número de serie.

> El archivo de instalación de StorageGRID incluye una licencia gratuita que no proporciona ningún derecho de soporte para el producto. Puede actualizar a una licencia que ofrezca soporte tras la instalación.



3. Seleccione **Siguiente**.

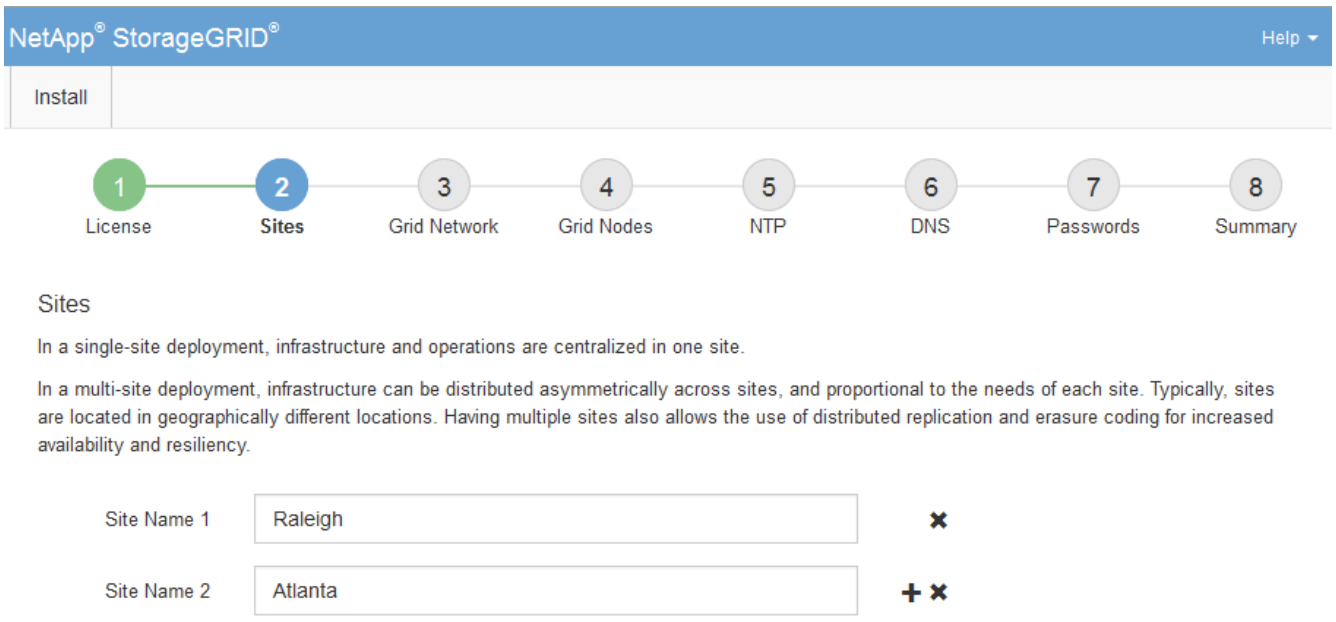
Agregar sitios

Debe crear al menos un sitio cuando instale StorageGRID. Puede crear sitios adicionales para aumentar la fiabilidad y la capacidad de almacenamiento de su sistema StorageGRID.

Pasos

1. En la página Sitios, introduzca el **Nombre del sitio**.
2. Para agregar sitios adicionales, haga clic en el signo más situado junto a la última entrada del sitio e introduzca el nombre en el nuevo cuadro de texto **Nombre del sitio**.

   Agregue tantos sitios adicionales como sea necesario para la topología de la cuadrícula. Puede agregar hasta 16 sitios.



3. Haga clic en **Siguiente**.

Especifique las subredes de red de red

Debe especificar las subredes que se utilizan en la red de cuadrícula.

Acerca de esta tarea

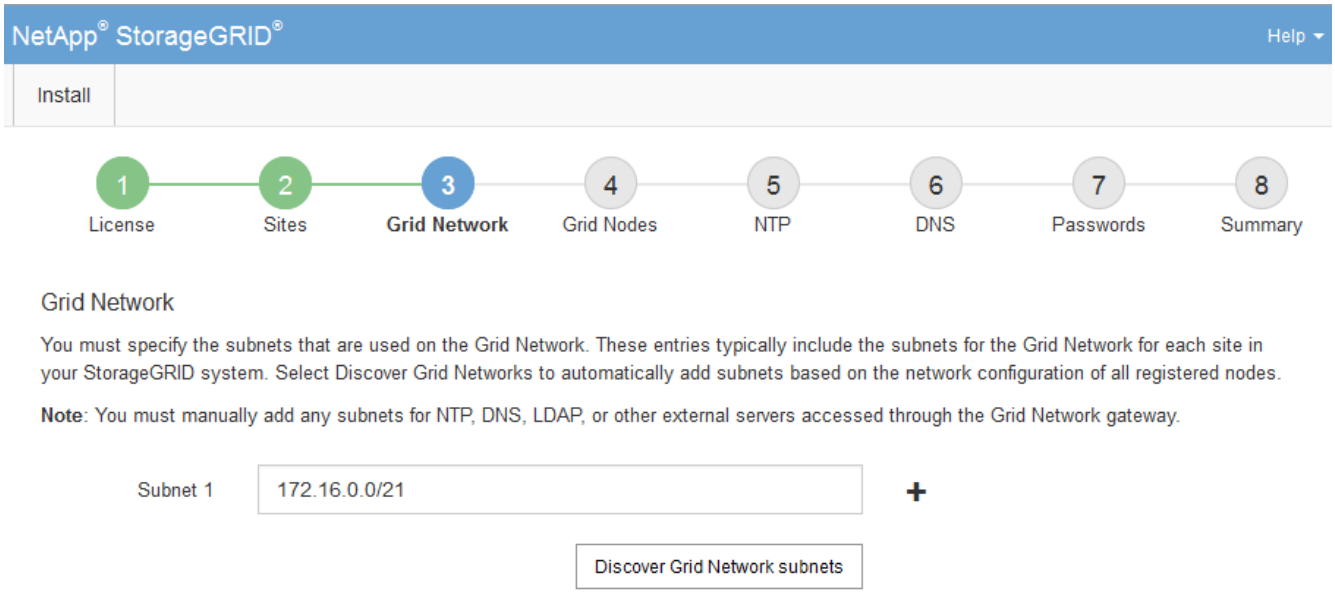
Las entradas de subred incluyen las subredes de la red de grid para cada sitio del sistema de StorageGRID, junto con las subredes a las que sea necesario acceder a través de la red de grid.

Si tiene varias subredes de cuadrícula, se requiere la puerta de enlace de red de cuadrícula. Todas las subredes de la cuadrícula especificadas deben ser accesibles a través de esta puerta de enlace.

Pasos

1. Especifique la dirección de red CIDR para al menos una red de cuadrícula en el cuadro de texto **Subnet 1**.
2. Haga clic en el signo más situado junto a la última entrada para añadir una entrada de red adicional.

   Si ya ha implementado al menos un nodo, haga clic en **detectar subredes** de redes de cuadrícula para rellenar automáticamente la Lista de subredes de red de cuadrícula con las subredes notificadas por los nodos de cuadrícula que se han registrado en el Gestor de cuadrícula.



3. Haga clic en **Siguiente**.

Aprobar los nodos de cuadrícula pendientes

Debe aprobar cada nodo de cuadrícula para poder unirse al sistema StorageGRID.

Antes de empezar

Ha puesto en marcha todos los nodos de grid de dispositivos virtuales y StorageGRID.

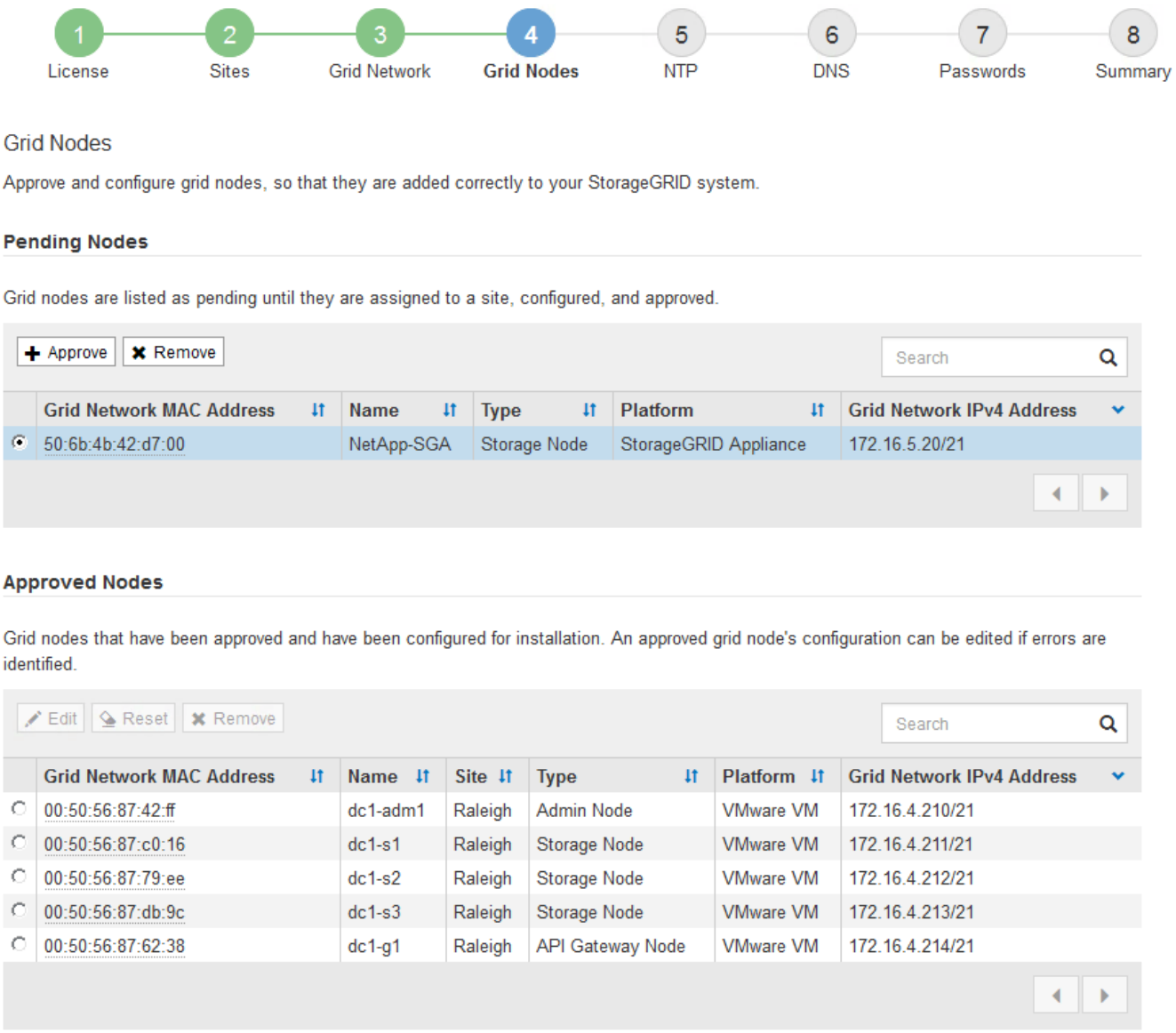
> Es más eficiente realizar una instalación única de todos los nodos, en lugar de instalar algunos ahora y algunos nodos más adelante.

Pasos

1. Revise la lista Pending Nodes y confirme que se muestran todos los nodos de grid que ha implementado.

Si falta un nodo de cuadrícula, confirme que se ha implementado correctamente.

2. Seleccione el botón de opción situado junto al nodo pendiente que desea aprobar.



3. Haga clic en **aprobar**.
4. En Configuración general, modifique la configuración de las siguientes propiedades según sea necesario:

   - **Sitio**: El nombre del sistema del sitio para este nodo de cuadrícula.
   - **Nombre**: El nombre del sistema para el nodo. El nombre predeterminado es el nombre que especifique cuando configure el nodo.

     Los nombres de sistema son necesarios para las operaciones internas de StorageGRID y no se pueden cambiar después de completar la instalación. Sin embargo, durante este paso del proceso de instalación, puede cambiar los nombres del sistema según sea necesario.

Para un nodo de VMware, aquí puede cambiar el nombre, pero esta acción no cambiará el nombre de la máquina virtual en vSphere.

- **Función NTP**: La función de Protocolo de hora de red (NTP) del nodo de red. Las opciones son **automático**, **primario** y **Cliente**. Al seleccionar **automático**, se asigna la función principal a los nodos de administración, los nodos de almacenamiento con servicios ADC, los nodos de puerta de enlace y cualquier nodo de cuadrícula que tenga direcciones IP no estáticas. Al resto de los nodos de grid se le asigna el rol de cliente.

> Asegúrese de que al menos dos nodos de cada sitio puedan acceder a al menos cuatro fuentes de NTP externas. Si solo un nodo de un sitio puede acceder a los orígenes NTP, se producirán problemas de tiempo si ese nodo falla. Además, designar dos nodos por sitio como orígenes NTP primarios garantiza una sincronización precisa si un sitio está aislado del resto de la cuadrícula.

- **Tipo de almacenamiento** (solo nodos de almacenamiento): Especifique que un nuevo nodo de almacenamiento se utilice exclusivamente para metadatos. Las opciones son **Objetos y metadatos** y **Solo metadatos**. Consulte "Tipos de nodos de almacenamiento" Para obtener más información sobre nodos de almacenamiento solo de metadatos.

> Cuando se instala un grid con nodos solo metadatos, este también debe contener un número mínimo de nodos para el almacenamiento de objetos. Para un grid de sitio único, hay al menos dos nodos de almacenamiento configurados para objetos y metadatos. Para un grid de varios sitios, al menos un nodo de almacenamiento por sitio está configurado para objetos y metadatos.

- **Servicio ADC** (sólo nodos de almacenamiento): Seleccione **automático** para que el sistema determine si el nodo requiere el servicio controlador de dominio administrativo (ADC). El servicio ADC realiza un seguimiento de la ubicación y disponibilidad de los servicios de red. Al menos tres nodos de almacenamiento en cada sitio deben incluir el servicio ADC. No puede agregar el servicio ADC a un nodo después de que se haya desplegado.

5. En Red de cuadrícula, modifique la configuración de las siguientes propiedades según sea necesario:

   - **Dirección IPv4 (CIDR)**: La dirección de red CIDR para la interfaz de red Grid (eth0 dentro del contenedor). Por ejemplo: 192.168.1.234/21
   - **Gateway**: El gateway de red de red de red de red de red de red de Por ejemplo: 192.168.0.1

   > La puerta de enlace es necesaria si hay varias subredes de la cuadrícula.

   > Si seleccionó DHCP para la configuración de red de cuadrícula y cambia el valor aquí, el nuevo valor se configurará como dirección estática en el nodo. Debe asegurarse de que la dirección IP resultante no esté dentro del pool de direcciones de DHCP.

6. Si desea configurar la red administrativa para el nodo de grid, añada o actualice los ajustes en la sección Admin Network, según sea necesario.

   Introduzca las subredes de destino de las rutas fuera de esta interfaz en el cuadro de texto **subredes (CIDR)**. Si hay varias subredes de administración, se requiere la puerta de enlace de administración.

   > Si seleccionó DHCP para la configuración de red del administrador y cambia el valor aquí, el nuevo valor se configurará como dirección estática en el nodo. Debe asegurarse de que la dirección IP resultante no esté dentro del pool de direcciones de DHCP.

   Dispositivos: Para un dispositivo StorageGRID, si la red de administración no se configuró durante la

instalación inicial mediante el instalador de dispositivos StorageGRID, no se puede configurar en este cuadro de diálogo Administrador de grid. En su lugar, debe seguir estos pasos:

a. Reinicie el dispositivo: En el instalador del equipo, seleccione **Avanzado** > **Reiniciar**.

   El reinicio puede tardar varios minutos.

b. Seleccione **Configurar redes** > **Configuración de enlaces** y active las redes apropiadas.
c. Seleccione **Configurar redes** > **Configuración IP** y configure las redes habilitadas.
d. Vuelva a la página de inicio y haga clic en **Iniciar instalación**.
e. En Grid Manager: Si el nodo aparece en la tabla Nodos aprobados, elimine el nodo.
f. Quite el nodo de la tabla Pending Nodes.
g. Espere a que el nodo vuelva a aparecer en la lista Pending Nodes.
h. Confirme que puede configurar las redes adecuadas. Ya deben rellenarse con la información proporcionada en la página de configuración de IP del instalador de dispositivos.

   Para obtener más información, consulte "Inicio rápido para la instalación de hardware" para localizar las instrucciones del aparato.

7. Si desea configurar la Red cliente para el nodo de cuadrícula, agregue o actualice los ajustes en la sección Red cliente según sea necesario. Si se configura la red de cliente, se requiere la puerta de enlace y se convierte en la puerta de enlace predeterminada del nodo después de la instalación.

   > Si seleccionó DHCP para la configuración de red de cliente y cambia el valor aquí, el nuevo valor se configurará como dirección estática en el nodo. Debe asegurarse de que la dirección IP resultante no esté dentro del pool de direcciones de DHCP.

   Electrodomésticos: Para un dispositivo StorageGRID, si la red cliente no se configuró durante la instalación inicial mediante el instalador de dispositivos StorageGRID, no se puede configurar en este cuadro de diálogo Administrador de grid. En su lugar, debe seguir estos pasos:

   a. Reinicie el dispositivo: En el instalador del equipo, seleccione **Avanzado** > **Reiniciar**.

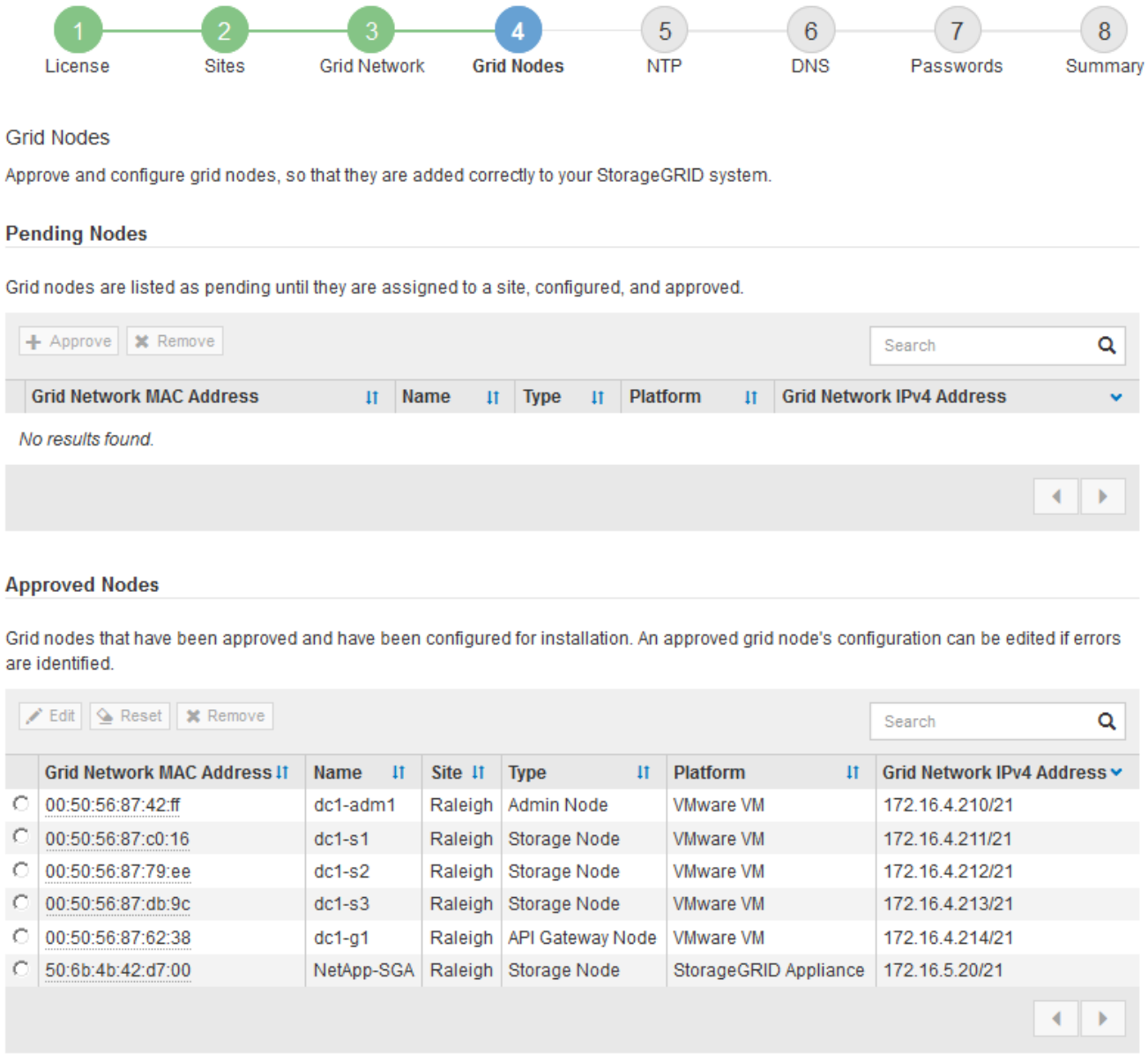
      El reinicio puede tardar varios minutos.

   b. Seleccione **Configurar redes** > **Configuración de enlaces** y active las redes apropiadas.
   c. Seleccione **Configurar redes** > **Configuración IP** y configure las redes habilitadas.
   d. Vuelva a la página de inicio y haga clic en **Iniciar instalación**.
   e. En Grid Manager: Si el nodo aparece en la tabla Nodos aprobados, elimine el nodo.
   f. Quite el nodo de la tabla Pending Nodes.
   g. Espere a que el nodo vuelva a aparecer en la lista Pending Nodes.
   h. Confirme que puede configurar las redes adecuadas. Ya deben rellenarse con la información proporcionada en la página de configuración de IP del instalador de dispositivos.

      Para obtener más información, consulte "Inicio rápido para la instalación de hardware" para localizar las instrucciones del aparato.

8. Haga clic en **Guardar**.

La entrada del nodo de grid se mueve a la lista de nodos aprobados.



9. Repita estos pasos para cada nodo de cuadrícula pendiente que desee aprobar.

   Debe aprobar todos los nodos que desee de la cuadrícula. Sin embargo, puede volver a esta página en cualquier momento antes de hacer clic en **instalar** en la página Resumen. Puede modificar las propiedades de un nodo de cuadrícula aprobado seleccionando su botón de opción y haciendo clic en **Editar**.

10. Cuando haya terminado de aprobar nodos de cuadrícula, haga clic en **Siguiente**.

Especifique la información del servidor de protocolo de tiempo de redes

Es necesario especificar la información de configuración del protocolo de tiempo de redes (NTP) para el sistema StorageGRID, de manera que se puedan mantener sincronizadas las operaciones realizadas en servidores independientes.

Acerca de esta tarea

Debe especificar las direcciones IPv4 para los servidores NTP.

Debe especificar servidores NTP externos. Los servidores NTP especificados deben usar el protocolo NTP.

Debe especificar cuatro referencias de servidor NTP de estrato 3 o superior para evitar problemas con la desviación del tiempo.

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

"Límite de soporte para configurar el servicio de tiempo de Windows para entornos de alta precisión"

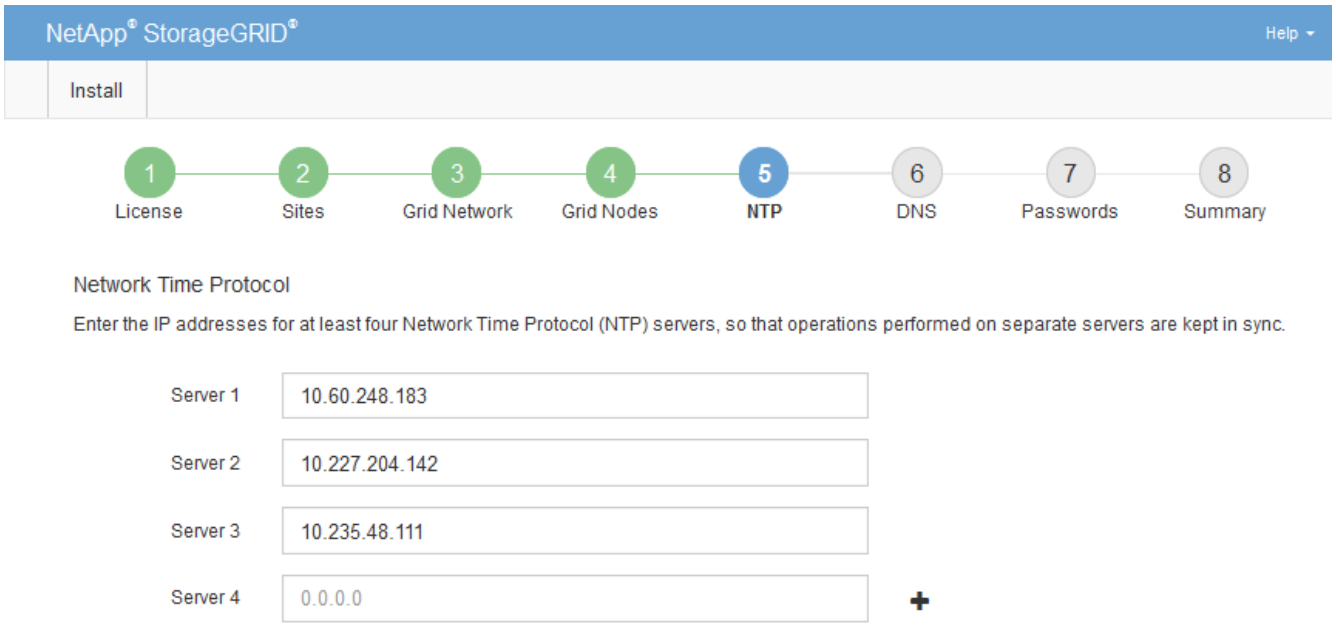
Los nodos a los que asignó previamente roles NTP primarios utilizan los servidores NTP externos.

> Asegúrese de que al menos dos nodos de cada sitio puedan acceder a al menos cuatro fuentes de NTP externas. Si solo un nodo de un sitio puede acceder a los orígenes NTP, se producirán problemas de tiempo si ese nodo falla. Además, designar dos nodos por sitio como orígenes NTP primarios garantiza una sincronización precisa si un sitio está aislado del resto de la cuadrícula.

Realizar comprobaciones adicionales de VMware, como garantizar que el hipervisor utilice el mismo origen NTP que la máquina virtual y utilizar VMTools para deshabilitar la sincronización horaria entre el hipervisor y las máquinas virtuales StorageGRID.

Pasos

1. Especifique las direcciones IPv4 para al menos cuatro servidores NTP en los cuadros de texto **servidor 1** a **servidor 4** .
2. Si es necesario, seleccione el signo más junto a la última entrada para agregar entradas adicionales del servidor.



3. Seleccione **Siguiente**.

Especifique la información del servidor DNS

Debe especificar la información DNS del sistema StorageGRID, de modo que pueda acceder a los servidores externos con nombres de host en lugar de direcciones IP.

Acerca de esta tarea

Especificando "Información del servidor DNS" Permite usar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP para notificaciones por correo electrónico y AutoSupport.

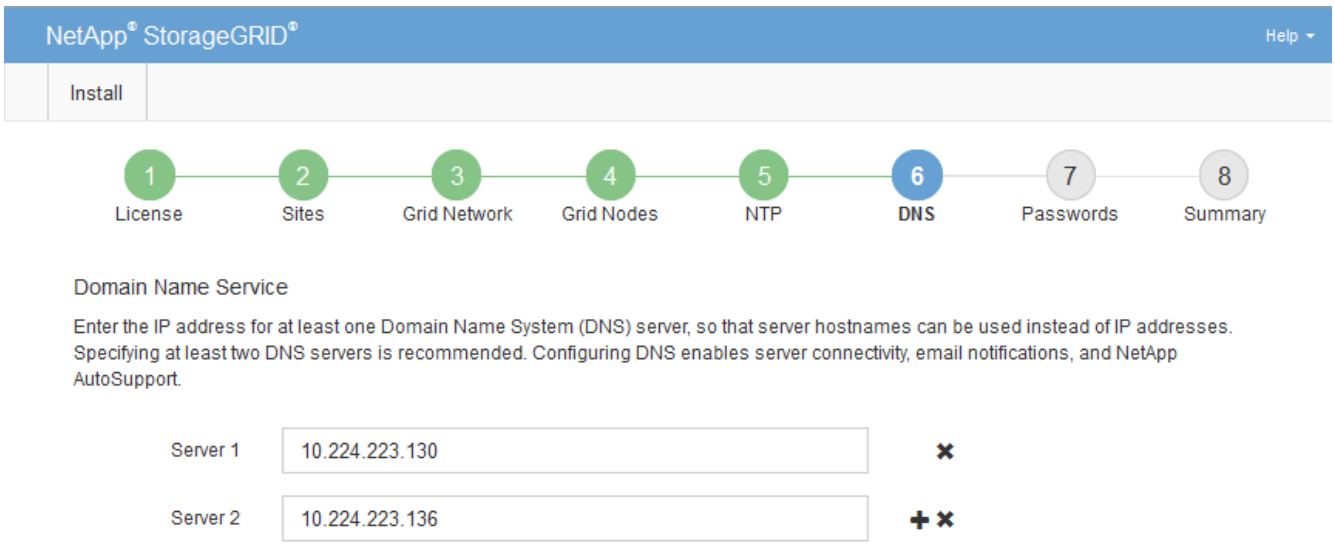
Para garantizar que el funcionamiento sea correcto, especifique dos o tres servidores DNS. Si especifica más de tres, es posible que solo se utilicen tres debido a las limitaciones conocidas del sistema operativo en algunas plataformas. Si tiene restricciones de enrutamiento en su entorno, puede "Personalice la lista de servidores DNS" Para nodos individuales (normalmente todos los nodos en un sitio) para usar un conjunto diferente de hasta tres servidores DNS.

Si es posible, utilice servidores DNS a los que cada sitio puede acceder localmente para asegurarse de que un sitio islandn pueda resolver los FQDN para destinos externos.

Si se omite o se configura incorrectamente la información del servidor DNS, se activa una alarma DNST en el servicio SSM de cada nodo de cuadrícula. La alarma se borra cuando DNS está configurado correctamente y la nueva información del servidor ha llegado a todos los nodos de la cuadrícula.

Pasos

1. Especifique la dirección IPv4 para al menos un servidor DNS en el cuadro de texto **servidor 1**.
2. Si es necesario, seleccione el signo más junto a la última entrada para agregar entradas adicionales del servidor.



La práctica recomendada es especificar al menos dos servidores DNS. Puede especificar hasta seis servidores DNS.

3. Seleccione **Siguiente**.

Especifique las contraseñas del sistema StorageGRID

Como parte de la instalación del sistema StorageGRID, debe introducir las contraseñas que se utilizarán para proteger el sistema y realizar tareas de mantenimiento.

Acerca de esta tarea

Utilice la página instalar contraseñas para especificar la contraseña de acceso de aprovisionamiento y la contraseña de usuario raíz de administración de grid.

- La clave de acceso de aprovisionamiento se usa como clave de cifrado y el sistema StorageGRID no la almacena.
- Debe disponer de la clave de acceso de aprovisionamiento para los procedimientos de instalación, ampliación y mantenimiento, incluida la descarga del paquete de recuperación. Por lo tanto, es importante almacenar la frase de contraseña de aprovisionamiento en una ubicación segura.
- Puede cambiar la frase de acceso de aprovisionamiento desde Grid Manager si tiene la actual.
- La contraseña de usuario raíz de gestión de grid se puede cambiar mediante Grid Manager.
- Las contraseñas de SSH y la consola de línea de comandos generadas aleatoriamente se almacenan en la `Passwords.txt` En el paquete de recuperación.

Pasos

1. En **Contraseña de aprovisionamiento**, ingrese la frase de contraseña de aprovisionamiento que será necesaria para realizar cambios en la topología de cuadrícula de su sistema StorageGRID.

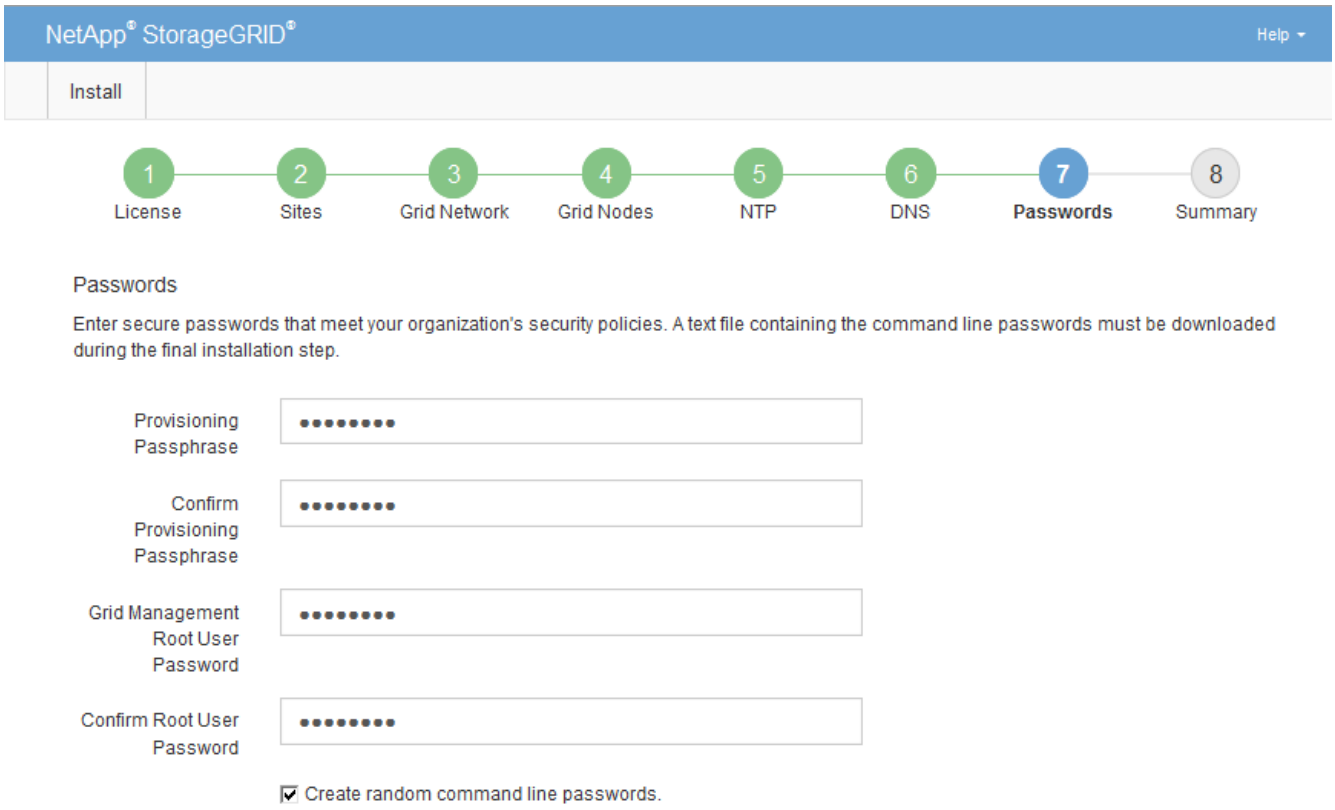
   Almacenar la clave de acceso de aprovisionamiento en un lugar seguro.

   > Si después de la instalación ha finalizado y desea cambiar la contraseña de acceso de aprovisionamiento más tarde, puede utilizar Grid Manager. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **contraseñas de cuadrícula**.

2. En **Confirmar la frase de paso de aprovisionamiento**, vuelva a introducir la contraseña de aprovisionamiento para confirmarla.
3. En **Grid Management Root User Password**, introduzca la contraseña que se utilizará para acceder a Grid Manager como usuario “root”.

   Guarde la contraseña en un lugar seguro.

4. En **Confirmar contraseña de usuario raíz**, vuelva a introducir la contraseña de Grid Manager para confirmarla.



5. Si va a instalar una cuadrícula con fines de prueba de concepto o demostración, opcionalmente desactive la casilla de verificación **Crear contraseñas de línea de comandos aleatorias**.

   En las implementaciones de producción, las contraseñas aleatorias deben utilizarse siempre por motivos de seguridad. Borrar **Crear contraseñas de línea de comandos aleatorias** solo para las cuadrículas de demostración si desea utilizar contraseñas predeterminadas para acceder a los nodos de la cuadrícula desde la línea de comandos usando la cuenta “root” o “admin”.

   > Se le solicitará que descargue el archivo del paquete de recuperación (`sgws-recovery-package-id-revision.zip`) Después de hacer clic en **instalar** en la página Resumen. Debe "descargue este archivo" para completar la instalación. Las contraseñas que se necesitan para acceder al sistema se almacenan en la `Passwords.txt` Archivo, incluido en el archivo del paquete de recuperación.

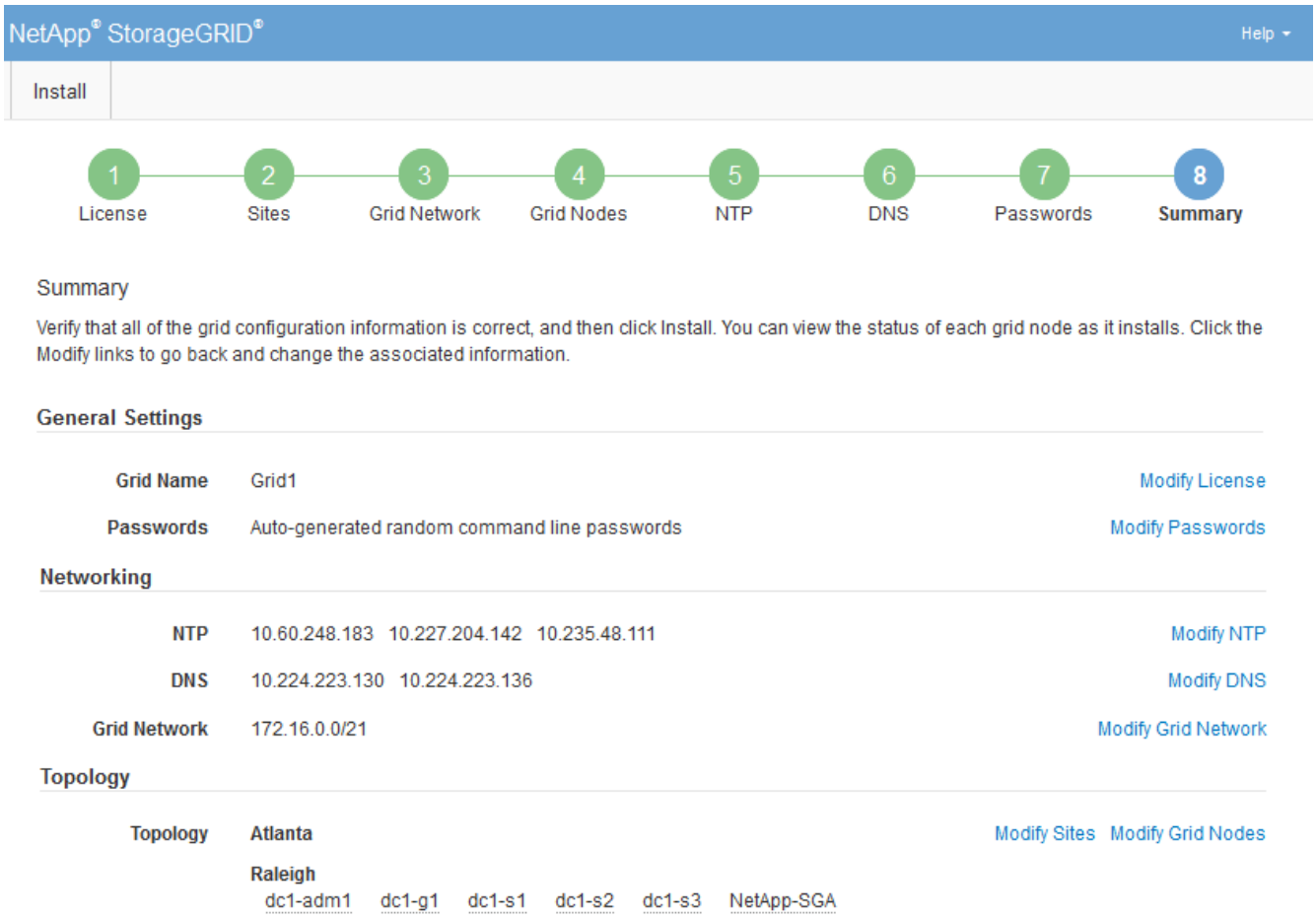
6. Haga clic en **Siguiente**.

Revise la configuración y complete la instalación

Debe revisar con cuidado la información de configuración que ha introducido para asegurarse de que la instalación se complete correctamente.

Pasos

1. Abra la página **Resumen**.



2. Verifique que toda la información de configuración de la cuadrícula sea correcta. Utilice los enlaces Modify de la página Summary para volver atrás y corregir los errores.
3. Haga clic en **instalar**.

> Si un nodo está configurado para utilizar la red de cliente, la puerta de enlace predeterminada para ese nodo cambia de la red de cuadrícula a la red de cliente cuando hace clic en **instalar**. Si se pierde la conectividad, debe asegurarse de acceder al nodo de administración principal a través de una subred accesible. Consulte "Directrices sobre redes" para obtener más detalles.

4. Haga clic en **Descargar paquete de recuperación**.

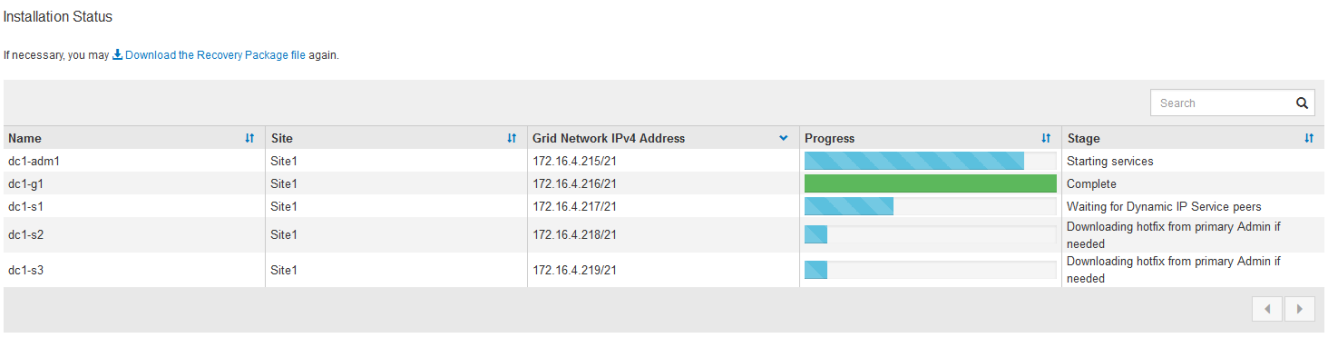
   Cuando la instalación avance hasta el punto en el que se define la topología de la cuadrícula, se le pedirá que descargue el archivo del paquete de recuperación (`.zip`), y confirme que puede obtener acceso al contenido de este archivo. Debe descargar el archivo de paquete de recuperación para que pueda recuperar el sistema StorageGRID si falla uno o más nodos de grid. La instalación continúa en segundo plano, pero no es posible completar la instalación y acceder al sistema StorageGRID hasta que se descargue y verifique este archivo.

5. Compruebe que puede extraer el contenido del `.zip` archivar y, a continuación, guardarlo en dos ubicaciones seguras, seguras e independientes.

> El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

6. Seleccione la casilla de verificación **He descargado y verificado correctamente el archivo del paquete de recuperación** y haga clic en **Siguiente**.

   Si la instalación sigue en curso, aparece la página de estado. Esta página indica el progreso de la instalación para cada nodo de cuadrícula.



   Cuando se llega a la fase completa de todos los nodos de cuadrícula, aparece la página de inicio de sesión de Grid Manager.

7. Inicie sesión en Grid Manager con el usuario "root" y la contraseña que especificó durante la instalación.

Directrices posteriores a la instalación

Después de completar la implementación y la configuración de un nodo de grid, siga estas directrices para el direccionamiento DHCP y los cambios de configuración de red.

- Si se utilizó DHCP para asignar direcciones IP, configure una reserva DHCP para cada dirección IP en las redes que se estén utilizando.

  DHCP solo puede configurarse durante la fase de implementación. No puede configurar DHCP durante la configuración.

  > Los nodos se reinician cuando cambian sus direcciones IP, lo que puede provocar interrupciones de servicio si un cambio de dirección DHCP afecta a varios nodos al mismo tiempo.

- Debe usar los procedimientos de cambio IP si desea cambiar direcciones IP, máscaras de subred y puertas de enlace predeterminadas para un nodo de grid. Consulte "Configurar las direcciones IP".
- Si realiza cambios de configuración de redes, incluidos los cambios de enrutamiento y puerta de enlace, es posible que se pierda la conectividad de cliente al nodo de administración principal y a otros nodos de grid. En función de los cambios de red aplicados, es posible que deba restablecer estas conexiones.

Información general de la instalación de la API de REST

StorageGRID proporciona la API de instalación de StorageGRID para realizar tareas de instalación.

La API utiliza la plataforma API de código abierto de Swagger para proporcionar la documentación de API. Swagger permite que tanto desarrolladores como no desarrolladores interactúen con la API en una interfaz de usuario que ilustra cómo responde la API a los parámetros y las opciones. En esta documentación se asume que está familiarizado con las tecnologías web estándar y el formato de datos JSON.

Cualquier operación de API que realice mediante la página web de documentos de API es una operación en directo. Tenga cuidado de no crear, actualizar o eliminar datos de configuración u otros datos por error.

Cada comando de API REST incluye la URL de la API, una acción HTTP, los parámetros de URL necesarios o opcionales y una respuesta de API esperada.

API de instalación de StorageGRID

La API de instalación de StorageGRID solo está disponible cuando está configurando inicialmente el sistema StorageGRID y si necesita realizar una recuperación de nodo de administración principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de la API, vaya a la página web de instalación en el nodo de administración principal y seleccione **Ayuda** > **Documentación de la API** en la barra de menús.

La API de instalación de StorageGRID incluye las siguientes secciones:

- **Config** — Operaciones relacionadas con la versión del producto y las versiones de la API. Puede mostrar la versión de la versión del producto y las versiones principales de la API que admite esa versión.
- **Grid** — Operaciones de configuración a nivel de cuadrícula. Puede obtener y actualizar la configuración de la cuadrícula, incluidos los detalles de la cuadrícula, las subredes de la red de cuadrícula, las contraseñas de la cuadrícula y las direcciones IP del servidor NTP y DNS.
- **Nodes** — Operaciones de configuración a nivel de nodo. Puede recuperar una lista de nodos de cuadrícula, eliminar un nodo de cuadrícula, configurar un nodo de cuadrícula, ver un nodo de cuadrícula y restablecer la configuración de un nodo de cuadrícula.
- **Aprovisionamiento** — Operaciones de aprovisionamiento. Puede iniciar la operación de aprovisionamiento y ver el estado de la operación de aprovisionamiento.
- **Recuperación** — Operaciones de recuperación del nodo de administración principal. Puede restablecer la información, cargar el paquete de recuperación, iniciar la recuperación y ver el estado de la operación de recuperación.
- **Paquete de recuperación** — Operaciones para descargar el paquete de recuperación.
- **Esquemas** — esquemas API para implementaciones avanzadas
- **Sites** — Operaciones de configuración a nivel de sitio. Puede crear, ver, eliminar y modificar un sitio.

A continuación, ¿dónde ir

Después de completar una instalación, realice las tareas de integración y configuración necesarias. Puede realizar las tareas opcionales según sea necesario.

Tareas requeridas

- Configure VMware vSphere Hypervisor para el reinicio automático.

  Debe configurar el hipervisor para reiniciar las máquinas virtuales cuando se reinicia el servidor. Sin el reinicio automático, las máquinas virtuales y los nodos de grid se mantienen apagados tras el reinicio del servidor. Para ver más detalles, consulte la documentación de VMware vSphere Hypervisor.

- "Cree una cuenta de inquilino" Para cada protocolo de cliente (Swift o S3) que se utilizará para almacenar objetos en el sistema StorageGRID.

- "Acceso al sistema de control" mediante la configuración de grupos y cuentas de usuario. Opcionalmente, puede hacerlo "configurar un origen de identidad federado" (Como Active Directory u OpenLDAP), para que pueda importar grupos y usuarios de administración. O bien, puede hacerlo "crear usuarios y grupos locales".
- Integre y pruebe el "S3 API" o. "API Swift" Aplicaciones cliente que utilizará para cargar objetos en el sistema StorageGRID.
- "Configure las reglas de gestión de la vida útil de la información (ILM) y la política de ILM" se desea utilizar para proteger los datos de objetos.
- Si la instalación incluye nodos de almacenamiento del dispositivo, utilice el sistema operativo SANtricity para realizar las siguientes tareas:
  - Conéctese a cada dispositivo StorageGRID.
  - Comprobar recepción de datos AutoSupport.

    Consulte "Configure el hardware".
- Revise y siga el "Directrices de fortalecimiento del sistema StorageGRID" eliminar los riesgos de seguridad.
- "Configure las notificaciones por correo electrónico para las alertas del sistema".
- Si el sistema StorageGRID incluye algún nodo de archivado (obsoleto), configure la conexión del nodo de archivado al sistema de almacenamiento de archivado externo de destino.

Tareas opcionales

- "Actualice las direcciones IP del nodo de grid" Si han cambiado desde que planificó el despliegue y generó el paquete de recuperación.
- "Configurar el cifrado del almacenamiento", si es necesario.
- "Configurar la compresión del almacenamiento" para reducir el tamaño de los objetos almacenados, si es necesario.

Solucionar problemas de instalación

Si se produce algún problema durante la instalación del sistema StorageGRID, puede acceder a los archivos de registro de la instalación.

A continuación se muestran los archivos de registro de la instalación principales, que el soporte técnico puede necesitar para resolver problemas.

- `/var/local/log/install.log` (se encuentra en todos los nodos de grid)
- `/var/local/log/gdu-server.log` (Encontrado en el nodo de administración principal)

Información relacionada

Para obtener información sobre cómo acceder a los archivos de registro, consulte "Referencia de archivos de registro".

Si necesita ayuda adicional, póngase en contacto con "Soporte de NetApp".

La reserva de recursos de la máquina virtual requiere ajustes

Los archivos OVF incluyen una reserva de recursos diseñada para garantizar que cada nodo de grid tiene suficiente RAM y CPU para funcionar de forma eficiente. Si crea máquinas virtuales mediante el despliegue de estos archivos OVF en VMware y el número predefinido de recursos no está disponible, las máquinas virtuales no se iniciarán.

Acerca de esta tarea

Si tiene la seguridad de que el host de máquina virtual tiene suficientes recursos para cada nodo de grid, ajuste manualmente los recursos asignados para cada máquina virtual e intente iniciar las máquinas virtuales.

Pasos

1. En el árbol del cliente del hipervisor de VMware vSphere, seleccione la máquina virtual que no se ha iniciado.
2. Haga clic con el botón secundario en la máquina virtual y seleccione **Editar configuración**.
3. En la ventana Propiedades de máquinas virtuales, seleccione la ficha **Recursos**.
4. Ajuste los recursos asignados a la máquina virtual:
   a. Seleccione **CPU** y, a continuación, utilice el control deslizante Reservación para ajustar el MHz reservado para esta máquina virtual.
   b. Seleccione **memoria** y, a continuación, utilice el control deslizante Reservación para ajustar el MB reservado para esta máquina virtual.
5. Haga clic en **Aceptar**.
6. Repita esto según sea necesario para otras máquinas virtuales alojadas en el mismo host de VM.

Se ha desactivado la contraseña de instalación temporal

Cuando se implementa un nodo VMware, puede especificar opcionalmente una contraseña de instalación temporal. Debe tener esta contraseña para acceder a la consola de la máquina virtual o utilizar SSH antes de que el nuevo nodo se una al grid.

Si optó por deshabilitar la contraseña de instalación temporal, debe realizar pasos adicionales para depurar los problemas de instalación.

Puede realizar una de las siguientes acciones:

- Vuelva a desplegar la máquina virtual, pero especifique una contraseña de instalación temporal para poder acceder a la consola o usar SSH para depurar los problemas de instalación.
- Use vCenter para establecer la contraseña:
  a. Vaya a **VM**, seleccione la pestaña **Configure** y seleccione **vApp Options**.
  b. Actualice **CUSTOM_TEMPORARY_PASSWORD** con el valor personalizado de la contraseña o actualice **TEMPORARY_PASSWORD_TYPE** con el valor **use node name**.
  c. Reinicie la máquina virtual para aplicar la nueva contraseña.

Actualice el software StorageGRID

Actualizar el software StorageGRID: Descripción general

Utilice estas instrucciones para actualizar un sistema StorageGRID a una nueva versión.

Acerca de estas instrucciones

Estas instrucciones describen las novedades de StorageGRID 11,8 y proporcionan instrucciones paso a paso para actualizar todos los nodos del sistema StorageGRID a la nueva versión.

Antes de empezar

Revise estos temas para saber más sobre las nuevas funciones y mejoras que se han aplicado en StorageGRID 11,8, determine si alguna función se ha obsoleto o se ha eliminado y obtenga información sobre los cambios en las API de StorageGRID.

- "Novedades de StorageGRID 11,8"
- "Operaciones eliminadas o obsoletas"
- "Cambios en la API de gestión de grid"
- "Cambios en la API de gestión de inquilinos"

Novedades en StorageGRID 11,8

Esta versión de StorageGRID introduce las siguientes funciones y cambios funcionales.

Instalar, actualizar, revisión

Contraseñas de instalación temporal

Cuando usted "Implemente un nodo de StorageGRID como una máquina virtual" O bien utilice VMware vSphere para "automatice la implementación de nodos de grid", ahora se le pedirá que establezca una contraseña de instalación temporal. Esta contraseña se usa únicamente si necesita acceder a la consola de la máquina virtual o usar SSH antes de que el nuevo nodo se una al grid.

Dispositivos

Sitio de documentación para dispositivos

La documentación de los dispositivos StorageGRID se movió a una nueva "sitio de documentación de los dispositivos".

Compatibilidad con FIPS

Compatibilidad con criptografía validada FIPS 140-2.

Mejoras de SGF6112

Compatibilidad con StorageGRID 11,8 y la versión 3.8.0 del firmware del instalador de dispositivos StorageGRID:

- Mejora significativa del rendimiento PUT para las nuevas instalaciones de SGF6112.
- Arranque seguro UEFI en los nodos SGF6112 actualizados y nuevos.
- Gestor de claves local para contraseñas de unidades DAS NVMe SSD.

Configurar y gestionar

Por defecto en toda la cuadrícula de consistencia

Puede cambiar el "consistencia predeterminada en toda la cuadrícula" Mediante Grid Manager o el punto final grid-config del "API privada de gestión de grid". El nuevo valor predeterminado se aplicará a los depósitos creados después del cambio.

Etiquetas de políticas de ILM

Permite controlar políticas de ILM por bloque mediante etiquetas de bloques. Se pueden crear varias políticas de ILM activas e inactivas al mismo tiempo. Consulte "Políticas de ILM:información general".

Puntos finales de Kafka

Compatibilidad con puntos finales de Kafka para "notificaciones de eventos de bloques".

Equilibrador de carga para el tráfico de interfaz de gestión

Cree extremos de equilibrio de carga para gestionar la carga de trabajo de la interfaz de gestión en los nodos de administración. Consulte "consideraciones que tener en cuenta al equilibrio de carga". Como parte de este cambio, ahora puede usar los puertos 443, 8443 y 9443 de Grid Manager y Tenant Manager al crear extremos de balanceador de carga HTTPS para el acceso de clientes S3 o Swift.

Pestaña Gestionar unidades

Añadido "Pestaña Gestionar unidades" Para el dispositivo SGF6112.

Nodos de almacenamiento solo de metadatos

Ahora puede especificar que sea nuevo "Nodo de almacenamiento basado en software" se utilizará para almacenar solo metadatos en lugar de objetos y metadatos.

SSO soporta nombres principales de usuario

Cuando "Configuración del inicio de sesión único (SSO)" Para el servicio de federación de Active Directory (AD FS) o PingFederate, ahora puede asignar el nombre principal de usuario a. `Name ID` en la regla de reclamaciones o a. `sAMAccountName=${username}` en la instancia del adaptador.

Configuración de políticas TLS y compatibilidad con KMIP

- StorageGRID ahora es compatible con el protocolo TLS 1,2 o TLS 1,3 para conexiones KMIP. Consulte "Consideraciones y requisitos para usar un servidor de gestión de claves".
- "Hashicorp ahora es totalmente compatible con KMIP".
- Se han realizado mejoras en "Configuración de la política TLS".

Expanda el grid, mantenga el grid, recupere o sustituya los nodos

Mejora del clon de la cuenta

Las cuentas existentes se pueden clonar en una cuadrícula remota. Consulte "Qué es el clon de cuenta".

Los nodos de archivo pueden decomisionarse

Ahora puede utilizar el procedimiento Nodos de retirada para eliminar los nodos de archivado no utilizados que estén desconectados de la cuadrícula. Consulte "Retirada de nodos de red desconectados".

Los nodos de archivado quedaron obsoletos en StorageGRID 11,7.

Restauración de volúmenes automática

Se añadió una conmutación para que la restauración de volúmenes se realizara automáticamente. Consulte "Restaurar datos de objetos con Grid Manager".

Código de borrado, cambios en la configuración y procedimiento de reequilibrio

Mejoras en las configuraciones de codificación de borrado.

Redistribuya fragmentos con código de borrado entre nodos de almacenamiento nuevos y existentes. Vuelva a calcular el saldo durante las tareas de mantenimiento para proporcionar una mejor distribución

cuando se completen las tareas. Consulte "Procedimiento de reequilibrio de código de borrado".

Seguimiento de la pila de API de gestión

La configuración de seguridad **Management API stack trace** te permite controlar si se devuelve un rastreo de pila en las respuestas de error de Grid Manager y Tenant Manager API. Consulte "Cambie la configuración de seguridad de la interfaz".

Procedimiento de reinicio progresivo

Ahora puede utilizar el "procedimiento de reinicio progresivo" para reiniciar varios nodos de grid sin provocar una interrupción del servicio.

Administrador de grid

Redes de clientes no confiables, información sobre puertos adicionales

La lista de puertos de Grid Manager abiertos a la red de clientes que no son de confianza se encuentra ahora en una columna denominada “Abrir a red de clientes que no son de confianza” en **CONFIGURACIÓN** > **Red** > **Puntos finales de equilibrio de carga** > **Interfaz de administración** (anteriormente ubicada en la página de control de Firewall). Consulte "Configurar puntos finales del equilibrador de carga".

Administrador de inquilinos

S3 Consola ya no experimental

Funcionalidad adicional descrita en "Utilice la consola S3".

Permiso de inquilino

La "permiso de gestión de inquilinos", Ver todos los cubos, se ha añadido.

API REST DE S3

- "Cambios en la compatibilidad con la API DE REST de S3".
- S3 Borrar marcadores con UUID. Consulte "Cómo se eliminan los objetos" y.. "SDEL: ELIMINACIÓN DE S3".
- "S3 Seleccione ScanRange" Se utiliza cuando se proporciona en las solicitudes de archivos CSV y de parquet.

Características y capacidades eliminadas o obsoletas

Algunas funciones y funcionalidades se eliminaron o quedaron obsoletas en esta versión. Revise estos elementos para saber si necesita actualizar las aplicaciones del cliente o modificar la configuración antes de realizar la actualización.

Definiciones

Anticuado

La característica *no debe ser usada en nuevos ambientes de producción. Los entornos de producción existentes pueden seguir utilizando la función.

Fin de la vida

Última versión enviada que contiene la función. Ninguna versión futura admitirá la función.

Quitada

Primera versión que **no** contiene la característica.

Compatibilidad con fin de la función StorageGRID 11,8

Las funciones obsoletas se eliminarán en las versiones principales N+2. Por ejemplo, si una característica está obsoleta en la versión N (por ejemplo, 6,3), la última versión en la que existirá la característica es N+1 (por ejemplo, 6,4). La versión N+2 (por ejemplo, 6,5) es la primera versión cuando la función no existe en el producto.

Consulte "Soporte de la versión del software" para obtener más información.

> En ciertas situaciones, NetApp podría terminar el soporte para determinadas funciones antes de lo indicado.

Función	Anticuado	Fin de la vida	Quitada
Soporte para nodos de archivado	11,7	11,8	11,9
Auditar la exportación a través de CIFS/Samba	11,1	11,6	11,7
Servicio CLB	11,4	11,6	11,7
Tiempo de ejecución del contenedor Docker	11,8	11,9	12,0
Exportación de auditoría NFS	11,8	11,9	12,0
Soporte para API Swift	11,7	11,9	12,0

Cambios en la API de gestión de grid

StorageGRID 11,8 utiliza la versión 4 de la API de administración de grid. La versión 4 deja de ser la versión 3; sin embargo, las versiones 1, 2 y 3 siguen siendo compatibles.

> Puede continuar utilizando versiones obsoletas de la API de gestión con StorageGRID 11,8; no obstante, la compatibilidad con estas versiones de la API se quitará en una futura versión de StorageGRID. Después de actualizar a StorageGRID 11,8, las API obsoletas se pueden desactivar mediante el `PUT /grid/config/management` API.

Para obtener más información, visite "Utilice la API de gestión de grid".

Cambios para `ilm-policies` API v4

Aplicación efectiva a partir de StorageGRID 11,8, versión 4 del `ilm-policies` API contiene las siguientes diferencias con respecto a la versión 3:

- Las políticas históricas ya no se devuelven. Se ha agregado una nueva API independiente para obtener datos históricos de políticas y etiquetas en `/grid/ilm-history`.

- Propiedades eliminadas: `proposed`, `historical`, `historicalRules`, `activationTime`.
- Propiedades agregadas: `active` (booleano), `activatedBy` (Matriz de UUID de etiqueta a la que está asignada la política).
- Parámetro de consulta de tipo opcional para `GET ilm-policies` ahora toma los valores `inactive` y.. `active`. Los valores anteriores eran `proposed`, `active`, y. `historical`.

Nuevos extremos para la gestión de unidades

Puede utilizar los puntos finales de la API **/grid/drive-details/{nodeId}** para realizar operaciones en las unidades en modelos específicos de nodos de almacenamiento del dispositivo.

Cambios en la API de gestión de inquilinos

StorageGRID 11,8 utiliza la versión 4 de la API de gestión de inquilinos. La versión 4 deja de ser la versión 3; sin embargo, las versiones 1, 2 y 3 siguen siendo compatibles.

> Puede continuar utilizando versiones obsoletas de la API de administración de inquilinos con StorageGRID 11,8; sin embargo, el soporte para estas versiones de la API se eliminará en una futura versión de StorageGRID. Después de actualizar a StorageGRID 11,8, las API obsoletas se pueden desactivar mediante el `PUT /grid/config/management` API.

Para obtener más información, visite "Conozca la API de gestión de inquilinos".

Nuevos extremos para etiquetas de políticas de ILM

Puede usar los extremos de la API **/org/ilm-policy-tags** y **/org/containers/{bucketName}/ilm-policy-tags** para realizar operaciones relacionadas con las etiquetas de política de ILM.

Planifique y prepare la actualización

Estime el tiempo para completar una actualización

Considere cuándo actualizarse, en función de la duración que pueda tardar la actualización. Tenga en cuenta qué operaciones se pueden realizar y qué no se pueden realizar en cada etapa de la actualización.

Acerca de esta tarea

El tiempo necesario para realizar una actualización de StorageGRID depende de diversos factores, como la carga del cliente y el rendimiento del hardware.

La tabla resume las tareas principales de actualización y enumera el tiempo aproximado necesario para cada tarea. Los pasos de la tabla proporcionan instrucciones que puede utilizar para estimar el tiempo de actualización del sistema.

Tarea de actualización	Descripción	Tiempo aproximado necesario	Durante esta tarea
Ejecute comprobaciones previas y actualice el nodo de administración principal	Se ejecutan las comprobaciones previas a la actualización y el nodo de administración principal se detiene, actualiza y reinicia.	De 30 minutos a 1 hora, con los nodos de las aplicaciones SG100 y SG1000 que requieren más tiempo. Los errores de comprobación previa no resueltos aumentarán esta vez.	No puede acceder al nodo de administración principal. Es posible que se notifiquen errores de conexión que puede ignorar. La ejecución de las comprobaciones previas de actualización antes de iniciar la actualización permite resolver cualquier error antes de la ventana de mantenimiento de actualización programada.
Inicie el servicio de actualización	Se distribuye el archivo de software y se inicia el servicio de actualización.	3 minutos por nodo de grid	
Actualice otros nodos de grid	Se actualiza el software de los demás nodos de grid, en el orden en el que se aprueban los nodos. Se desactivará cada nodo del sistema de uno en uno.	de 15 minutos a 1 hora por nodo, con nodos de los dispositivos que requieren más tiempo **Nota**: Para los nodos del dispositivo, el instalador del dispositivo StorageGRID se actualiza automáticamente a la última versión.	• No cambie la configuración de la cuadrícula. • No cambie la configuración del nivel de auditoría. • No actualice la configuración de ILM. • Se le impide realizar otros procedimientos de mantenimiento, como revisión, retirada o expansión. **Nota**: Si necesita realizar una recuperación, póngase en contacto con el soporte técnico.
Active las funciones	Se habilitan las nuevas funciones para la nueva versión.	Menos de 5 minutos	• No cambie la configuración de la cuadrícula. • No cambie la configuración del nivel de auditoría. • No actualice la configuración de ILM. • No puede realizar otro procedimiento de mantenimiento.

Tarea de actualización	Descripción	Tiempo aproximado necesario	Durante esta tarea
Actualizar la base de datos	El proceso de actualización comprueba cada nodo para verificar que no es necesario actualizar la base de datos de Cassandra.	10 segundos por nodo o unos minutos para todo el grid	La actualización de StorageGRID 11,7 a 11,8 no requiere una actualización de la base de datos Cassandra; sin embargo, el servicio Cassandra se detendrá y se reiniciará en cada nodo de almacenamiento. En las próximas versiones de la función StorageGRID, el paso de actualización de la base de datos de Cassandra podría tardar varios días en completarse.
Pasos de actualización finales	Se eliminan los archivos temporales y se completa la actualización a la versión nueva.	5 minutos	Cuando se complete la tarea **Pasos de actualización finales**, puede realizar todos los procedimientos de mantenimiento.

Pasos

1. Calcule el tiempo necesario para actualizar todos los nodos de grid.
   a. Multiplique el número de nodos en su sistema StorageGRID por 1 hora/nodo.

      Como regla general, los nodos de dispositivos tardan más en actualizarse que los nodos basados en software.

   b. Añada 1 hora a esta hora para tener en cuenta el tiempo necesario para descargar el `.upgrade` realice las comprobaciones previas y complete los pasos finales de actualización.
2. Si tiene nodos Linux, añada 15 minutos para cada nodo para tener en cuenta el tiempo necesario para descargar e instalar el paquete RPM o DEB.
3. Calcule el tiempo total estimado para la actualización agregando los resultados de los pasos 1 y 2.

Ejemplo: Tiempo estimado de actualización a StorageGRID 11,8

Supongamos que el sistema tiene 14 nodos de grid, de los cuales 8 son nodos Linux.

1. Multiplique 14 por 1 hora/nodo.
2. Añada 1 hora para tener en cuenta los pasos de descarga, comprobaciones previas y finales.

   El tiempo estimado para actualizar todos los nodos es de 15 horas.

3. Multiplique 8 por 15 minutos/node para tener en cuenta el tiempo que se tarda en instalar el paquete RPM o DEB en los nodos Linux.

   El tiempo estimado para este paso es de 2 horas.

4. Agregue los valores juntos.

   Debe esperar hasta 17 horas para completar la actualización del sistema a StorageGRID 11,8.0.

Según sea necesario, puede dividir la ventana de mantenimiento en ventanas más pequeñas aprobando subconjuntos de nodos de cuadrícula para actualizar en varias sesiones. Por ejemplo, quizás prefiera actualizar los nodos en el sitio A en una sesión y luego actualizar los nodos del sitio B en una sesión posterior. Si elige realizar la actualización en más de una sesión, tenga en cuenta que no podrá comenzar a usar las nuevas funciones hasta que se hayan actualizado todos los nodos.

Cómo se ve afectado el sistema durante la actualización

Conozca cómo se verá afectado su sistema StorageGRID durante la actualización.

Las actualizaciones de StorageGRID no son disruptivas

El sistema StorageGRID puede procesar y recuperar datos de las aplicaciones cliente durante el proceso de actualización. Si aprueba que se actualicen todos los nodos del mismo tipo (por ejemplo, Nodos de almacenamiento), los nodos se desactivan de uno en uno, por lo que no hay momento en que no estén disponibles todos los nodos de grid o todos los nodos de grid de un determinado tipo.

Para garantizar la disponibilidad continua, asegúrese de que su política de ILM contenga reglas que especifiquen el almacenamiento de varias copias de cada objeto. También debe asegurarse de que todos los clientes externos de S3 o Swift estén configurados para enviar solicitudes a una de las siguientes:

- Dirección IP virtual de grupo de alta disponibilidad
- Un equilibrador de carga de terceros de alta disponibilidad
- Múltiples nodos de puerta de enlace para cada cliente
- Varios nodos de almacenamiento para cada cliente

Las aplicaciones cliente pueden experimentar interrupciones a corto plazo

El sistema StorageGRID puede procesar y recuperar datos de las aplicaciones cliente durante el proceso de actualización; sin embargo, las conexiones de cliente a nodos de pasarela individuales o nodos de almacenamiento se pueden interrumpir temporalmente si la actualización necesita reiniciar los servicios de esos nodos. La conectividad se restaurará una vez que se complete el proceso de actualización y se reanuden los servicios en los nodos individuales.

Es posible que deba programar tiempos de inactividad para aplicar una actualización si no se acepta la pérdida de conectividad durante un período breve. Puede utilizar la aprobación selectiva para programar la actualización de determinados nodos.

Puede utilizar varias puertas de enlace y grupos de alta disponibilidad para proporcionar conmutación automática al respaldo durante el proceso de actualización. Consulte las instrucciones para "configuración de grupos de alta disponibilidad".

El firmware del dispositivo se ha actualizado

Durante la actualización de StorageGRID 11,8:

- Todos los nodos de dispositivos StorageGRID se actualizan automáticamente a la versión 3,8 del firmware del instalador de dispositivos StorageGRID.
- Los dispositivos SG6060 y SGF6024 se actualizan automáticamente a la versión de firmware del BIOS 3B07.EX y a la versión de firmware BMC 3.99.07.

- Los dispositivos SG100 y SG1000 se actualizan automáticamente a la versión de firmware del BIOS 3B12.EC y a la versión de firmware BMC 4.73.07.
- El dispositivo SGF6112 se actualiza automáticamente a la versión de firmware 3A10.QD del BIOS y a la versión 3.15.07 del firmware BMC.
- SGF6112 se convierte del modo de inicio heredado al modo de inicio UEFI con arranque seguro activado.

Las políticas de ILM se tratan de forma diferente según su estado

- La política activa seguirá siendo la misma después de la actualización.
- En la actualización, sólo se conservan las últimas 10 políticas históricas.
- Si hay una política propuesta, se eliminará durante la actualización.

Es posible que se activen alertas

Es posible que se activen alertas cuando se inician y se detienen los servicios y cuando el sistema StorageGRID funciona como un entorno de versiones mixtas (algunos nodos de grid que ejecutan una versión anterior, mientras que otros se han actualizado a una versión posterior). Es posible que se activen otras alertas una vez que se complete la actualización.

Por ejemplo, es posible que vea la alerta **No se puede comunicar con el nodo** cuando se detienen los servicios, o puede que vea la alerta **Error de comunicación de Cassandra** cuando algunos nodos se han actualizado a StorageGRID 11,8 pero otros nodos siguen ejecutando StorageGRID 11,7. En general, estas alertas se borran cuando se completa la actualización.

La alerta **ILM placement Unable** podría activarse cuando los nodos de almacenamiento se detienen durante la actualización a StorageGRID 11,8. Esta alerta podría persistir durante un día después de que se completa la actualización.

Una vez completada la actualización, puede revisar cualquier alerta relacionada con la actualización seleccionando **Alertas resueltas recientemente** o **Alertas actuales** desde el panel de control de Grid Manager.

Se generan muchas notificaciones SNMP

Tenga en cuenta que es posible que se genere un gran número de notificaciones SNMP cuando se detengan los nodos de grid y se reinician durante la actualización. Para evitar el exceso de notificaciones, desactive la casilla de verificación **Activar notificaciones de agente SNMP** (**CONFIGURACIÓN** > **Monitoreo** > **Agente SNMP**) para desactivar las notificaciones SNMP antes de iniciar la actualización. A continuación, vuelva a habilitar las notificaciones cuando finalice la actualización.

Los cambios de configuración están restringidos

> Esta lista se aplica específicamente a las actualizaciones de StorageGRID 11,7 a StorageGRID 11,8. Si va a actualizar a otra versión de StorageGRID, consulte la lista de cambios restringidos en las instrucciones de actualización para esa versión.

Hasta que finalice la tarea **Activar nueva función**:

- No realice ningún cambio en la configuración de la cuadrícula.
- No active ni desactive ninguna función nueva.
- No actualice la configuración de ILM. De lo contrario, es posible que experimente un comportamiento de ILM inconsistente e inesperado.

- No aplique una revisión ni recupere un nodo de grid.

> Si necesita recuperar un nodo durante la actualización, póngase en contacto con el soporte técnico.

- No debe gestionar grupos de alta disponibilidad, interfaces VLAN ni extremos de balanceador de carga mientras actualiza a StorageGRID 11,8.
- No elimine ningún grupo de alta disponibilidad hasta que haya finalizado la actualización a StorageGRID 11,8. Es posible que se vuelva inaccesible la dirección IP virtual en otros grupos de alta disponibilidad.

Hasta que finalice la tarea **pasos de actualización final**:

- No realice un procedimiento de expansión.
- No realice un procedimiento de decomiso.

No puede ver los detalles del depósito ni gestionar los depósitos desde el gestor de inquilinos

Durante la actualización a StorageGRID 11,8 (es decir, mientras el sistema funciona como un entorno de versión mixta), no se pueden ver los detalles de los bloques ni gestionar bloques mediante el Administrador de inquilinos. Aparece uno de los siguientes errores en la página Cuches del Administrador de inquilinos:

- No puedes usar esta API mientras actualizas a 11,8.
- No puede ver los detalles de las versiones de los bloques en el administrador de inquilinos mientras actualiza a 11,8.

Este error se resolverá después de que se complete la actualización a 11,8.

Solución alternativa

Mientras la actualización a 11,8 está en curso, utilice las siguientes herramientas para ver los detalles de los bloques o gestionar bloques, en lugar de utilizar el Gestor de inquilinos:

- Para realizar operaciones S3 estándar en un cucharón, utilice cualquiera de los "API REST DE S3" o la "API de gestión de inquilinos".
- Para realizar operaciones personalizadas de StorageGRID en un bloque (por ejemplo, ver y modificar la coherencia del bloque, habilitar o deshabilitar las actualizaciones de la hora del último acceso o configurar la integración de búsqueda), use la API de gestión de inquilinos.

Impacto de una actualización en grupos y cuentas de usuario

Es posible que tenga que actualizar los grupos y las cuentas de usuario de forma adecuada una vez finalizada la actualización.

Cambios en los permisos y opciones de grupo

Después de actualizar a StorageGRID 11,8, asigne opcionalmente los siguientes permisos nuevos a grupos de usuarios inquilinos.

Permiso	Descripción	Detalles
Ver todos los cubos	Permite a los usuarios ver todas las configuraciones de bloques y bloques.	El permiso Gestionar todos los cubos sustituye al permiso Ver todos los cubos.

Consulte "Permisos de gestión de inquilinos".

Comprobar la versión instalada de StorageGRID

Antes de iniciar la actualización, verifique que la versión anterior de StorageGRID esté actualmente instalada con la última revisión disponible aplicada.

Acerca de esta tarea

Antes de actualizar a StorageGRID 11,8, su grid debe tener instalado StorageGRID 11,7. Si actualmente está utilizando una versión anterior de StorageGRID, debe instalar todos los archivos de actualización anteriores junto con sus revisiones más recientes (muy recomendado) hasta que la versión actual de su grid sea StorageGRID 11,7.*x.y*.

En la 7 desde la versión 11,5,ejemplo.

> NetApp recomienda encarecidamente que aplique la revisión más reciente para cada versión de StorageGRID antes de actualizar a la siguiente versión y que también aplique la revisión más reciente para cada versión nueva que instale. En algunos casos, debe aplicar una revisión para evitar el riesgo de pérdida de datos. Consulte "Descargas de NetApp: StorageGRID" y las notas de la versión de cada revisión para obtener más información.

Pasos

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. En la parte superior de Grid Manager, seleccione **Ayuda** > **Acerca de**.
3. Verifique que **Version** es 11,7.*x.y*.

   En el número de versión de StorageGRID 11,7.*x.y*:

   - La versión **major** tiene un valor *x* de 0 (11,7.0).
   - Un **hotfix**, si se ha aplicado uno, tiene un valor *y* (por ejemplo, 11,7.0,1).
4. Si **Version** no es 11,7.*x.y*, vaya a. "Descargas de NetApp: StorageGRID" para descargar los archivos de cada versión anterior, incluida la revisión más reciente de cada versión.
5. Obtenga las instrucciones de actualización de cada versión descargada. A continuación, realice el procedimiento de actualización de software para esa versión y aplique la revisión más reciente para esa versión (recomendado expresamente).

   Consulte "Procedimiento de revisión de StorageGRID".

Ejemplo: Actualice a StorageGRID 11,7 desde la versión 11,5

El ejemplo siguiente muestra los pasos para actualizar de la versión 11,5 de StorageGRID a la versión 11,7 en la preparación para una actualización de StorageGRID 11,8.

Descargue e instale software en la siguiente secuencia para preparar el sistema para la actualización:

1. Aplique la última revisión de StorageGRID 11,5.0.*y*.
2. Actualice a la versión principal de StorageGRID 11.6.0.
3. Aplique la última revisión de StorageGRID 11,6.0.*y*.
4. Actualice a la versión principal de StorageGRID 11.7.0.

5. Aplique la última revisión de StorageGRID 11,7.0.*y*.

Obtenga los materiales necesarios para una actualización de software

Antes de comenzar la actualización de software, obtenga todos los materiales necesarios.

Elemento	Notas
Portátil de servicio	El portátil de servicio debe tener: • Puerto de red • Cliente SSH (por ejemplo, PuTTY)
"Navegador web compatible"	Normalmente, el navegador admite cambios para cada versión de StorageGRID. Asegúrese de que su navegador sea compatible con la nueva versión de StorageGRID.
Clave de acceso de aprovisionamiento	La frase de contraseña se crea y documenta cuando se instala el sistema StorageGRID por primera vez. La clave de acceso de aprovisionamiento no aparece en la `Passwords.txt` archivo.
Linux RPM o archivo DEB	Si alguno de los nodos se implementa en hosts Linux, debe "Descargue e instale el paquete RPM o DEB en todos los hosts" antes de iniciar la actualización. **Importante**: Asegúrese de que su sistema operativo esté actualizado al kernel 4,15 de Linux o superior.
Documentación de StorageGRID	• "Notas de la versión" Para StorageGRID 11,8 (es necesario iniciar sesión). Asegúrese de leerlos detenidamente antes de iniciar la actualización. • "Guía de resolución de actualización de software StorageGRID" para la versión principal a la que está actualizando (es necesario iniciar sesión) • Otros "Documentación de StorageGRID 11,8", según sea necesario.

Compruebe el estado del sistema

Antes de actualizar un sistema StorageGRID, verifique que el sistema esté listo para acomodar la actualización. Asegúrese de que el sistema funciona con normalidad y de que todos los nodos de grid funcionan.

Pasos

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Compruebe y resuelva cualquier alerta activa.
3. Confirme que no hay ninguna tarea de cuadrícula en conflicto activa ni pendiente.
   a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
   b. Seleccione ***site*** > ***primary Admin Node*** > **CMN** > **Grid Tasks** > **Configuration**.

Las tareas de evaluación de la gestión del ciclo de vida de la información (ILME) son las únicas tareas de la cuadrícula que se pueden ejecutar simultáneamente con la actualización del software.

c. Si hay otras tareas de cuadrícula activas o pendientes, espere a que finalicen o liberen el bloqueo.

> Póngase en contacto con el soporte técnico si una tarea no finaliza o libera el bloqueo.

4. Consulte "Comunicaciones internas de los nodos de grid" y.. "Comunicaciones externas" Para asegurarse de que todos los puertos requeridos para StorageGRID 11,8 se abren antes de la actualización.

> No son necesarios puertos adicionales para actualizar a StorageGRID 11,8.

El siguiente puerto requerido fue agregado en StorageGRID 11,7. Asegúrese de que está disponible antes de actualizar a StorageGRID 11,8.

Puerto	Descripción
18086	Puerto TCP utilizado para las solicitudes S3 del equilibrador de carga de StorageGRID a LDR y el nuevo servicio LDR. Antes de la actualización, confirme que este puerto está abierto desde todos los nodos de cuadrícula a todos los nodos de almacenamiento. El bloqueo de este puerto provocará S3 interrupciones de servicio después de la actualización a StorageGRID 11,8.

> Si ha abierto algún puerto de firewall personalizado, se le notificará durante las comprobaciones previas de la actualización. Debe comunicarse con el soporte técnico antes de continuar con la actualización.

Actualizar el software de

Inicio rápido de la actualización

Antes de iniciar la actualización, revise el flujo de trabajo general. La página de actualización de StorageGRID le guiará en cada paso de actualización.

1 Prepare los hosts Linux

Si se pone en marcha algún nodo StorageGRID en hosts Linux, "Instale el paquete RPM o DEB en cada host" antes de iniciar la actualización.

2 Cargue archivos de actualización y correcciones urgentes

Desde el nodo de administración principal, acceda a la página Actualización de StorageGRID y cargue el archivo de actualización y el archivo de revisión, si es necesario.

3 Descargue el paquete de recuperación

Descargue el paquete de recuperación actual antes de iniciar la actualización.

4 Ejecute las comprobaciones previas a la actualización

Las comprobaciones previas de actualización ayudan a detectar problemas para que pueda resolverlos antes de iniciar la actualización real.

5 Inicie la actualización

Cuando inicia la actualización, las comprobaciones previas se ejecutan de nuevo y el nodo de administración principal se actualiza automáticamente. No puede acceder a Grid Manager mientras se está actualizando el nodo de administración principal. Además, los registros de auditoría no estarán disponibles. Esta actualización puede llevar hasta 30 minutos.

6 Descargue el paquete de recuperación

Después de actualizar el nodo de administración principal, descargue un nuevo paquete de recuperación.

7 Aprobar nodos

Puede aprobar nodos de cuadrícula individuales, grupos de nodos de cuadrícula o todos los nodos de cuadrícula.

> ⚠ No apruebe la actualización para un nodo de grid a menos que esté seguro de que el nodo está listo para detenerse y reiniciarse.

8 Reanudar las operaciones

Una vez que se han actualizado todos los nodos de grid, se habilitan las nuevas funciones para que se puedan reanudar las operaciones. Debe esperar para realizar un procedimiento de retirada o expansión hasta que la tarea en segundo plano **Upgrade database** y la tarea **Final upgrade steps** se hayan completado.

Información relacionada

"Estime el tiempo para completar una actualización"

Linux: Descargue e instale el paquete RPM o DEB en todos los hosts

Si hay algún nodo de StorageGRID implementado en hosts Linux, descargue e instale un paquete RPM o DEB adicional en cada uno de estos hosts antes de iniciar la actualización.

Descargue archivos de actualización, Linux y correcciones urgentes

Cuando realiza una actualización de StorageGRID desde Grid Manager, se le pedirá que descargue el archivo de actualización y cualquier revisión necesaria como primer paso. Sin embargo, si necesita descargar archivos para actualizar los hosts de Linux, puede ahorrar tiempo descargando todos los archivos necesarios

con antelación.

Pasos

1. Vaya a. "Descargas de NetApp: StorageGRID".
2. Seleccione el botón para descargar la última versión, o seleccione otra versión en el menú desplegable y seleccione **Ir**.

   Las versiones de software de StorageGRID tienen este formato: 11.*x.y*. Las revisiones StorageGRID tienen este formato: 11.*x. y.z*.

3. Inicie sesión con el nombre de usuario y la contraseña de su cuenta de NetApp.
4. Si aparece un aviso de Precaución/Lectura, tome nota del número de revisión y seleccione la casilla de verificación.
5. Lea el Contrato de licencia de usuario final, seleccione la casilla de verificación y, a continuación, seleccione * Aceptar y continuar *.

   Aparece la página de descargas de la versión seleccionada. La página contiene tres columnas.

6. Desde la segunda columna (**Upgrade StorageGRID**), descargue dos archivos:
   - El archivo de actualización para la última versión (este es el archivo en la sección etiquetada como **VMware, SG1000, o SG100 Primary Admin Node**). Si bien este archivo no es necesario hasta que realice la actualización, descargarlo ahora ahorrará tiempo.
   - Un archivo RPM o DEB en cualquiera de los dos `.tgz` o. `.zip` formato. Seleccione la `.zip` Archivo si está ejecutando Windows en el portátil de servicio.
     - Red Hat Enterprise Linux
       `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
       `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
     - Ubuntu o Debian
       `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`
       `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`
7. Si necesita aceptar un aviso de Precaución/MustRead debido a una revisión requerida, descargue la revisión:
   a. Vuelva a. "Descargas de NetApp: StorageGRID".
   b. Seleccione el número de revisión en la lista desplegable.
   c. Acepte de nuevo el aviso de precaución y el EULA.
   d. Descargue y guarde la revisión y su README.

      Se le pedirá que cargue el archivo de revisión en la página de actualización de StorageGRID cuando inicie la actualización.

Instale el archivo en todos los hosts Linux

Realice estos pasos antes de actualizar el software StorageGRID.

Pasos

1. Extraiga los paquetes RPM o DEB del archivo de instalación.
2. Instale los paquetes RPM o DEB en todos los hosts Linux.

Consulte los pasos para instalar servicios de host StorageGRID en las instrucciones de instalación:

- "Red Hat Enterprise Linux: Instale los servicios de host de StorageGRID"
- "Ubuntu o Debian: Instalar los servicios de host de StorageGRID"

Los nuevos paquetes se instalan como paquetes adicionales. No elimine los paquetes existentes.

Realice la actualización

Puede actualizar a StorageGRID 11,8 y aplicar la revisión más reciente para esa versión al mismo tiempo. La página de actualización de StorageGRID proporciona la ruta de actualización recomendada y enlaza directamente a las páginas de descarga correctas.

Antes de empezar

Ha revisado todas las consideraciones y completado todos los pasos de planificación y preparación.

Acceda a la página Actualización de StorageGRID

Como primer paso, acceda a la página Actualización de StorageGRID en Grid Manager.

Pasos

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Seleccione **MANTENIMIENTO** > **sistema** > **actualización de software**.
3. En el mosaico de actualización de StorageGRID, seleccione **Actualizar**.

Seleccione los archivos

La ruta de actualización de la página Actualización de StorageGRID indica las versiones principales (por ejemplo, 11,8.0) y las revisiones (por ejemplo, 11,8.0,1) que debe instalar para obtener la versión más reciente de StorageGRID. Debe instalar las versiones recomendadas y las revisiones en el orden que se muestra.

Si no se muestra ninguna ruta de actualización, es posible que su navegador no pueda acceder al sitio de soporte de NetApp o que se deshabilite la casilla de comprobación **Comprobar actualizaciones de software** de la página AutoSupport (**SUPPORT** > **Herramientas** > **AutoSupport**).

Pasos

1. Para el paso **Seleccionar archivos**, revise la ruta de actualización.
2. En la sección Descargar archivos, seleccione cada enlace de **Descargar** para descargar los archivos requeridos del sitio de soporte de NetApp.

   Si no se muestra ninguna ruta de actualización, vaya al "Descargas de NetApp: StorageGRID" para determinar si hay una nueva versión o revisión disponible y para descargar los archivos que necesita.

   Si necesitaba descargar e instalar un paquete RPM o DEB en todos los hosts Linux, es posible que ya tenga los archivos de actualización y correcciones urgentes de StorageGRID enumerados en la ruta de actualización.

3. Seleccione **Examinar** para cargar el archivo de actualización de la versión en StorageGRID: `NetApp_StorageGRID_11.8.0_Software_uniqueID.upgrade`

Cuando se realiza el proceso de carga y validación, aparece una marca de verificación verde junto al nombre del archivo.

4. Si descargó un archivo de revisión, seleccione **Examinar** para cargar ese archivo. La revisión se aplicará automáticamente como parte de la actualización de la versión.
5. Seleccione **continuar**.

Realice comprobaciones previas

Ejecutar comprobaciones previas le permite detectar y resolver cualquier problema de actualización antes de empezar a actualizar su grid.

Pasos

1. Para el paso **Ejecutar comprobaciones previas**, comience introduciendo la frase de acceso de aprovisionamiento para su cuadrícula.
2. Seleccione **Descargar paquete de recuperación**.

   Debe descargar la copia actual del archivo del paquete de recuperación antes de actualizar el nodo de administración principal. El archivo de paquete de recuperación permite restaurar el sistema si se produce un fallo.

3. Cuando se descargue el archivo, confirme que puede acceder al contenido, incluido el `Passwords.txt` archivo.
4. Copie el archivo descargado (`.zip`) a dos ubicaciones seguras, seguras y separadas.

   > El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

5. Seleccione **Ejecutar comprobaciones previas** y espere a que se completen las comprobaciones previas.
6. Revise los detalles de cada comprobación previa informada y resuelva los errores notificados. Consulte "Guía de resolución de actualización de software StorageGRID" Para el lanzamiento de StorageGRID 11,8.

   Debe resolver todas las comprobaciones previas *ERRORES* antes de actualizar el sistema. Sin embargo, no es necesario abordar la comprobación previa *WARNINGS* antes de actualizar.

   > Si ha abierto algún puerto de firewall personalizado, se le notificará durante la validación de las comprobaciones previas. Debe comunicarse con el soporte técnico antes de continuar con la actualización.

7. Si ha realizado algún cambio en la configuración para resolver los problemas notificados, seleccione **Ejecutar comprobaciones previas** de nuevo para obtener resultados actualizados.

   Si se han resuelto todos los errores, se le solicitará que inicie la actualización.

Inicie la actualización y actualice el nodo de administración principal

Cuando inicia la actualización, las comprobaciones previas a la actualización se vuelven a ejecutar y el nodo de administración primario se actualiza automáticamente. Esta parte de la actualización puede tardar hasta 30 minutos.

No podrá acceder a ninguna otra página de Grid Manager mientras se esté actualizando el nodo de administración principal. Además, los registros de auditoría no estarán disponibles.

Pasos

1. Seleccione **Iniciar actualización**.

   Aparecerá una advertencia para recordarle que perderá temporalmente el acceso a Grid Manager.

2. Seleccione **OK** para confirmar la advertencia e iniciar la actualización.
3. Espere a que se realicen las comprobaciones previas de actualización y a que se actualice el nodo de administrador principal.

   Si se notifica algún error de comprobación previa, soluciónelo y seleccione **Iniciar actualización** de nuevo.

   Si el grid tiene otro nodo de administración que está en línea y listo, puede utilizarlo para supervisar el estado del nodo de administración principal. En cuanto se actualice el nodo de administración principal, puede aprobar los otros nodos de grid.

4. Según sea necesario, seleccione **Continuar** para acceder al paso **Actualizar otros nodos**.

Actualice otros nodos

Es necesario actualizar todos los nodos de grid, pero es posible realizar varias sesiones de actualización y personalizar la secuencia de actualización. Por ejemplo, quizás prefiera actualizar los nodos en el sitio A en una sesión y luego actualizar los nodos del sitio B en una sesión posterior. Si elige realizar la actualización en más de una sesión, tenga en cuenta que no podrá comenzar a usar las nuevas funciones hasta que se hayan actualizado todos los nodos.

Si el orden en el que se actualizan los nodos es importante, apruebe los nodos o grupos de nodos de uno en uno y espere a que la actualización se complete en cada nodo antes de aprobar el siguiente nodo o grupo de nodos.

Cuando la actualización se inicia en un nodo de grid, los servicios de ese nodo se detienen. Más tarde, el nodo de grid se reinicia. Para evitar interrupciones del servicio para las aplicaciones cliente que se comunican con el nodo, no apruebe la actualización de un nodo a menos que esté seguro de que el nodo está listo para detenerse y reiniciarse. Según sea necesario, programe una ventana de mantenimiento o notifique a los clientes.

Pasos

1. Para el paso **Actualizar otros nodos**, revise el Resumen, que proporciona la hora de inicio de la actualización en su conjunto y el estado de cada tarea de actualización principal.
   - **Start upgrade service** es la primera tarea de actualización. Durante esta tarea, el archivo de software se distribuye a los nodos de grid y el servicio de actualización se inicia en cada nodo.
   - Cuando se complete la tarea **Iniciar servicio de actualización**, se iniciará la tarea **Actualizar otros nodos de grid** y se le pedirá que descargue una nueva copia del Paquete de recuperación.
2. Cuando se le solicite, introduzca la frase de contraseña de aprovisionamiento y descargue una nueva copia del paquete de recuperación.

Debe descargar una nueva copia del archivo del paquete de recuperación después de actualizar el nodo de administración principal. El archivo de paquete de recuperación permite restaurar el sistema si se produce un fallo.

3. Revise las tablas de estado para cada tipo de nodo. Hay tablas para nodos de administración no principales, nodos de puerta de enlace, nodos de almacenamiento y nodos de archivado.

   Un nodo de cuadrícula puede estar en una de estas etapas cuando aparecen las tablas por primera vez:

   - Desembalaje de la actualización
   - Descarga
   - En espera de ser aprobado

4. Cuando esté listo para seleccionar nodos de cuadrícula para la actualización (o si necesita anular la aprobación de los nodos seleccionados), siga estas instrucciones:

Tarea	Instrucción
Busque nodos específicos para aprobar, como todos los nodos de un sitio concreto	Introduzca la cadena de búsqueda en el campo **Search**
Seleccione todos los nodos para actualizar	Seleccione **Aprobar todos los nodos**
Seleccione todos los nodos del mismo tipo para la actualización (por ejemplo, todos los nodos de almacenamiento)	Seleccione el botón **Aprobar todo** para el tipo de nodo Si aprueba más de un nodo del mismo tipo, los nodos se actualizarán de uno en uno.
Seleccione un nodo individual para actualizar	Seleccione el botón **Aprobar** para el nodo
Posponga la actualización en todos los nodos seleccionados	Seleccione **Unapprove all nodes**
Posponga la actualización en todos los nodos seleccionados del mismo tipo	Seleccione el botón **Unapprove All** para el tipo de nodo
Posponga la actualización en un nodo individual	Seleccione el botón **Unapprove** para el nodo

5. Espere a que los nodos aprobados continúen por estas etapas de actualización:
   - Aprobado y a la espera de actualización
   - Deteniendo servicios

     No se puede eliminar un nodo cuando su etapa alcanza **parando servicios**. El botón **Unapprove** está desactivado.

   - Parando contenedor
   - Limpieza de imágenes de Docker

- Actualizando paquetes de SO base

> Cuando un nodo de dispositivo llega a esta etapa, se actualiza el software del instalador de dispositivos StorageGRID del dispositivo. Este proceso automatizado garantiza que la versión del instalador de dispositivos StorageGRID permanezca sincronizada con la versión del software StorageGRID.

- Reiniciando

> Es posible que algunos modelos de dispositivos se reinicien varias veces para actualizar el firmware y el BIOS.

- Realizando pasos después del reinicio
- Iniciando servicios
- Listo

6. Repita el paso de aprobación tantas veces como sea necesario hasta que se hayan actualizado todos los nodos de grid.

Se completó la actualización

Cuando todos los nodos de grid han completado las etapas de actualización, la tarea **Actualizar otros nodos de grid** se muestra como completada. Las tareas de actualización restantes se ejecutan automáticamente en segundo plano.

Pasos

1. Tan pronto como se complete la tarea **Habilitar funciones** (que ocurre rápidamente), puede comenzar a usar el "otras nuevas" En la versión actualizada de StorageGRID.
2. Durante la tarea **Upgrade database**, el proceso de actualización comprueba cada nodo para verificar que la base de datos Cassandra no necesita ser actualizada.

> La actualización de StorageGRID 11,7 a 11,8 no requiere una actualización de la base de datos Cassandra; sin embargo, el servicio Cassandra se detendrá y se reiniciará en cada nodo de almacenamiento. En las próximas versiones de la función StorageGRID, el paso de actualización de la base de datos de Cassandra podría tardar varios días en completarse.

3. Cuando la tarea **Upgrade database** se haya completado, espere unos minutos hasta que se completen los pasos **Final upgrade**.
4. Cuando se hayan completado los **Pasos de actualización finales**, la actualización se realizará. El primer paso, **Seleccionar archivos**, se vuelve a mostrar con un banner de éxito verde.
5. Compruebe que las operaciones de grid se han vuelto a la normalidad:
   a. Compruebe que los servicios funcionan con normalidad y que no hay alertas inesperadas.
   b. Confirmar que las conexiones de los clientes con el sistema StorageGRID funcionan tal como se espera.

Solucione problemas de actualización

Si algo sale mal al realizar una actualización, es posible que pueda resolver el problema usted mismo. Si no se puede resolver un problema, recopile toda la información posible y

póngase en contacto con el soporte técnico.

No se completó la actualización

Las secciones siguientes describen cómo recuperar de situaciones en las que la actualización ha fallado parcialmente.

Errores de las comprobaciones previas de actualización

Para detectar y resolver problemas, puede ejecutar manualmente las comprobaciones previas de la actualización antes de iniciar la actualización real. La mayoría de los errores de las comprobaciones previas proporcionan información sobre cómo resolver el problema.

Errores de aprovisionamiento

Si el proceso de aprovisionamiento automático falla, póngase en contacto con el soporte técnico.

El nodo de grid se bloquea o no puede iniciarse

Si un nodo de grid se bloquea durante el proceso de actualización o no puede iniciarse correctamente después de que se complete la actualización, póngase en contacto con el soporte técnico para investigar y corregir cualquier problema subyacente.

La ingesta o la recuperación de datos se interrumpe

Si la ingesta o la recuperación de datos se interrumpen inesperadamente si no actualiza un nodo de grid, póngase en contacto con el soporte técnico.

Errores de actualización de base de datos

Si se produce un error en la actualización de la base de datos, vuelva a intentar la actualización. Si vuelve a fallar, póngase en contacto con el soporte técnico de.

Información relacionada

"Comprobación del estado del sistema antes de actualizar el software"

Problemas de la interfaz de usuario

Es posible que tenga problemas con Grid Manager o el administrador de inquilinos durante o después de la actualización.

Grid Manager muestra varios mensajes de error durante la actualización

Si actualiza el explorador o navega a otra página de Grid Manager mientras se está actualizando el nodo de administración principal, es posible que vea varios mensajes de tipo «503: Service unavailable» y «Problema de conexión con el servidor». Puede ignorar con seguridad estos mensajes; dejarán de aparecer pronto cuando se actualice el nodo.

Si estos mensajes aparecen durante más de una hora después de iniciar la actualización, podría haber ocurrido algo que impidiera que se actualizara el nodo de administración principal. Si no puede resolver el problema por su cuenta, póngase en contacto con el soporte técnico.

La interfaz Web no responde de la manera esperada

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

Si tiene problemas con la interfaz web:

- Asegúrese de utilizar un "navegador web compatible".

  Normalmente, el navegador admite cambios para cada versión de StorageGRID.

- 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.

Mensajes de error de comprobación de disponibilidad de imagen Docker

Al intentar iniciar el proceso de actualización, es posible que reciba un mensaje de error que indica que la suite de validación de comprobación de disponibilidad de imágenes de Docker identificó los siguientes problemas. Todos los problemas deben resolverse antes de completar la actualización.

Póngase en contacto con el soporte técnico si no está seguro de los cambios necesarios para resolver los problemas identificados.

Mensaje	Causa	Solución
No se puede determinar la versión de actualización. Actualizar el archivo de información de la versión `{file_path}` no coincide con el formato esperado.	El paquete de actualización está dañado.	Vuelva a cargar el paquete de actualización e inténtelo de nuevo. Si el problema persiste, póngase en contacto con el soporte técnico.
Actualizar el archivo de información de la versión `{file_path}` no se ha encontrado. No se puede determinar la versión de actualización.	El paquete de actualización está dañado.	Vuelva a cargar el paquete de actualización e inténtelo de nuevo. Si el problema persiste, póngase en contacto con el soporte técnico.
No se puede determinar la versión instalada actualmente en `{node_name}`.	Un archivo crítico del nodo está dañado.	Póngase en contacto con el soporte técnico.
Error de conexión al intentar mostrar las versiones `{node_name}`	El nodo está desconectado o la conexión se ha interrumpido.	Compruebe que todos los nodos estén en línea y sean accesibles desde el nodo administrador principal, y vuelva a intentarlo.

Mensaje	Causa	Solución
El host para nodo `{node_name}` No tiene StorageGRID `{upgrade_version}` imagen cargada. Las imágenes y los servicios deben instalarse en el host para poder continuar con la actualización.	Los paquetes RPM o DEB para la actualización no se han instalado en el host donde se está ejecutando el nodo o las imágenes siguen en proceso de importación. **Nota:** este error sólo se aplica a los nodos que se ejecutan como contenedores en Linux.	Compruebe que se hayan instalado los paquetes RPM o DEB en todos los hosts Linux en los que se estén ejecutando los nodos. Asegúrese de que la versión es correcta tanto para el servicio como para el archivo de imágenes. Espere unos minutos e inténtelo de nuevo. Consulte "Linux: Instale el paquete RPM o DEB en todos los hosts".
Error al comprobar el nodo `{node_name}`	Error inesperado.	Espere unos minutos e inténtelo de nuevo.
Error no detectado mientras se ejecutan las comprobaciones previas. `{error_string}`	Error inesperado.	Espere unos minutos e inténtelo de nuevo.

Aplique la revisión de StorageGRID

Procedimiento de revisión de StorageGRID: Descripción general

Es posible que deba aplicar una revisión a su sistema StorageGRID si se detectan y resuelven problemas con el software entre versiones de funciones.

Las correcciones urgentes de StorageGRID contienen cambios de software que se pueden hacer disponibles fuera de una función o una versión de revisión. Los mismos cambios se incluyen en una versión futura. Además, cada versión de revisión contiene un resumen de todas las revisiones previas dentro de la característica o versión de revisión.

Consideraciones para aplicar una revisión

No puede aplicar una revisión de StorageGRID cuando se está ejecutando otro procedimiento de mantenimiento. Por ejemplo, no se puede aplicar una revisión mientras se está ejecutando un procedimiento de decomiso, expansión o recuperación.

> Si un procedimiento de retirada de nodo o sitio está en pausa, puede aplicar una revisión de forma segura. Además, puede ser capaz de aplicar una revisión durante las fases finales de un procedimiento de actualización de StorageGRID. Consulte las instrucciones para actualizar el software StorageGRID para obtener detalles.

Después de cargar la revisión en Grid Manager, la revisión se aplica automáticamente al nodo de administración principal. A continuación, puede aprobar la aplicación de la revisión al resto de los nodos del sistema StorageGRID.

Si una revisión no se puede aplicar a uno o más nodos, el motivo del error aparece en la columna Detalles de la tabla de progreso de la revisión. Debe resolver los problemas que causaron los fallos y luego volver a intentar todo el proceso. Los nodos con una aplicación de la revisión realizada con éxito anteriormente se

omitirán en aplicaciones posteriores. Puede volver a intentar de forma segura el proceso de revisión tantas veces como sea necesario hasta que todos los nodos se hayan actualizado. La revisión debe instalarse correctamente en todos los nodos de cuadrícula para que la aplicación se complete.

Mientras los nodos de cuadrícula se actualizan con la nueva versión de revisión, los cambios reales en una revisión sólo pueden afectar a servicios específicos en tipos de nodos específicos. Por ejemplo, una revisión sólo podría afectar al servicio LDR en nodos de almacenamiento.

Cómo se aplican las revisiones para la recuperación y expansión

Después de que se haya aplicado una revisión a la cuadrícula, el nodo de administración principal instala automáticamente la misma versión de revisión en los nodos restaurados por operaciones de recuperación o agregados en una expansión.

Sin embargo, si necesita recuperar el nodo de administración principal, debe instalar manualmente la versión de StorageGRID correcta y, a continuación, aplicar la revisión. La versión final de StorageGRID del nodo de administrador principal debe coincidir con la versión de los otros nodos de la cuadrícula.

En el ejemplo siguiente se ilustra cómo aplicar una revisión al recuperar el nodo de administración principal:

1. Suponga que la cuadrícula está ejecutando una versión de StorageGRID 11.*A.B* con la revisión más reciente. La “versión de cuadrícula” es 11.*A.B.y*.
2. Se produce un error en el nodo del administrador principal.
3. Vuelva a poner en marcha el nodo de administración principal con StorageGRID 11.*A.B* y realice el procedimiento de recuperación.

> Como es necesario para que coincida con la versión de grid, puede utilizar una versión inferior al poner en marcha el nodo, no es necesario poner en marcha primero la versión principal.

4. A continuación, aplica la revisión 11.*A.B.y* al nodo de administración principal.

Para obtener más información, consulte "Configure el nodo de administración principal de reemplazo".

Cómo se ve afectado el sistema cuando se aplica una revisión

Debe entender cómo se verá afectado su sistema StorageGRID al aplicar una revisión.

Las correcciones urgentes de StorageGRID no son disruptivas

El sistema StorageGRID puede procesar y recuperar datos de las aplicaciones cliente durante el proceso de revisión. Si aprueba todos los nodos del mismo tipo a la revisión (por ejemplo, Nodos de almacenamiento), los nodos se desactivan de uno en uno, por lo que no hay momento en que no estén disponibles todos los nodos de grid o todos los nodos de grid de un determinado tipo.

Para garantizar la disponibilidad continua, asegúrese de que su política de ILM contenga reglas que especifiquen el almacenamiento de varias copias de cada objeto. También debe asegurarse de que todos los clientes externos de S3 o Swift estén configurados para enviar solicitudes a una de las siguientes:

- Dirección IP virtual de grupo de alta disponibilidad
- Un equilibrador de carga de terceros de alta disponibilidad
- Múltiples nodos de puerta de enlace para cada cliente

- Varios nodos de almacenamiento para cada cliente

Las aplicaciones cliente pueden experimentar interrupciones a corto plazo

El sistema StorageGRID puede procesar y recuperar datos de aplicaciones cliente en todo el proceso de revisión; sin embargo, es posible que las conexiones de cliente a nodos de puerta de enlace o nodos de almacenamiento individuales se interrumpieran temporalmente si la revisión necesita reiniciar los servicios en esos nodos. La conectividad se restaurará una vez completado el proceso de revisión y los servicios se reanudan en los nodos individuales.

Es posible que necesite programar tiempos de inactividad para aplicar una revisión si la pérdida de conectividad durante un período corto no es aceptable. Puede utilizar la aprobación selectiva para programar la actualización de determinados nodos.

> Puede usar varias puertas de enlace y grupos de alta disponibilidad para proporcionar conmutación por error automática durante el proceso de revisión. Consulte las instrucciones para "configuración de grupos de alta disponibilidad".

Es posible que se activen alertas y notificaciones SNMP

Las alertas y notificaciones SNMP se pueden activar cuando se reinician los servicios y cuando el sistema StorageGRID funciona como un entorno de versiones mixtas (algunos nodos de grid que ejecutan una versión anterior, mientras que otros se han actualizado a una versión posterior). En general, estas alertas y notificaciones se borran cuando se completa la revisión.

Los cambios de configuración están restringidos

Al aplicar una revisión a StorageGRID:

- No realice ningún cambio en la configuración de la cuadrícula (por ejemplo, especificando subredes de red de grid o aprobando nodos de cuadrícula pendientes) hasta que la revisión se haya aplicado a todos los nodos.
- No actualice la configuración de ILM hasta que la corrección urgente se haya aplicado a todos los nodos.

Obtener los materiales necesarios para la revisión

Antes de aplicar una revisión, debe obtener todos los materiales requeridos.

Elemento	Notas
Archivo de revisión de StorageGRID	Debe descargar el archivo de revisión de StorageGRID.
• Puerto de red • "Navegador web compatible" • Cliente SSH (por ejemplo, PuTTY)	

Elemento	Notas
Paquete de recuperación (`.zip`)	Antes de aplicar una revisión, "Descargue el archivo más reciente del paquete de recuperación" en caso de que ocurra algún problema durante la revisión. Luego, después de aplicar la revisión, descargue una nueva copia del archivo del paquete de recuperación y guárdelo en una ubicación segura. El archivo de paquete de recuperación actualizado le permite restaurar el sistema si se produce un fallo.
Archivo Passwords.txt	Opcional y utilizado sólo si aplica una revisión manualmente mediante el cliente SSH. La `Passwords.txt` El archivo forma parte del paquete de recuperación `.zip` archivo.
Clave de acceso de aprovisionamiento	La frase de contraseña se crea y documenta cuando se instala el sistema StorageGRID por primera vez. La clave de acceso de aprovisionamiento no aparece en la `Passwords.txt` archivo.
Documentación relacionada	`readme.txt` archivo para la revisión. Este archivo se incluye en la página de descarga de la revisión. Asegúrese de revisar el `readme` archivar cuidadosamente antes de aplicar la revisión.

Descargue el archivo de revisión

Debe descargar el archivo de revisión antes de poder aplicar la revisión.

Pasos

1. Vaya a. "Descargas de NetApp: StorageGRID".
2. Seleccione la flecha abajo en **Software disponible** para ver una lista de revisiones disponibles para descargar.

   Las versiones del archivo de revisión tienen el formato: 11.4.*x.y*_.

3. Revise los cambios que se incluyen en la actualización.

   Si tienes solo "Se ha recuperado el nodo de administración principal" y necesita aplicar una revisión, seleccione la misma versión de revisión que está instalada en los otros nodos de grid.

   a. Seleccione la versión de revisión que desea descargar y seleccione **Ir**.
   b. Inicie sesión con el nombre de usuario y la contraseña de su cuenta de NetApp.
   c. Lea y acepte el contrato de licencia para usuario final.

      Aparece la página de descarga de la versión seleccionada.

   d. Descargue la revisión `readme.txt` archivo para ver un resumen de los cambios incluidos en la revisión.
4. Seleccione el botón de descarga de la revisión y guarde el archivo.

No cambie el nombre de este archivo.

Si está utilizando un dispositivo MacOS, el archivo de revisión se puede guardar automáticamente como un `.txt` archivo. Si es así, debe cambiar el nombre del archivo sin el `.txt` extensión.

5. Seleccione una ubicación para la descarga y seleccione **Guardar**.

Compruebe el estado del sistema antes de aplicar la revisión

Debe comprobar que el sistema esté listo para acomodar la revisión.

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Si es posible, asegúrese de que el sistema funciona con normalidad y de que todos los nodos de grid están conectados a la cuadrícula.

   Los nodos conectados tienen marcas de comprobación de color verde En la página Nodes.

3. Compruebe y resuelva las alertas actuales si es posible.
4. Asegúrese de que no hay otros procedimientos de mantenimiento en curso, como un procedimiento de actualización, recuperación, ampliación o retirada.

   Debe esperar a que se complete cualquier procedimiento de mantenimiento activo antes de aplicar una revisión.

   No puede aplicar una revisión de StorageGRID cuando se está ejecutando otro procedimiento de mantenimiento. Por ejemplo, no se puede aplicar una revisión mientras se está ejecutando un procedimiento de decomiso, expansión o recuperación.

   Si es un nodo o un sitio "el procedimiento de decomisionar se pone en pausa", puede aplicar de forma segura una revisión. Además, puede ser capaz de aplicar una revisión durante las fases finales de un procedimiento de actualización de StorageGRID. Consulte las instrucciones para "Actualizando el software StorageGRID".

Aplicar revisión

La revisión se aplica automáticamente por primera vez al nodo de administración principal. A continuación, debe aprobar la aplicación de la revisión a otros nodos de cuadrícula hasta que todos los nodos ejecuten la misma versión de software. Puede personalizar la secuencia de aprobación seleccionando aprobar nodos de cuadrícula individuales, grupos de nodos de cuadrícula o todos los nodos de cuadrícula.

Antes de empezar

- Ha revisado el "consideraciones sobre la aplicación de una revisión".
- Tiene la clave de acceso de aprovisionamiento.
- Tiene acceso root o permiso de mantenimiento.

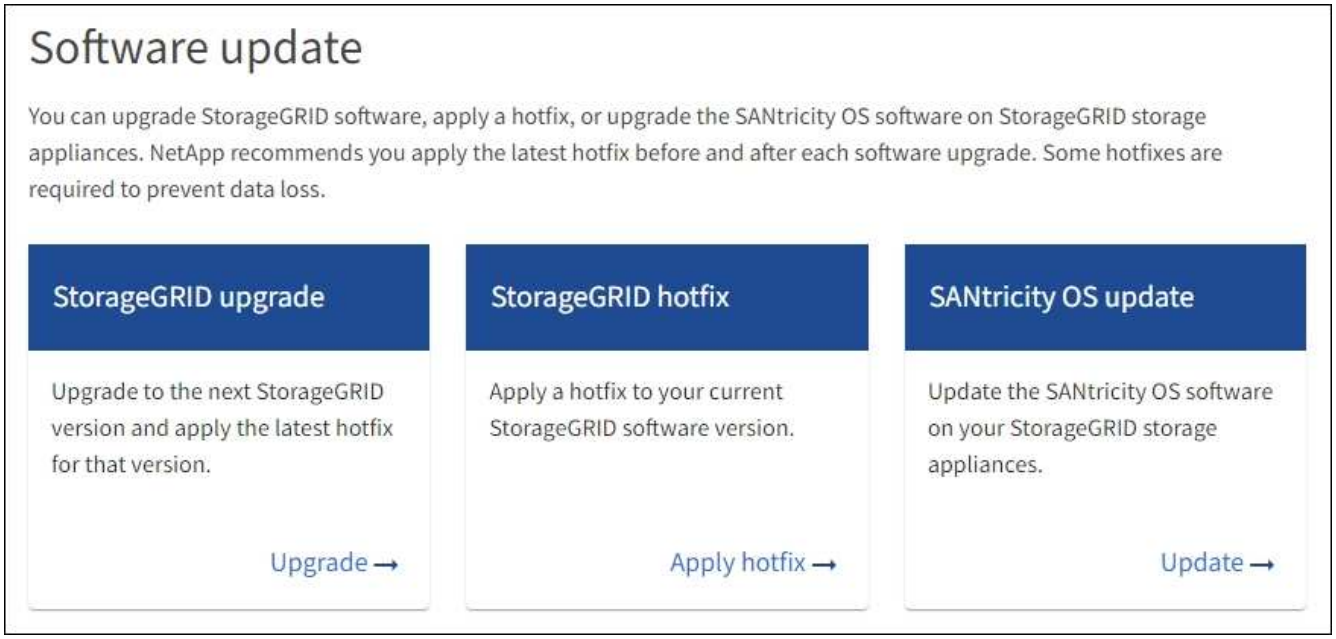
Acerca de esta tarea

- Puede retrasar la aplicación de una revisión a un nodo, pero el proceso de revisión no se completa hasta que aplique la revisión a todos los nodos.
- No puede realizar una actualización de software de StorageGRID ni una actualización de SANtricity OS hasta que haya completado el proceso de corrección.

Pasos

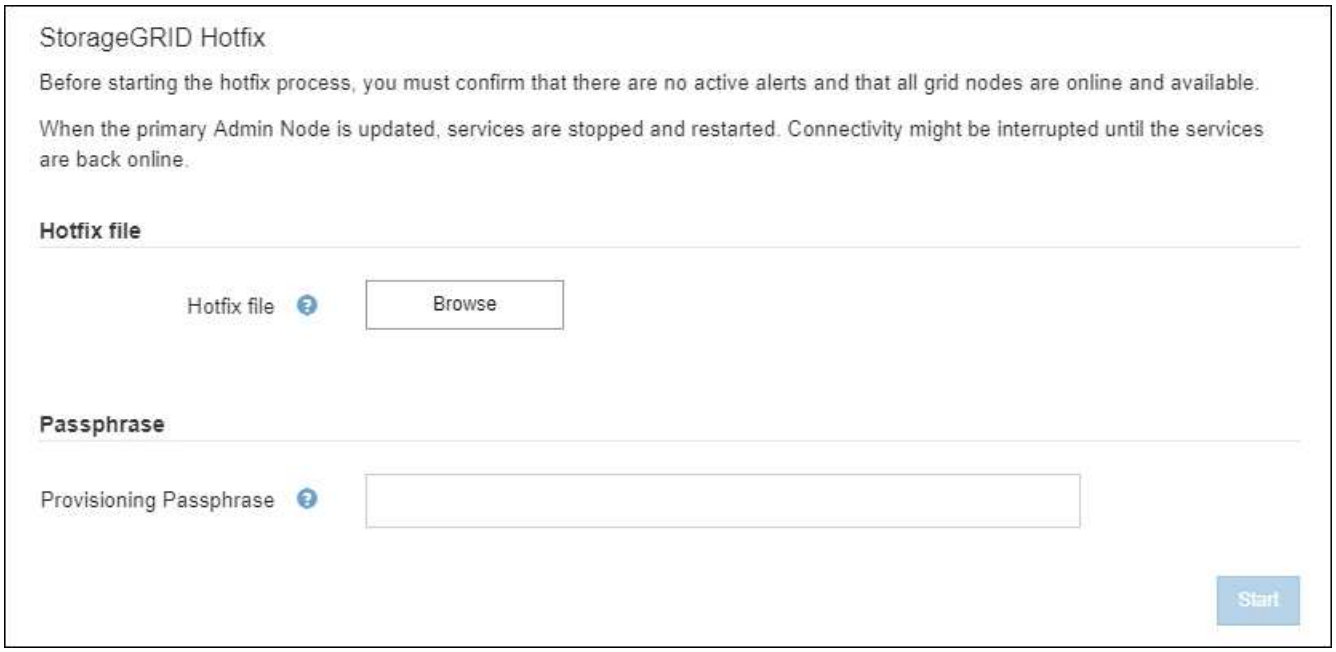
1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Seleccione **MANTENIMIENTO** > **sistema** > **actualización de software**.

   Aparece la página actualización de software.



3. Seleccione **aplicar revisión**.

   Aparece la página de corrección de StorageGRID.



4. Seleccione el archivo de corrección que descargó del sitio de soporte de NetApp.

   a. Seleccione **examinar**.

   b. Localice y seleccione el archivo.

      `hotfix-install-version`

   c. Seleccione **Abrir**.

      El archivo se carga. Cuando la carga haya finalizado, el nombre del archivo se mostrará en el campo Detalles.

      No cambie el nombre del archivo porque forma parte del proceso de verificación.

5. Introduzca la clave de acceso de aprovisionamiento en el cuadro de texto.

   El botón **Inicio** se activa.

6. Seleccione **Iniciar**.

   Aparece una advertencia que indica que la conexión del explorador puede perderse temporalmente cuando se reinician los servicios del nodo de administración principal.

7. Seleccione **Aceptar** para comenzar a aplicar la revisión al nodo de administración principal.

   Cuando se inicia la revisión:

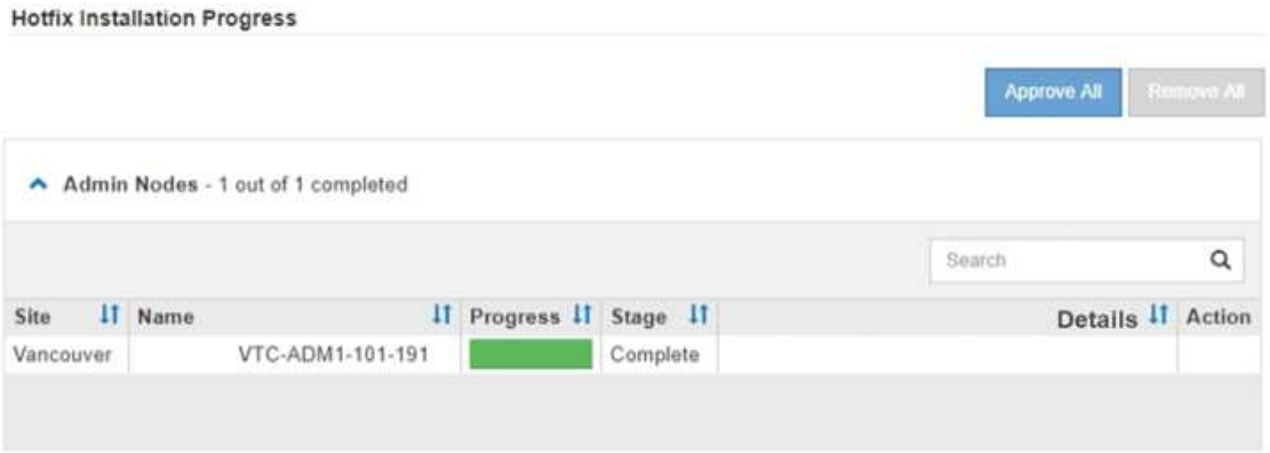
   a. Se ejecutan las validaciones de la revisión.

      Si se informa de algún error, solucione, vuelva a cargar el archivo de revisión y seleccione **Iniciar** de nuevo.

   b. Aparece la tabla de progreso de la instalación de la revisión.

      En esta tabla se muestran todos los nodos de la cuadrícula y la fase actual de la instalación de la revisión para cada nodo. Los nodos de la tabla se agrupan por tipo (nodos de administración, nodos de puerta de enlace, nodos de almacenamiento y nodos de archivado).

   c. La barra de progreso llega al final y el nodo de administración principal se muestra como completado.



8. Opcionalmente, ordene las listas de nodos de cada agrupación en orden ascendente o descendente por **Sitio**, **Nombre**, **progreso**, **etapa** o **Detalles**. O bien, introduzca un término en el cuadro **Buscar** para buscar nodos específicos.
9. Apruebe los nodos de cuadrícula que están listos para actualizarse. Los nodos aprobados del mismo tipo se actualizan de uno en uno.

   > No apruebe la revisión de un nodo a menos que esté seguro de que el nodo está listo para actualizarse. Cuando se aplica la revisión a un nodo de cuadrícula, algunos servicios de ese nodo se pueden reiniciar. Estas operaciones pueden provocar interrupciones del servicio en los clientes que se comunican con el nodo.

   - Seleccione uno o más botones **aprobar** para agregar uno o más nodos individuales a la cola de revisiones.
   - Seleccione el botón **aprobar todo** de cada agrupación para agregar todos los nodos del mismo tipo a la cola de revisiones. Si ha introducido criterios de búsqueda en el cuadro **Buscar**, el botón **aprobar todo** se aplica a todos los nodos seleccionados por los criterios de búsqueda.

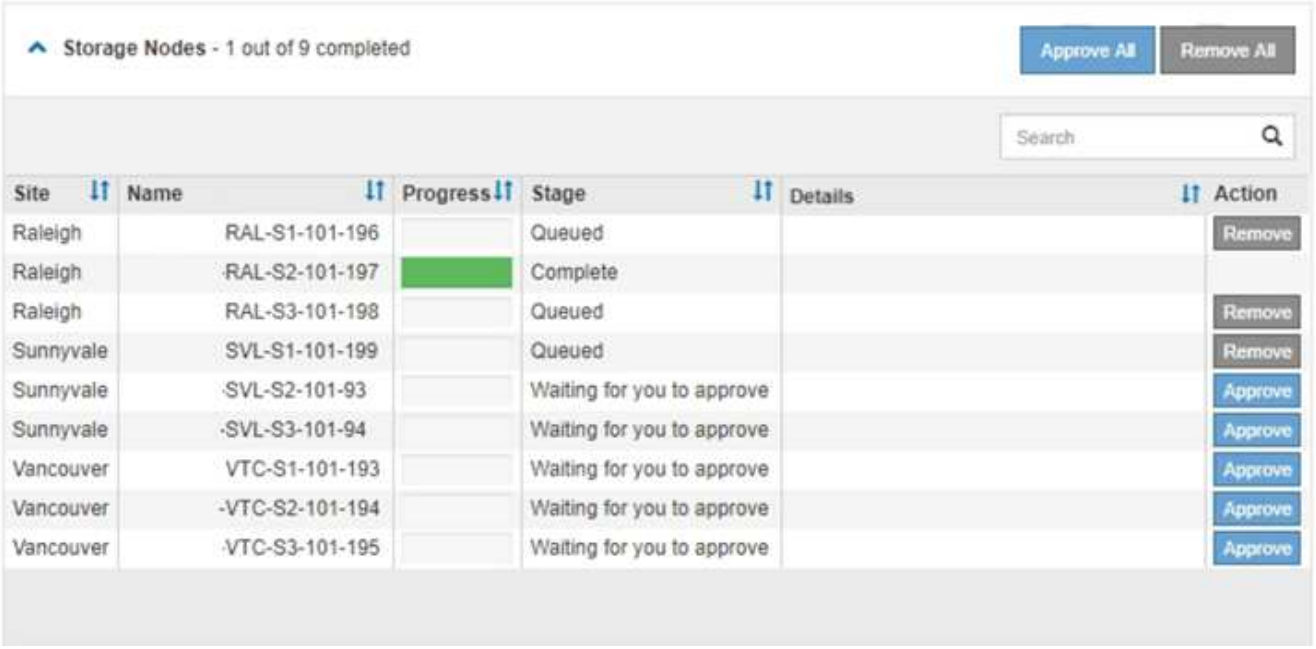
     > El botón **aprobar todo** situado en la parte superior de la página aprueba todos los nodos enumerados en la página, mientras que el botón **aprobar todo** situado en la parte superior de una agrupación de tablas sólo aprueba todos los nodos de ese grupo. Si el orden en el que se actualizan los nodos es importante, apruebe los nodos o grupos de nodos de uno en uno y espere a que la actualización se complete en cada nodo antes de aprobar los siguientes nodos.

   - Seleccione el botón de nivel superior **aprobar todo** en la parte superior de la página para agregar todos los nodos de la cuadrícula a la cola de revisiones.

     > Debe completar la revisión de StorageGRID antes de poder iniciar una actualización de software diferente. Si no puede completar la revisión, póngase en contacto con el soporte técnico.

   - Seleccione **Quitar** o **Quitar todo** para quitar un nodo o todos los nodos de la cola de revisiones.

     Cuando la etapa progresa más allá de “En cola”, el botón **Eliminar** se oculta y ya no se puede eliminar el nodo del proceso de revisión.



10. Espere mientras la revisión se aplica a cada nodo de cuadrícula aprobado.

    Cuando la revisión se ha instalado correctamente en todos los nodos, se cierra la tabla de progreso de instalación de Hotfix. Un banner verde muestra la fecha y la hora en que se completó la revisión.

11. Si la revisión no se pudo aplicar a ningún nodo, revise el error para cada nodo, resuelva el problema y repita estos pasos.

    El procedimiento no se completa hasta que la revisión se aplica correctamente a todos los nodos. Puede volver a intentar de forma segura el proceso de revisión tantas veces como sea necesario hasta que se complete.

Configure y gestione un sistema StorageGRID

Administre StorageGRID

Administrar StorageGRID: Descripción general

Siga estas instrucciones para configurar y administrar un sistema StorageGRID.

Acerca de estas instrucciones

Las tareas principales para configurar y administrar StorageGRID le permiten:

- Utilice Grid Manager para configurar grupos y usuarios
- Cree cuentas de inquilino para permitir que las aplicaciones cliente S3 y Swift almacenen y recuperen objetos
- Configurar y gestionar redes StorageGRID
- Configure AutoSupport
- Gestione la configuración del nodo

Antes de empezar

- Tiene una visión general del sistema StorageGRID.
- Tiene un conocimiento muy detallado de los shell de comandos de Linux, las conexiones de red y la instalación y configuración del hardware de servidor.

Comience a usar Grid Manager

Requisitos del navegador web

Debe utilizar un navegador web compatible.

Navegador Web	Versión mínima admitida
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Debe establecer la ventana del navegador en un ancho recomendado.

Ancho del navegador	Píxeles
Mínimo	1024
Óptimo	1280

Inicie sesión en Grid Manager

Para acceder a la página de inicio de sesión de Grid Manager, introduzca el nombre de dominio completo (FQDN) o la dirección IP de un nodo de administración en la barra de direcciones de un explorador web compatible.

Descripción general

Cada sistema StorageGRID incluye un nodo de administrador primario y cualquier número de nodos de administrador que no son primarios. Puede iniciar sesión en Grid Manager en cualquier nodo de administrador para gestionar el sistema StorageGRID. Sin embargo, los nodos administradores no son exactamente los mismos:

- Las confirmaciones de alarma (sistema heredado) realizadas en un nodo de administración no se copian en otros nodos de administración. Por este motivo, es posible que la información mostrada para las alarmas no tenga el mismo aspecto en cada nodo de administración.
- Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

Conéctese a un grupo de alta disponibilidad

Si se incluyen nodos de administración en un grupo de alta disponibilidad (ha), puede conectarse mediante la dirección IP virtual del grupo de alta disponibilidad o un nombre de dominio completo que asigne la dirección IP virtual. El nodo de administración principal se debe seleccionar como la interfaz principal del grupo, de modo que al acceder a Grid Manager, se tiene acceso en el nodo de administración principal a menos que el nodo de administración principal no esté disponible. Consulte "Gestión de grupos de alta disponibilidad".

Utilice SSO

Los pasos de inicio de sesión son ligeramente diferentes si "Se ha configurado el inicio de sesión único (SSO)".

Inicie sesión en Grid Manager en el primer nodo de administración

Antes de empezar

- Tiene sus credenciales de inicio de sesión.
- Está utilizando un "navegador web compatible".
- Las cookies están habilitadas en su navegador web.
- Pertenece a un grupo de usuarios que tiene al menos un permiso.
- Tiene la dirección URL de Grid Manager:

  `https://FQDN_or_Admin_Node_IP/`

  Puede usar el nombre de dominio completo, la dirección IP de un nodo de administración o la dirección IP virtual de un grupo de alta disponibilidad de nodos de administración.

  Para acceder a Grid Manager en un puerto que no sea el puerto predeterminado para HTTPS (443), incluya el número de puerto en la dirección URL:

  `https://FQDN_or_Admin_Node_IP:port/`

SSO no está disponible en el puerto restringido de Grid Manager. Se debe usar el puerto 443.

Pasos

1. Inicie un explorador web compatible.
2. En la barra de direcciones del navegador, introduzca la dirección URL de Grid Manager.
3. Si se le solicita una alerta de seguridad, instale el certificado con el asistente de instalación del explorador. Consulte "Gestionar certificados de seguridad".
4. Inicie sesión en Grid Manager.

   La pantalla de inicio de sesión que aparece depende de si se ha configurado el inicio de sesión único (SSO) para StorageGRID.

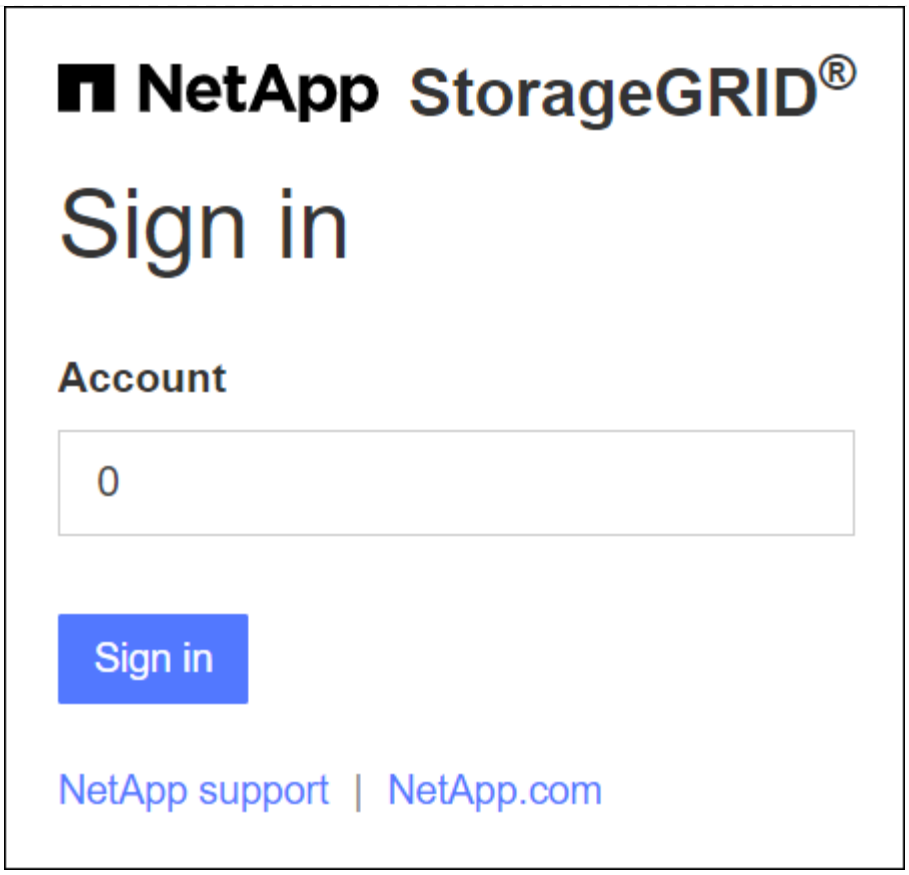
No se utiliza SSO

a. Introduzca su nombre de usuario y contraseña para el administrador de grid.

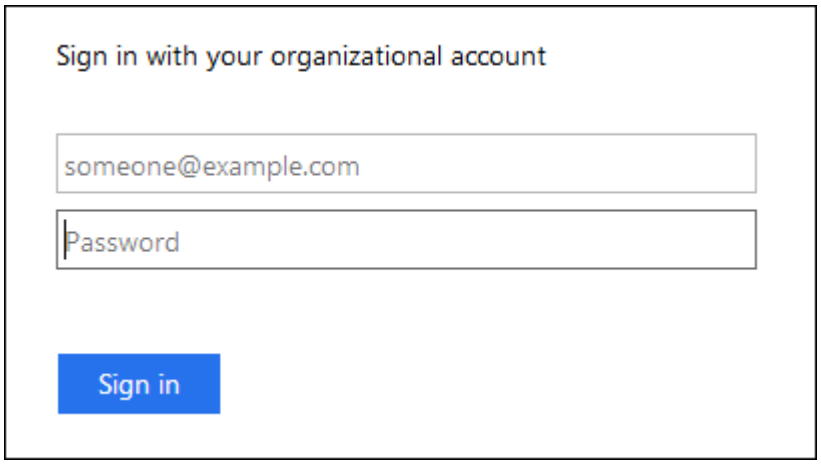
b. Seleccione **Iniciar sesión**.

Uso de SSO

- Si StorageGRID utiliza SSO y esta es la primera vez que accede a la URL en este explorador:
  i. Seleccione **Iniciar sesión**. Puede dejar el 0 en el campo Cuenta.



ii. Introduzca sus credenciales de SSO estándar en la página de inicio de sesión con SSO de su organización. Por ejemplo:



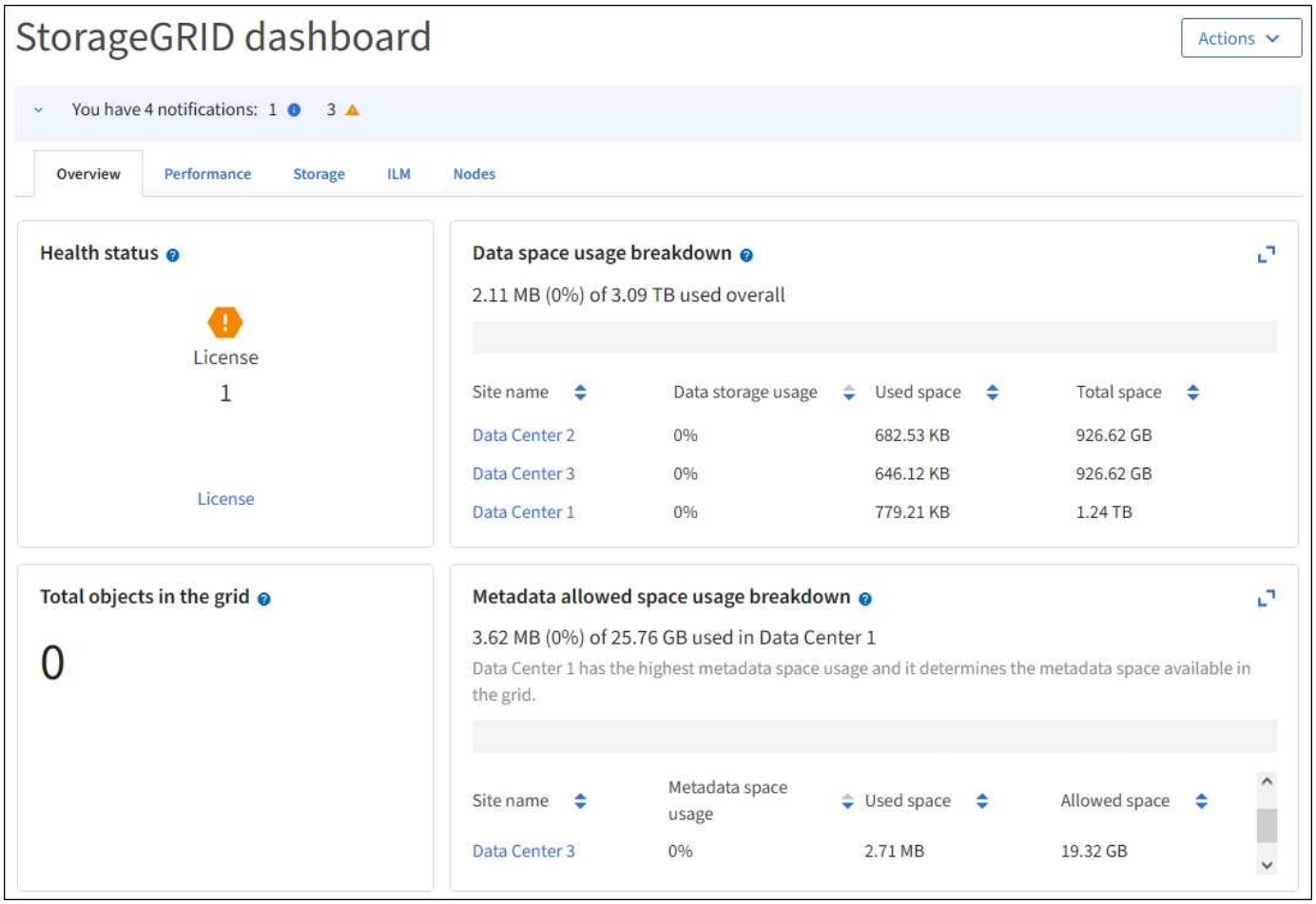
- Si StorageGRID utiliza SSO y se ha accedido previamente a Grid Manager o a una cuenta de inquilino:

  i. Introduzca **0** (el ID de cuenta de Grid Manager) o seleccione **Grid Manager** si aparece en la lista de cuentas recientes.

ii. Seleccione **Iniciar sesión**.

iii. Inicie sesión con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización.

Al iniciar sesión, aparece la página inicial de Grid Manager, que incluye el panel de control. Para saber qué información se proporciona, consulte "Permite ver y gestionar el panel de control".



Conéctese a otro nodo de administración

Siga estos pasos para iniciar sesión en otro nodo de administración.

No se utiliza SSO

Pasos

1. En la barra de direcciones del navegador, introduzca el nombre de dominio completo o la dirección IP del otro nodo de administración. Incluya el número de puerto según sea necesario.
2. Introduzca su nombre de usuario y contraseña para el administrador de grid.
3. Seleccione **Iniciar sesión**.

Uso de SSO

Si StorageGRID está utilizando SSO y ha iniciado sesión en un nodo de administración, puede acceder a otros nodos de administración sin tener que volver a iniciar sesión.

Pasos

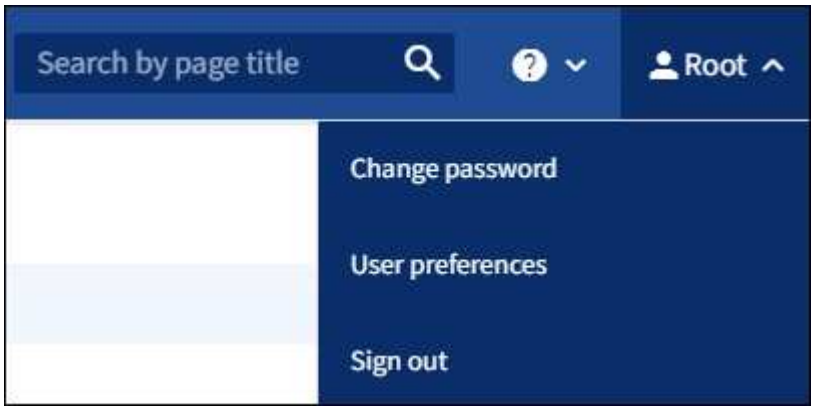
1. Introduzca el nombre de dominio completo o la dirección IP del otro nodo de administración en la barra de direcciones del navegador.
2. Si su sesión de SSO ha caducado, vuelva a introducir sus credenciales.

Cierre la sesión en Grid Manager

Cuando haya terminado de trabajar con Grid Manager, debe cerrar sesión para asegurarse de que los usuarios no autorizados no puedan acceder al sistema StorageGRID. Es posible que cerrar el navegador no le cierre la sesión del sistema según la configuración de cookies del navegador.

Pasos

1. Seleccione su nombre de usuario en la esquina superior derecha.



2. Selecciona **Cerrar sesión**.

Opción	Descripción
SSO no en uso	Ha cerrado sesión en el nodo de administrador. Se muestra la página de inicio de sesión de Grid Manager. **Nota:** Si ha iniciado sesión en más de un nodo de administración, debe cerrar sesión en cada nodo.
SSO habilitado	Inició sesión en todos los nodos de administrador a los que accedían. Aparece la página de inicio de sesión de StorageGRID. **Grid Manager** aparece como el valor predeterminado en la lista desplegable **Cuentas recientes**, y el campo **ID de cuenta** muestra 0. **Nota:** Si SSO está habilitado y usted también ha iniciado sesión en el Gestor de Inquilinos, también debe hacerlo "cierre la sesión de la cuenta de inquilino" para "Cierre la sesión de SSO".

Cambie la contraseña

Si es un usuario local de Grid Manager, puede cambiar su propia contraseña.

Antes de empezar

Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".

Acerca de esta tarea

Si inicia sesión en StorageGRID como usuario federado o si está habilitado el inicio de sesión único (SSO), no

podrá cambiar la contraseña en Grid Manager. En su lugar, debe cambiar la contraseña en el origen de identidad externo, por ejemplo, Active Directory u OpenLDAP.

Pasos

1. En el encabezado de Grid Manager, seleccione ***su nombre*** > **Cambiar contraseña**.
2. Introduzca su contraseña actual.
3. Escriba una nueva contraseña.

   La contraseña debe contener al menos 8 caracteres y no más de 32. Las contraseñas distinguen mayúsculas de minúsculas.

4. Vuelva a introducir la nueva contraseña.
5. Seleccione **Guardar**.

Consulte la información de licencia de StorageGRID

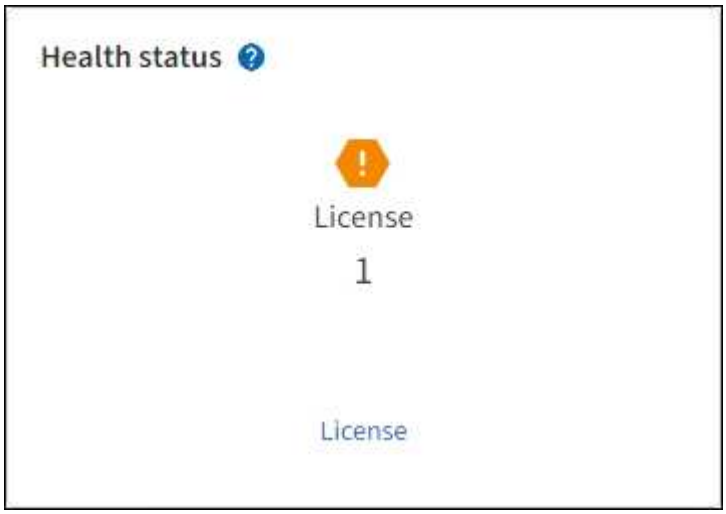
Puede ver la información de licencia del sistema StorageGRID, como la capacidad de almacenamiento máxima de su grid, cuando sea necesario.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".

Acerca de esta tarea

Si hay un problema con la licencia de software para este sistema StorageGRID, la tarjeta de estado del panel incluye un icono de estado de licencia y un enlace de **Licencia**. El número indica el número de problemas relacionados con la licencia.



Pasos

1. Para acceder a la página Licencia, realice una de las siguientes acciones:
   - Seleccione **MANTENIMIENTO** > **sistema** > **Licencia**.
   - En la tarjeta de estado de salud del panel de control, seleccione el icono de estado de la licencia o el enlace **Licencia**.

     Este vínculo sólo aparece si hay un problema con la licencia.

2. Vea los detalles de sólo lectura de la licencia actual:
   - ID del sistema de StorageGRID, que es el número de identificación exclusivo para esta instalación de StorageGRID
   - Número de serie de la licencia
   - Tipo de licencia, ya sea **Perpetual** o **Suscripción**
   - Capacidad de almacenamiento bajo licencia del grid
   - Capacidad de almacenamiento admitida
   - Fecha de finalización de la licencia. **N/A** aparece para una licencia perpetua.
   - Fecha de finalización del soporte

     Esta fecha se lee del archivo de licencia actual y puede estar obsoleta si se amplió o renovó el contrato de servicio de soporte después de obtener el archivo de licencia. Para actualizar este valor, consulte "Actualice la información de licencia de StorageGRID". También puede consultar la fecha de finalización real del contrato mediante Active IQ.

   - Contenido del archivo de texto de licencia

Actualice la información de licencia de StorageGRID

Debe actualizar la información de licencia del sistema de StorageGRID en cualquier momento que cambien las condiciones de su licencia. Por ejemplo, debe actualizar la información de la licencia si adquiere capacidad de almacenamiento adicional para su grid.

Antes de empezar

- Tiene un nuevo archivo de licencia que se aplicará al sistema StorageGRID.
- Ya tienes "permisos de acceso específicos".
- Tiene la clave de acceso de aprovisionamiento.

Pasos

1. Seleccione **MANTENIMIENTO** > **sistema** > **Licencia**.
2. En la sección Actualizar licencia, seleccione **Examinar**.
3. Busque y seleccione el nuevo archivo de licencia (`.txt`).

   El nuevo archivo de licencia se valida y muestra.

4. Introduzca la clave de acceso de aprovisionamiento.
5. Seleccione **Guardar**.

Use la API

Utilice la API de gestión de grid

Puede realizar tareas de administración del sistema mediante la API REST de Grid Management en lugar de la interfaz de usuario de Grid Manager. Por ejemplo, se recomienda utilizar la API para automatizar operaciones o crear varias entidades, como los usuarios, más rápidamente.

Recursos de alto nivel

La API de gestión de grid proporciona los siguientes recursos de nivel superior:

- `/grid`: Access está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados.
- `/org`: Access está restringido a los usuarios que pertenecen a un grupo LDAP local o federado para una cuenta de inquilino. Para obtener más información, consulte "Usar una cuenta de inquilino".
- `/private`: Access está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados. Las API privadas están sujetas a cambios sin previo aviso. Los extremos privados de StorageGRID también ignoran la versión de API de la solicitud.

Emita solicitudes API

La API de gestión de grid utiliza la plataforma API de código abierto de Swagger. Swagger proporciona una interfaz de usuario intuitiva que permite a los desarrolladores y no desarrolladores realizar operaciones en tiempo real en StorageGRID con la API.

La interfaz de usuario de Swagger proporciona detalles y documentación completos para cada operación de API.

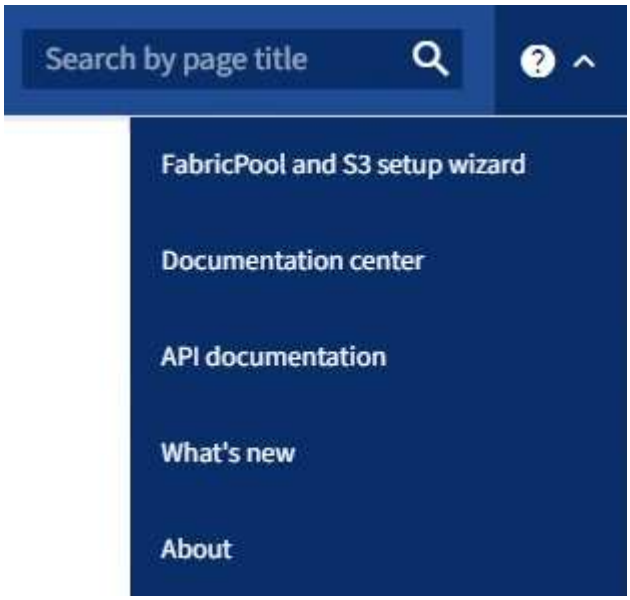
Antes de empezar

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

> Cualquier operación de API que realice mediante la página web de documentos de API es una operación en directo. Tenga cuidado de no crear, actualizar o eliminar datos de configuración u otros datos por error.

Pasos

1. En el encabezado de Grid Manager, selecciona el icono de ayuda y selecciona **Documentación de API**.



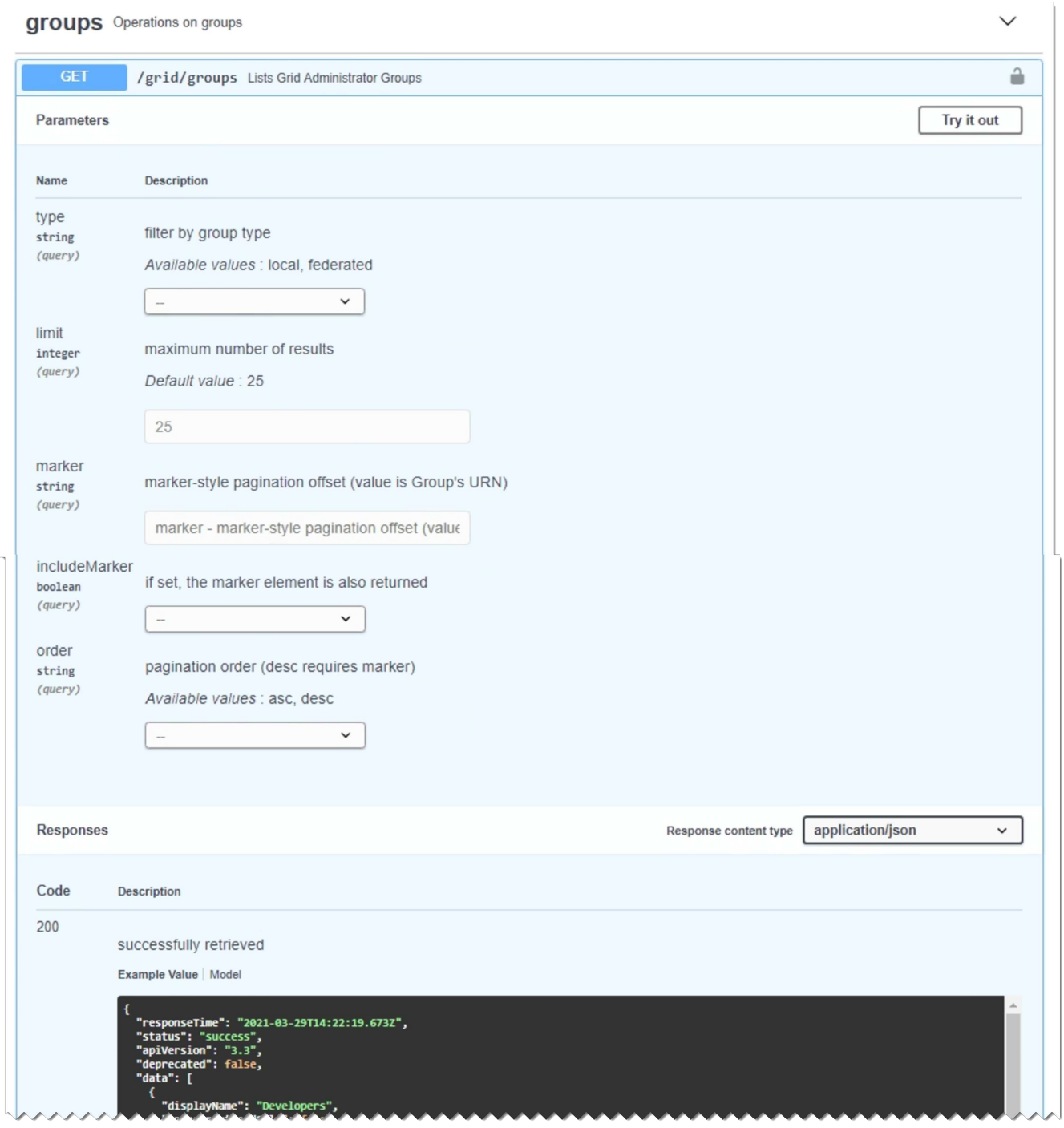
2. Para realizar una operación con la API privada, seleccione **Ir a documentación de API privada** en la página API de administración de StorageGRID.

Las API privadas están sujetas a cambios sin previo aviso. Los extremos privados de StorageGRID también ignoran la versión de API de la solicitud.

3. Seleccione la operación deseada.

   Al expandir una operación de API, puede ver las acciones HTTP disponibles, como GET, PUT, UPDATE y DELETE.

4. Seleccione una acción HTTP para ver los detalles de la solicitud, incluida la dirección URL del extremo, una lista de los parámetros necesarios o opcionales, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.



5. Determine si la solicitud requiere parámetros adicionales, como un ID de grupo o de usuario. A

continuación, obtenga estos valores. Es posible que primero deba emitir una solicitud de API diferente para obtener la información que necesita.

6. Determine si necesita modificar el cuerpo de solicitud de ejemplo. Si es así, puede seleccionar **Modelo** para conocer los requisitos de cada campo.
7. Seleccione **probar**.
8. Proporcione los parámetros necesarios o modifique el cuerpo de la solicitud según sea necesario.
9. Seleccione **Ejecutar**.
10. Revise el código de respuesta para determinar si la solicitud se ha realizado correctamente.

Operaciones de API de gestión de grid

La API de gestión de grid organiza las operaciones disponibles en las siguientes secciones.

> Esta lista solo incluye las operaciones disponibles en la API pública.

- **CUENTAS**: Operaciones para administrar cuentas de inquilinos de almacenamiento, incluyendo la creación de nuevas cuentas y la recuperación del uso de almacenamiento para una cuenta dada.
- **ALARMAS**: Operaciones para listar alarmas actuales (sistema heredado), y devolver información sobre el estado de la cuadrícula, incluyendo las alertas actuales y un resumen de los estados de conexión de nodos.
- **ALERT-HISTORY**: Operaciones en alertas resueltas.
- **RECEPTORES DE ALERTA**: Operaciones en receptores de notificación de alerta (correo electrónico).
- **ALERT-RULES**: Operaciones en reglas de alerta.
- **ALERT-SILENCES**: Operaciones en silencios de alerta.
- **ALERTAS**: Operaciones en alertas.
- **AUDIT**: Operaciones para listar y actualizar la configuración de auditoría.
- **AUTH**: Operaciones para realizar la autenticación de sesión de usuario.

  La API de administración de grid admite el esquema de autenticación de token de Bearer. Para iniciar sesión, debe proporcionar un nombre de usuario y una contraseña en el cuerpo JSON de la solicitud de autenticación (es decir, `POST /api/v3/authorize`). Si el usuario se autentica correctamente, se devuelve un token de seguridad. Este token se debe proporcionar en el encabezado de las siguientes solicitudes de API ("autorización: Portador *token*"). El token caduca después de 16 horas.

  > Si el inicio de sesión único está habilitado para el sistema StorageGRID, debe realizar pasos diferentes para la autenticación. Consulte Autenticación en la API si el inicio de sesión único está activado.

  Consulte Protección contra errores de solicitudes entre sitios para obtener información sobre cómo mejorar la seguridad de la autenticación.

- **CERTIFICADOS DE CLIENTE**: Operaciones para configurar certificados de cliente de modo que se pueda acceder a StorageGRID de forma segura utilizando herramientas de monitoreo externas.
- **Config**: Operaciones relacionadas con el lanzamiento del producto y versiones de la API de administración de grid. Es posible mostrar la versión del producto y las versiones principales de la API de Grid Management compatibles con esta versión, así como deshabilitar las versiones obsoletas de la API.

- **Funciones desactivadas**: Operaciones para ver características que podrían haber sido desactivadas.
- **Servidores dns**: Operaciones para listar y cambiar servidores DNS externos configurados.
- **Drive-details**: Operaciones en unidades para modelos específicos de dispositivos de almacenamiento.
- **Endpoint-domain-names**: Operaciones para listar y cambiar los nombres de dominio de punto final S3.
- **Código de borrado**: Operaciones en perfiles de codificación de borrado.
- **EXPANSIÓN**: Operaciones de expansión (nivel de procedimiento).
- **EXPANSION-NODES**: Operaciones en expansión (nivel de nodo).
- **Sitios de expansión**: Operaciones en expansión (nivel de sitio).
- **Grid-networks**: Operaciones para listar y cambiar la Lista de Red de Grid.
- **Grid-passwords**: Operaciones para la gestión de contraseñas de grid.
- **GRUPOS**: Operaciones para administrar grupos de administradores de grid locales y para recuperar grupos de administradores de grid federados desde un servidor LDAP externo.
- **Identity-source**: Operaciones para configurar una fuente de identidad externa y sincronizar manualmente la información federada del grupo y del usuario.
- **ilm**: Operaciones de gestión del ciclo de vida de la información (ILM).
- **Procedimientos en curso**: Recupera los procedimientos de mantenimiento que están actualmente en curso.
- **LICENCIA**: Operaciones para recuperar y actualizar la licencia de StorageGRID.
- **Logs**: Operaciones para recopilar y descargar archivos de registro.v
- **Métricas**: Operaciones en métricas StorageGRID, incluidas consultas métricas instantáneas en un único punto en el tiempo y consultas métricas de rango durante un intervalo de tiempo. La API de gestión de grid utiliza la herramienta de supervisión de sistemas Prometheus como origen de datos de back-end. Para obtener información sobre la construcción de consultas Prometheus, consulte el sitio web Prometheus.

> Métricas que incluyen `private` en sus nombres sólo se utilizan de forma interna. Estas métricas están sujetas a cambios entre las versiones de StorageGRID sin previo aviso.

- **Node-details**: Operaciones en los detalles del nodo.
- **Node-health**: Operaciones en el estado de salud del nodo.
- **Node-storage-state**: Operaciones en el estado de almacenamiento del nodo.
- **Servidores ntp**: Operaciones para listar o actualizar servidores externos de Protocolo de Tiempo de Red (NTP).
- **OBJETOS**: Operaciones en objetos y metadatos de objetos.
- **RECUPERACIÓN**: Operaciones para el procedimiento de recuperación.
- **Recovery-package**: Operaciones para descargar el paquete de recuperación.
- **REGIONES**: Operaciones para ver y crear regiones.
- **S3-object-lock**: Operaciones en la configuración global de S3 Object Lock.
- **Server-certificate**: Operaciones para ver y actualizar los certificados de servidor de Grid Manager.
- **snmp**: Operaciones en la configuración SNMP actual.
- **Storage-watermarks**: Marcas de agua del nodo de almacenamiento.
- **Clases de tráfico**: Operaciones para las políticas de clasificación de tráfico.

- **Red-cliente-no confiable**: Operaciones en la configuración de la red cliente no confiable.
- **Usuarios**: Operaciones para ver y administrar usuarios de Grid Manager.

Creación de versiones de la API de gestión de grid

La API de gestión de grid utiliza versiones para permitir actualizaciones sin interrupciones.

Por ejemplo, esta URL de solicitud especifica la versión 4 de la API.

`https://hostname_or_ip_address/api/v4/authorize`

La versión principal de la API se salta cuando se realizan cambios que son *no compatibles* con versiones anteriores. La versión secundaria de la API se salta cuando se realizan cambios que son compatibles con versiones anteriores. Los cambios compatibles incluyen la adición de nuevos extremos o nuevas propiedades.

En el ejemplo siguiente se muestra cómo la versión de API se bONTAP en función del tipo de cambios realizados.

Tipo de cambio en la API	Versión anterior	Nueva versión
Compatible con versiones anteriores	2,1	2,2
No es compatible con versiones anteriores	2,1	3,0

Al instalar el software StorageGRID por primera vez, solo se habilita la versión más reciente de la API. Sin embargo, cuando actualice a una versión de función nueva de StorageGRID, seguirá teniendo acceso a la versión de API anterior para al menos una versión de función de StorageGRID.

> Puede configurar las versiones admitidas. Consulte la sección **config** de la documentación de la API de Swagger para el "API de gestión de grid" si quiere más información. Debe desactivar la compatibilidad con la versión anterior después de actualizar todos los clientes API para que usen la versión más reciente.

Las solicitudes obsoletas se marcan como obsoletas de las siguientes formas:

- El encabezado de la respuesta es "Dedeprecated: True"
- El cuerpo de respuesta JSON incluye "obsoleto": TRUE
- Se agrega una advertencia obsoleta a nms.log. Por ejemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determine qué versiones de API son compatibles con la versión actual

Utilice la `GET /versions` Solicitud de API para devolver una lista de las versiones principales de la API admitidas. Esta solicitud se encuentra en la sección **config** de la documentación de la API de Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Especifique una versión API para una solicitud

Puede especificar la versión de API mediante un parámetro path (`/api/v4`) o un encabezado (`Api-Version: 4`). Si proporciona ambos valores, el valor de encabezado anula el valor de ruta de acceso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protección contra falsificación de solicitudes entre sitios (CSRF)

Puede ayudar a protegerse contra ataques de falsificación de solicitudes entre sitios (CSRF) contra StorageGRID mediante tokens CSRF para mejorar la autenticación que usa cookies. El administrador de grid y el administrador de inquilinos habilitan automáticamente esta característica de seguridad; otros clientes de API pueden elegir si habilitar la función cuando se conectan.

Un atacante que pueda activar una solicitud a un sitio diferente (por ejemplo, con UNA POST de formulario HTTP) puede provocar ciertas solicitudes mediante las cookies del usuario que ha iniciado sesión.

StorageGRID ayuda a proteger contra ataques de CSRF mediante tokens CSRF. Cuando se activa, el contenido de una cookie específica debe coincidir con el contenido de un encabezado específico o de un parámetro DE cuerpo DE POST específico.

Para habilitar la función, configure la `csrfToken` parámetro a. `true` durante la autenticación. El valor predeterminado es `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Cuando es verdadero, un `GridCsrfToken` Cookie se establece con un valor aleatorio para las operaciones de inicio de sesión en Grid Manager y en `AccountCsrfToken` Cookie se establece con un valor aleatorio para las operaciones de inicio de sesión en el Administrador de inquilinos.

Si la cookie está presente, todas las solicitudes que puedan modificar el estado del sistema (POST, PUT, PATCH, DELETE) deben incluir una de las siguientes:

- La `X-Csrf-Token` Encabezado, con el valor del encabezado establecido en el valor de la cookie de token de CSRF.
- Para los extremos que aceptan un cuerpo codificado mediante formulario: A. `csrfToken` parámetro de cuerpo de solicitud codificado mediante formulario.

Consulte la documentación de API en línea para obtener detalles y ejemplos adicionales.

> Las solicitudes que tienen un conjunto de cookies de token CSRF también aplicarán el encabezado de tipo de contenido: Aplicación/json para cualquier solicitud que espere un cuerpo de solicitud JSON como una protección adicional contra los ataques CSRF.

Use la API si está activado el inicio de sesión único

Utilizar la API si está activado el inicio de sesión único (Active Directory)

Si lo tiene "Inicio de sesión único configurado y habilitado (SSO)" Además, se utiliza Active Directory como proveedor SSO, debe emitir una serie de solicitudes API para obtener un token de autenticación válido para la API de administración de grid o la API de administración de inquilinos.

Inicie sesión en la API si está habilitado el inicio de sesión único

Estas instrucciones se aplican si utiliza Active Directory como proveedor de identidades SSO.

Antes de empezar

- Conoce el nombre de usuario y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar uno de los siguientes ejemplos:

- La `storagegrid-ssoauth.py` Script Python, que se encuentra en el directorio de archivos de

instalación de StorageGRID (`./rpms` Para Red Hat Enterprise Linux, `./debs` Para Ubuntu o Debian, y. `./vsphere` Para VMware).

- Ejemplo de flujo de trabajo de solicitudes curl.

  El flujo de trabajo curl podría llegar a ocurrir si lo hace demasiado lentamente. Es posible que aparezca el error: `A valid SubjectConfirmation was not found on this Response`.

  > El flujo de trabajo curl de ejemplo no protege la contraseña de ser vista por otros usuarios.

Si tiene un problema de codificación URL, puede que aparezca el error: `Unsupported SAML version`.

Pasos

1. Seleccione uno de los siguientes métodos para obtener un token de autenticación:
   - Utilice la `storagegrid-ssoauth.py` Guión Python. Vaya al paso 2.
   - Usar solicitudes curl. Vaya al paso 3.
2. Si desea utilizar el `storagegrid-ssoauth.py` Guión, pase el script al intérprete Python y ejecute el script.

   Cuando se le solicite, escriba valores para los siguientes argumentos:

   - El método SSO. Introduzca ADFS o adfs.
   - El nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID
   - La dirección de StorageGRID
   - El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.

3. Si desea usar solicitudes curl, use el siguiente procedimiento.

   a. Declare las variables necesarias para iniciar sesión.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

> Para acceder a la API de gestión de grid, utilice 0 AS `TENANTACCOUNTID`.

b. Para recibir una URL de autenticación firmada, emita una solicitud DE ENVÍO `/api/v3/authorize-saml`, Y quite la codificación JSON adicional de la respuesta.

En este ejemplo se muestra una solicitud POST para una dirección URL de autenticación firmada `TENANTACCOUNTID`. Los resultados se pasan a. `python -m json.tool` Para quitar la codificación JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La respuesta de este ejemplo incluye una dirección URL firmada codificada por URL, pero no incluye la capa de codificación JSON adicional.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Guarde la `SAMLRequest` de la respuesta para su uso en comandos posteriores.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Obtenga una URL completa que incluya el ID de solicitud de cliente de AD FS.

Una opción es solicitar el formulario de inicio de sesión mediante la URL de la respuesta anterior.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

La respuesta incluye el ID de solicitud del cliente:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Guarde el ID de solicitud de cliente de la respuesta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Envíe sus credenciales a la acción de formulario de la respuesta anterior.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS devuelve un redireccionamiento 302, con información adicional en los encabezados.

> Si la autenticación multifactor (MFA) está habilitada para el sistema SSO, la entrada del formulario también contendrá la segunda contraseña u otras credenciales.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Guarde la `MSISAuth` cookie de la respuesta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Envíe una solicitud GET a la ubicación especificada con las cookies de LA PUBLICACIÓN de autenticación.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Los encabezados de respuesta contendrán información de sesión de AD FS para el uso posterior del cierre de sesión y el cuerpo de respuesta contiene el SAMLResponse en un campo de formulario oculto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Guarde la `SAMLResponse` en el campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizando el guardado `SAMLResponse`, Haga un StorageGRID`/api/saml-response` Solicitud para generar un token de autenticación de StorageGRID.

Para `RelayState`, Utilice el ID de cuenta de arrendatario o utilice 0 si desea iniciar sesión en la API de administración de grid.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La respuesta incluye el token de autenticación.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Guarde el token de autenticación en la respuesta como `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ahora puede utilizar `MYTOKEN` Para otras solicitudes, del mismo modo que utilizaría la API si no se utiliza SSO.

Cierre sesión en la API si el inicio de sesión único está habilitado

Si se ha activado el inicio de sesión único (SSO), debe emitir una serie de solicitudes API para cerrar sesión en la API de gestión de grid o en la API de gestión de inquilinos.
Estas instrucciones se aplican si utiliza Active Directory como proveedor de identidades SSO

Acerca de esta tarea

Si es necesario, puede cerrar sesión en la API de StorageGRID cerrando sesión en la página de cierre de sesión único de su organización. O bien, puede activar el cierre de sesión único (SLO) desde StorageGRID, que requiere un token de portador de StorageGRID válido.

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase la cookie «sso=true» a la API de SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Se devuelve una URL de cierre de sesión:

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Guarde la URL de cierre de sesión.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. Envíe una solicitud a la URL de cierre de sesión para activar SLO y redirigir de nuevo a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Se devuelve la respuesta de 302. La ubicación de redirección no se aplica a la salida de sólo API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Elimine el token del portador de StorageGRID.

La eliminación del token del portador de StorageGRID funciona de la misma forma que sin SSO. Si no se proporciona 'cookie 'sso=true', el usuario se cierra la sesión de StorageGRID sin afectar al estado de SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

1. `204 No Content` la respuesta indica que el usuario ha cerrado la sesión.

```
HTTP/1.1 204 No Content
```

Use la API si el inicio de sesión único está habilitado (Azure)

Si lo tiene "Inicio de sesión único configurado y habilitado (SSO)" Además, utilice Azure como proveedor SSO, puede utilizar dos scripts de ejemplo para obtener un token de autenticación válido para la API de gestión de grid o la API de gestión de inquilinos.

Inicie sesión en la API si el inicio de sesión único de Azure está habilitado

Estas instrucciones se aplican si utiliza Azure como proveedor de identidades de SSO

Antes de empezar

- Conoce la dirección de correo electrónico y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar las siguientes secuencias de comandos de ejemplo:

- La `storagegrid-ssoauth-azure.py` Guión Python
- La `storagegrid-ssoauth-azure.js` Secuencia de comandos Node.js

Ambos scripts se encuentran en el directorio de archivos de instalación de StorageGRID (`./rpms` Para Red Hat Enterprise Linux, `./debs` Para Ubuntu o Debian, y. `./vsphere` Para VMware).

Para escribir su propia integración de API con Azure, consulte `storagegrid-ssoauth-azure.py` guión. El script de Python hace dos solicitudes a StorageGRID directamente (primero para obtener el SAMLRequest, y más tarde para obtener el token de autorización), y también llama al script Node.js para interactuar con Azure para realizar las operaciones de SSO.

Las operaciones SSO se pueden ejecutar mediante una serie de solicitudes API, pero hacerlo no es sencillo. El módulo Puppeteer Node.js se utiliza para raspar la interfaz SSO de Azure.

Si tiene un problema de codificación URL, puede que aparezca el error: `Unsupported SAML version`.

Pasos

1. Instale las dependencias necesarias de la siguiente manera:
   a. Instale Node.js (consulte "https://nodejs.org/en/download/").

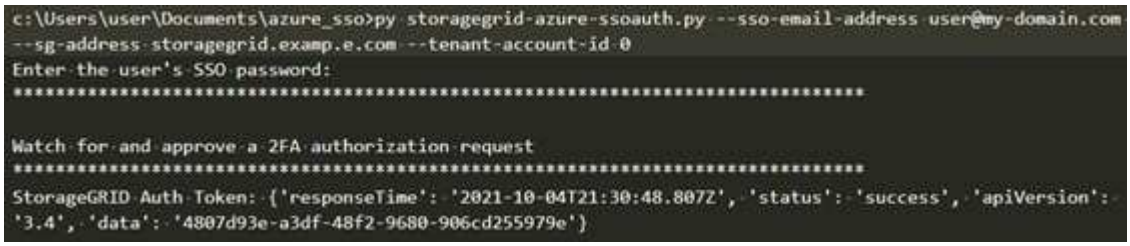
b. Instale los módulos Node.js necesarios (tippeteer y jsdom):

```
npm install -g <module>
```

2. Pase la secuencia de comandos de Python al intérprete de Python para ejecutar la secuencia de comandos.

   La secuencia de comandos Python llamará al script Node.js correspondiente para realizar las interacciones de SSO de Azure.

3. Cuando se le solicite, introduzca valores para los siguientes argumentos (o bien, pasarlos mediante parámetros):
   - La dirección de correo electrónico de SSO que se utiliza para iniciar sesión en Azure
   - La dirección de StorageGRID
   - El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos
4. Cuando se le solicite, introduzca la contraseña y esté preparado para proporcionar una autorización de MFA para Azure si así se lo solicita.



> La secuencia de comandos asume que la MFA se realiza utilizando Microsoft Authenticator. Es posible que necesite modificar el script para admitir otras formas de MFA (como introducir un código recibido en un mensaje de texto).

El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.

Utilizar la API si está activado el inicio de sesión único (PingFederate)

Si lo tiene "Inicio de sesión único configurado y habilitado (SSO)" Además, debe utilizar PingFederate como proveedor SSO, para obtener un token de autenticación válido para la API de gestión de grid o la API de gestión de inquilinos, debe emitir una serie de solicitudes API.

Inicie sesión en la API si está habilitado el inicio de sesión único

Estas instrucciones se aplican si está utilizando PingFederate como proveedor de identidades SSO

Antes de empezar

- Conoce el nombre de usuario y la contraseña de SSO para un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si desea acceder a la API de gestión de inquilinos, conoce el ID de cuenta de inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar uno de los siguientes ejemplos:

- La `storagegrid-ssoauth.py` Script Python, que se encuentra en el directorio de archivos de instalación de StorageGRID (`./rpms` Para Red Hat Enterprise Linux, `./debs` Para Ubuntu o Debian, y. `./vsphere` Para VMware).
- Ejemplo de flujo de trabajo de solicitudes curl.

  El flujo de trabajo curl podría llegar a ocurrir si lo hace demasiado lentamente. Es posible que aparezca el error: `A valid SubjectConfirmation was not found on this Response`.

  > El flujo de trabajo curl de ejemplo no protege la contraseña de ser vista por otros usuarios.

  Si tiene un problema de codificación URL, puede que aparezca el error: `Unsupported SAML version`.

Pasos

1. Seleccione uno de los siguientes métodos para obtener un token de autenticación:
   - Utilice la `storagegrid-ssoauth.py` Guión Python. Vaya al paso 2.
   - Usar solicitudes curl. Vaya al paso 3.
2. Si desea utilizar el `storagegrid-ssoauth.py` Guión, pase el script al intérprete Python y ejecute el script.

   Cuando se le solicite, escriba valores para los siguientes argumentos:

   - El método SSO. Puede introducir cualquier variación de “pingfederate” (PINGFEDERATE, pingfederate, etc.).
   - El nombre de usuario de SSO
   - El dominio en el que está instalado StorageGRID. Este campo no se utiliza para PingFederate. Puede dejarlo en blanco o introducir cualquier valor.
   - La dirección de StorageGRID
   - El ID de cuenta de inquilino, si desea acceder a la API de gestión de inquilinos.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   El token de autorización de StorageGRID se proporciona en la salida. Ahora puede utilizar el token para otras solicitudes, de forma similar a cómo utilizaría la API si no se estuviera utilizando SSO.
3. Si desea usar solicitudes curl, use el siguiente procedimiento.
   a. Declare las variables necesarias para iniciar sesión.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

Para acceder a la API de gestión de grid, utilice 0 AS `TENANTACCOUNTID`.

b. Para recibir una URL de autenticación firmada, emita una solicitud DE ENVÍO `/api/v3/authorize-saml`, Y quite la codificación JSON adicional de la respuesta.

En este ejemplo se muestra una solicitud POST para una dirección URL de autenticación firmada para TENANTACCOUNTID. Los resultados se pasan a python -m json.tool para quitar la codificación JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La respuesta de este ejemplo incluye una dirección URL firmada codificada por URL, pero no incluye la capa de codificación JSON adicional.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Guarde la `SAMLRequest` de la respuesta para su uso en comandos posteriores.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. Exporte la respuesta y el cookie y añada la respuesta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Exporte el valor 'pf.adapterId' y añada la respuesta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Exporte el valor 'href' (retire la barra diagonal inversa /) y añada la respuesta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Exporte el valor de 'acción':

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Enviar cookies junto con credenciales:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Guarde la `SAMLResponse` en el campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizando el guardado `SAMLResponse`, Haga un StorageGRID`/api/saml-response` Solicitud para generar un token de autenticación de StorageGRID.

Para `RelayState`, Utilice el ID de cuenta de arrendatario o utilice 0 si desea iniciar sesión en la API de administración de grid.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La respuesta incluye el token de autenticación.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Guarde el token de autenticación en la respuesta como `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ahora puede utilizar `MYTOKEN` Para otras solicitudes, del mismo modo que utilizaría la API si no se utiliza SSO.

Cierre sesión en la API si el inicio de sesión único está habilitado

Si se ha activado el inicio de sesión único (SSO), debe emitir una serie de solicitudes API para cerrar sesión en la API de gestión de grid o en la API de gestión de inquilinos.
Estas instrucciones se aplican si está utilizando PingFederate como proveedor de identidades SSO

Acerca de esta tarea

Si es necesario, puede cerrar sesión en la API de StorageGRID cerrando sesión en la página de cierre de sesión único de su organización. O bien, puede activar el cierre de sesión único (SLO) desde StorageGRID, que requiere un token de portador de StorageGRID válido.

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase la cookie «sso=true» a la API de SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Se devuelve una URL de cierre de sesión:

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Guarde la URL de cierre de sesión.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Envíe una solicitud a la URL de cierre de sesión para activar SLO y redirigir de nuevo a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Se devuelve la respuesta de 302. La ubicación de redirección no se aplica a la salida de sólo API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Elimine el token del portador de StorageGRID.

La eliminación del token del portador de StorageGRID funciona de la misma forma que sin SSO. Si no se proporciona 'cookie 'sso=true', el usuario se cierra la sesión de StorageGRID sin afectar al estado de SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

1. `204 No Content` la respuesta indica que el usuario ha cerrado la sesión.

```
HTTP/1.1 204 No Content
```

Desactivar las funcionalidades con la API

Puede utilizar la API de gestión de grid para desactivar por completo determinadas

funciones del sistema StorageGRID. Cuando se desactiva una función, no se pueden asignar permisos a nadie para realizar las tareas relacionadas con esa función.

Acerca de esta tarea

El sistema de funciones desactivadas le permite impedir el acceso a determinadas funciones del sistema StorageGRID. La desactivación de una característica es la única forma de impedir que el usuario raíz o los usuarios que pertenecen a grupos de administración con permiso **acceso raíz** puedan utilizar esa función.

Para comprender cómo puede ser útil esta funcionalidad, considere el siguiente escenario:

Company A es un proveedor de servicios que arrienda la capacidad de almacenamiento de su sistema StorageGRID mediante la creación de cuentas de inquilino. Para proteger la seguridad de los objetos de sus arrendatarios, la Compañía A desea asegurarse de que sus propios empleados nunca tengan acceso a ninguna cuenta de arrendatario después de que se haya implementado la cuenta.

*La empresa A puede lograr este objetivo mediante el sistema Desactivar características en la API de gestión de grid. Al desactivar completamente la característica **Cambiar contraseña raíz de arrendatario** en Grid Manager (tanto la interfaz de usuario como la API), la Compañía A puede garantizar que ningún usuario de administrador (incluido el usuario raíz y los usuarios pertenecientes a grupos con el permiso **acceso raíz**) puede cambiar la contraseña para el usuario raíz de cualquier cuenta de arrendatario.*

Pasos

1. Acceda a la documentación de Swagger para la API de Grid Management. Consulte "Utilice la API de gestión de grid".
2. Busque el extremo Desactivar funciones.
3. Para desactivar una función, como Cambiar contraseña raíz de inquilino, envíe un cuerpo a la API de este modo:

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   Cuando se completa la solicitud, la función Cambiar contraseña raíz de inquilino está desactivada. El permiso de administración de **Change tenant root password** ya no aparece en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña root para un inquilino fallará con “403 Forbidden”.

Reactivar las funciones desactivadas

De forma predeterminada, puede utilizar la API de administración de grid para reactivar una función que se haya desactivado. Sin embargo, si desea evitar que alguna vez se reactiven las funciones desactivadas, puede desactivar la propia función **activateFeatures**.

> La función **activateFeatures** no se puede reactivar. Si decide desactivar esta función, tenga en cuenta que perderá permanentemente la capacidad de reactivar otras funciones desactivadas. Para restaurar cualquier funcionalidad perdida, debe ponerse en contacto con el soporte técnico.

Pasos

1. Acceda a la documentación de Swagger para la API de Grid Management.
2. Busque el extremo Desactivar funciones.
3. Para reactivar todas las funciones, envíe un cuerpo a la API de este modo:

```
{ "grid": null }
```

Cuando se completa esta solicitud, se reactivan todas las funciones, incluida la función Cambiar contraseña raíz del inquilino. El permiso de administración **Cambiar contraseña raíz de arrendatario** aparece ahora en la interfaz de usuario y cualquier solicitud de API que intente cambiar la contraseña raíz de un inquilino se realizará correctamente, suponiendo que el usuario tenga el permiso de administración **acceso raíz** o **Cambiar contraseña raíz de inquilino**.

> ⓘ El ejemplo anterior hace que se reactiven las funciones *all* desactivadas. Si se han desactivado otras funciones que deben permanecer desactivadas, debe especificarlas explícitamente en la solicitud PUT. Por ejemplo, para reactivar la función Cambiar contraseña raíz de arrendatario y continuar desactivando la función de confirmación de alarma, envíe esta solicitud DE ENVÍO:
>
> ```
> { "grid": { "alarmAcknowledgment": true } }
> ```

Control del acceso a StorageGRID

Control de acceso StorageGRID: Descripción general

Puede controlar quién puede acceder a StorageGRID y qué tareas pueden realizar los usuarios creando o importando grupos y usuarios, y asignando permisos a cada grupo. De manera opcional, puede habilitar el inicio de sesión único (SSO), crear certificados de cliente y cambiar contraseñas de grid.

Controle el acceso a Grid Manager

Para determinar quién puede acceder a Grid Manager y a la API de gestión de grid, importe grupos y usuarios desde un servicio de federación de identidades o configure grupos locales y usuarios locales.

Uso "federación de identidades" realiza la configuración "grupos" y.. "usuarios" Más rápido, y permite a los usuarios iniciar sesión en StorageGRID usando credenciales conocidas. Puede configurar la federación de identidades si utiliza Active Directory, OpenLDAP u Oracle Directory Server.

> ⓘ Póngase en contacto con el soporte técnico si desea utilizar otro servicio LDAP v3.

Puede determinar qué tareas puede realizar cada usuario asignando diferentes "permisos" a cada grupo. Por ejemplo, es posible que desee que los usuarios de un grupo puedan gestionar las reglas de ILM y los usuarios de otro grupo para realizar tareas de mantenimiento. Un usuario debe pertenecer al menos a un grupo para acceder al sistema.

De manera opcional, puede configurar un grupo para que sea de sólo lectura. Los usuarios de un grupo de sólo lectura sólo pueden ver la configuración y las funciones. No pueden realizar cambios ni realizar ninguna operación en Grid Manager o la API de administración de grid.

Active el inicio de sesión único

El sistema StorageGRID admite el inicio de sesión único (SSO) con el estándar de lenguaje de marcado de aserción de seguridad 2.0 (SAML 2.0). Usted primero "Configure y habilite SSO", Todos los usuarios deben ser autenticados por un proveedor de identidad externo antes de que puedan acceder a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API. Los usuarios locales no pueden iniciar sesión en StorageGRID.

Cambie la clave de acceso de aprovisionamiento

La clave de acceso de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, así como para descargar el paquete de recuperación de StorageGRID. También se necesita la contraseña para descargar los backups de la información de topología de la cuadrícula y las claves de cifrado del sistema StorageGRID. Puede hacerlo "cambie la contraseña" según sea necesario.

Cambie las contraseñas de la consola de los nodos

Cada nodo de su grid tiene una contraseña única de la consola de nodos, la cual necesita iniciar sesión en el nodo como «administrador» mediante SSH, o al usuario raíz en una conexión de consola física o de máquina virtual. Según sea necesario, puedes "cambie la contraseña de la consola del nodo" para cada nodo.

Cambie la clave de acceso del aprovisionamiento

Use este procedimiento para cambiar la clave de acceso de aprovisionamiento de StorageGRID. La frase de acceso es necesaria para los procedimientos de recuperación, expansión y mantenimiento. La clave de acceso también se requiere para descargar los backups del paquete de recuperación que incluyen la información de topología de la cuadrícula, las contraseñas de la consola del nodo de la cuadrícula y las claves de cifrado del sistema StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permisos de acceso raíz o de mantenimiento.
- Tiene la clave de acceso de aprovisionamiento actual.

Acerca de esta tarea

La clave de acceso de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para "Descarga del paquete de recuperación". La clave de acceso de aprovisionamiento no aparece en la `Passwords.txt` archivo. Asegúrese de documentar la frase de acceso de aprovisionamiento y mantenerla en una ubicación segura.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso**> **contraseñas de cuadrícula**.
2. En **Cambiar contraseña de aprovisionamiento**, selecciona **Hacer un cambio**
3. Introduzca la clave de acceso de aprovisionamiento actual.
4. Introduzca la nueva frase de contraseña. La frase de contraseña debe contener al menos 8 caracteres y no más de 32. Las passphrasas distinguen entre mayúsculas y minúsculas.
5. Almacene la nueva clave de acceso de aprovisionamiento en una ubicación segura. Es necesario para los procedimientos de instalación, expansión y mantenimiento.
6. Vuelva a introducir la nueva contraseña y seleccione **Guardar**.

   El sistema muestra un banner verde de éxito cuando se completa el cambio de la clave de acceso de aprovisionamiento.

7. Seleccione **paquete de recuperación**.

8. Introduzca la nueva clave de acceso de aprovisionamiento para descargar el nuevo paquete de recuperación.

> Después de cambiar la contraseña de aprovisionamiento, debe descargar inmediatamente un nuevo paquete de recuperación. El archivo de paquete de recuperación permite restaurar el sistema si se produce un fallo.

Cambie las contraseñas de la consola de los nodos

Cada nodo de su grid tiene una contraseña de consola de nodo única, que necesita iniciar sesión en el nodo. Siga estos pasos para cambiar cada contraseña de la consola de nodos única para cada nodo de la cuadrícula.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento actual.

Acerca de esta tarea

Utilice la contraseña de la consola del nodo para iniciar sesión en un nodo como «administrador» mediante SSH, o para el usuario raíz en una conexión de consola física/máquina virtual. El proceso de cambiar la contraseña de la consola del nodo crea nuevas contraseñas para cada nodo de la cuadrícula y almacena las contraseñas en una actualización `Passwords.txt` en el paquete de recuperación. Las contraseñas se enumeran en la columna Password del archivo Passwords.txtl.

> Hay contraseñas de acceso SSH separadas para las claves SSH que se usan para la comunicación entre nodos. Este procedimiento no modifica las contraseñas de acceso SSH.

Acceda al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **contraseñas de cuadrícula**.
2. En **Cambiar contraseñas de consola de nodo**, selecciona **Hacer un cambio**.

Introduzca la clave de acceso de aprovisionamiento

Pasos

1. Introduzca la clave de acceso de aprovisionamiento para el grid.
2. Seleccione **continuar**.

Descargue el paquete de recuperación actual

Antes de cambiar las contraseñas de la consola del nodo, descargue el paquete de recuperación actual. Puede usar las contraseñas de este archivo si el proceso de cambio de contraseña falla en cualquier nodo.

Pasos

1. Seleccione **Descargar paquete de recuperación**.
2. Copie el archivo del paquete de recuperación (`.zip`) a dos ubicaciones seguras, seguras y separadas.

El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID.

3. Seleccione **continuar**.
4. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí** si está listo para empezar a cambiar las contraseñas de la consola del nodo.

   No puede cancelar este proceso una vez que se inicia.

Cambie las contraseñas de la consola de los nodos

Cuando se inicia el proceso de contraseña de la consola del nodo, se genera un nuevo paquete de recuperación que incluye las nuevas contraseñas. A continuación, las contraseñas se actualizan en cada nodo.

Pasos

1. Espere a que se genere el nuevo paquete de recuperación, lo que puede tardar unos minutos.
2. Seleccione **Descargar nuevo paquete de recuperación**.
3. Cuando finalice la descarga:

   a. Abra el `.zip` archivo.

   b. Confirme que puede acceder al contenido, incluido el `Passwords.txt` archivo, que contiene las nuevas contraseñas de la consola del nodo.

   c. Copie el nuevo archivo del paquete de recuperación (`.zip`) a dos ubicaciones seguras, seguras y separadas.

   No sobrescriba el paquete de recuperación antiguo.

   El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID.

4. Marque la casilla de verificación para indicar que ha descargado el nuevo paquete de recuperación y verificado el contenido.
5. Seleccione **Cambiar contraseñas de consola de nodos** y espere a que todos los nodos se actualicen con las nuevas contraseñas. Esto puede tardar varios minutos.

   Si se modifican contraseñas para todos los nodos, se muestra un banner verde de éxito. Vaya al paso siguiente.

   Si se produce un error durante el proceso de actualización, un mensaje de banner enumera la cantidad de nodos que no pudieron cambiar sus contraseñas. El sistema volverá a intentar automáticamente el proceso en cualquier nodo que no haya cambiado su contraseña. Si el proceso finaliza con algunos nodos que aún no han cambiado la contraseña, aparece el botón **Reintentar**.

   Si la actualización de la contraseña falló para uno o más nodos:

   a. Revise los mensajes de error que aparecen en la tabla.

   b. Resuelva los problemas.

   c. Seleccione **Reintentar**.

> Al volver a intentar solo se cambian las contraseñas de la consola de nodos en los nodos que fallaron durante los intentos anteriores de cambio de contraseña.

6. Después de cambiar las contraseñas de la consola de nodos para todos los nodos, elimine el primer paquete de recuperación que descargó.
7. Opcionalmente, utilice el enlace **Recovery package** para descargar una copia adicional del nuevo paquete de recuperación.

Usar la federación de identidades

El uso de la federación de identidades agiliza la configuración de grupos y usuarios y permite a los usuarios iniciar sesión en StorageGRID utilizando credenciales conocidas.

Configurar la federación de identidades para Grid Manager

Puede configurar la federación de identidades en Grid Manager si desea que los grupos y usuarios de administración se gestionen en otro sistema como Active Directory, Azure Active Directory (Azure AD), OpenLDAP u Oracle Directory Server.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Se utiliza Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidades.

> Si desea utilizar un servicio LDAP v3 que no esté en la lista, póngase en contacto con el soporte técnico.

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Consulte Instrucciones para configurar un servidor OpenLDAP.
- Si tiene pensado habilitar el inicio de sesión único (SSO), ha revisado el "requisitos y consideraciones para el inicio de sesión único".
- Si planea utilizar la seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidades usa TLS 1.2 o 1.3. Consulte "Cifrados compatibles para conexiones TLS salientes".

Acerca de esta tarea

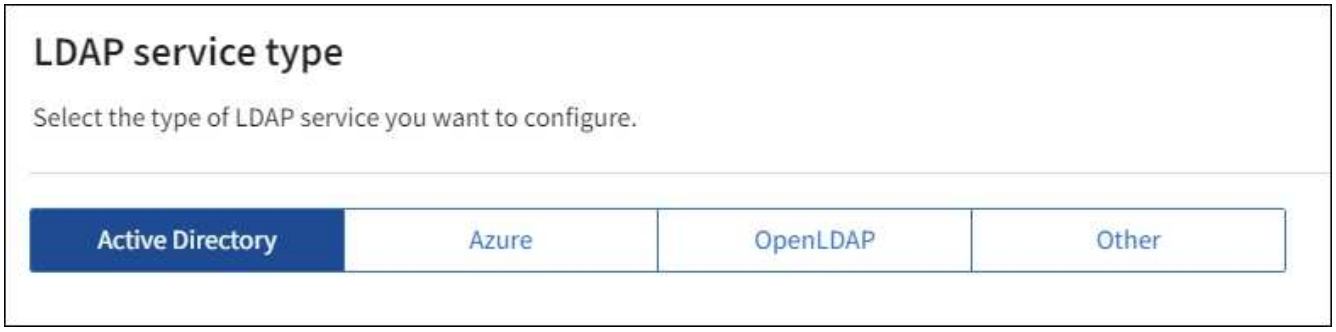
Puede configurar un origen de identidades para Grid Manager si desea importar grupos de otro sistema, como Active Directory, Azure AD, OpenLDAP u Oracle Directory Server. Puede importar los siguientes tipos de grupos:

- Grupos de administración. Los usuarios de los grupos de administración pueden iniciar sesión en Grid Manager y realizar tareas basándose en los permisos de administración asignados al grupo.
- Grupos de usuarios de inquilinos para inquilinos que no utilizan su propio origen de identidad. Los usuarios de grupos de inquilinos pueden iniciar sesión en el Administrador de inquilinos y realizar tareas, en función de los permisos asignados al grupo en el Administrador de inquilinos. Consulte "Cree una cuenta de inquilino" y.. "Usar una cuenta de inquilino" para obtener más detalles.

Introduzca la configuración

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **federación de identidades**.
2. Seleccione **Activar federación de identidades**.
3. En la sección Tipo de servicio LDAP, seleccione el tipo de servicio LDAP que desea configurar.



   Seleccione **otros** para configurar valores para un servidor LDAP que utilice Oracle Directory Server.

4. Si ha seleccionado **otros**, complete los campos de la sección atributos LDAP . De lo contrario, vaya al paso siguiente.
   - **Nombre único de usuario**: Nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo es equivalente a. `sAMAccountName` Para Active Directory y. `uid` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `uid`.
   - **UUID de usuario**: Nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a. `objectGUID` Para Active Directory y. `entryUUID` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `nsuniqueid`. El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
   - **Nombre único del grupo**: Nombre del atributo que contiene el identificador único de un grupo LDAP. Este atributo es equivalente a. `sAMAccountName` Para Active Directory y. `cn` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `cn`.
   - **UUID de grupo**: Nombre del atributo que contiene el identificador único permanente de un grupo LDAP. Este atributo es equivalente a. `objectGUID` Para Active Directory y. `entryUUID` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `nsuniqueid`. El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
5. Para todos los tipos de servicio LDAP, introduzca la información de servidor LDAP y conexión de red necesaria en la sección Configure LDAP Server.
   - **Hostname**: El nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP.
   - **Puerto**: El puerto utilizado para conectarse al servidor LDAP.

     El puerto predeterminado para STARTTLS es 389 y el puerto predeterminado para LDAPS es 636. Sin embargo, puede utilizar cualquier puerto siempre que su firewall esté configurado correctamente.

   - **Nombre de usuario**: La ruta completa del nombre completo (DN) para el usuario que se conectará al servidor LDAP.

Para Active Directory, también puede especificar el nombre de inicio de sesión de nivel inferior o el nombre principal del usuario.

El usuario especificado debe tener permiso para enumerar grupos y usuarios y para tener acceso a los siguientes atributos:

- `sAMAccountName` o. `uid`
- `objectGUID`, `entryUUID`, o. `nsuniqueid`
- `cn`
- `memberOf` o. `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, y. `userPrincipalName`
- **Azure**: `accountEnabled` y.. `userPrincipalName`

◦ **Contraseña**: La contraseña asociada al nombre de usuario.

> Si cambia la contraseña en el futuro, debe actualizarla en esta página.

◦ **DN base de grupo**: La ruta completa del nombre distinguido (DN) para un subárbol LDAP que desea buscar grupos. En el ejemplo de Active Directory (a continuación), se pueden usar como grupos federados todos los grupos cuyo nombre distintivo sea relativo al DN base (DC=storagegrid,DC=example,DC=com).

> Los valores de **Nombre único de grupo** deben ser únicos dentro del **DN base de grupo** al que pertenecen.

◦ **DN base de usuario**: La ruta completa del nombre completo (DN) de un subárbol LDAP que desea buscar usuarios.

> Los valores de **Nombre único de usuario** deben ser únicos dentro del **DN base de usuario** al que pertenecen.

◦ **Formato de nombre de usuario de enlace** (opcional): El patrón de nombre de usuario predeterminado StorageGRID debe usarse si el patrón no se puede determinar automáticamente.

Se recomienda proporcionar **Formato de nombre de usuario Bind** porque puede permitir que los usuarios inicien sesión si StorageGRID no puede enlazar con la cuenta de servicio.

Introduzca uno de estos patrones:

- **Patrón UserPrincipalName (Active Directory y Azure)**: `[USERNAME]@*example*.com`
- **Patrón de nombre de inicio de sesión de nivel inferior (Active Directory y Azure)**: `*example*\[USERNAME]`
- **Patrón de nombre completo**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Incluya **[USERNAME]** exactamente como está escrito.

6. En la sección Seguridad de la capa de transporte (TLS), seleccione una configuración de seguridad.
   ◦ **Use STARTTLS**: Utilice STARTTLS para asegurar las comunicaciones con el servidor LDAP. Esta es

la opción recomendada para Active Directory, OpenLDAP u otros, pero esta opción no es compatible con Azure.

- **Use LDAPS**: La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debe seleccionar esta opción para Azure.
- **No utilice TLS**: El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Azure.

> El uso de la opción **no usar TLS** no es compatible si el servidor de Active Directory aplica la firma LDAP. Debe usar STARTTLS o LDAPS.

7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.
   - **Utilizar certificado CA del sistema operativo**: Utilice el certificado predeterminado de CA de red instalado en el sistema operativo para asegurar las conexiones.
   - **Utilizar certificado de CA personalizado**: Utilice un certificado de seguridad personalizado.

     Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto del certificado de CA.

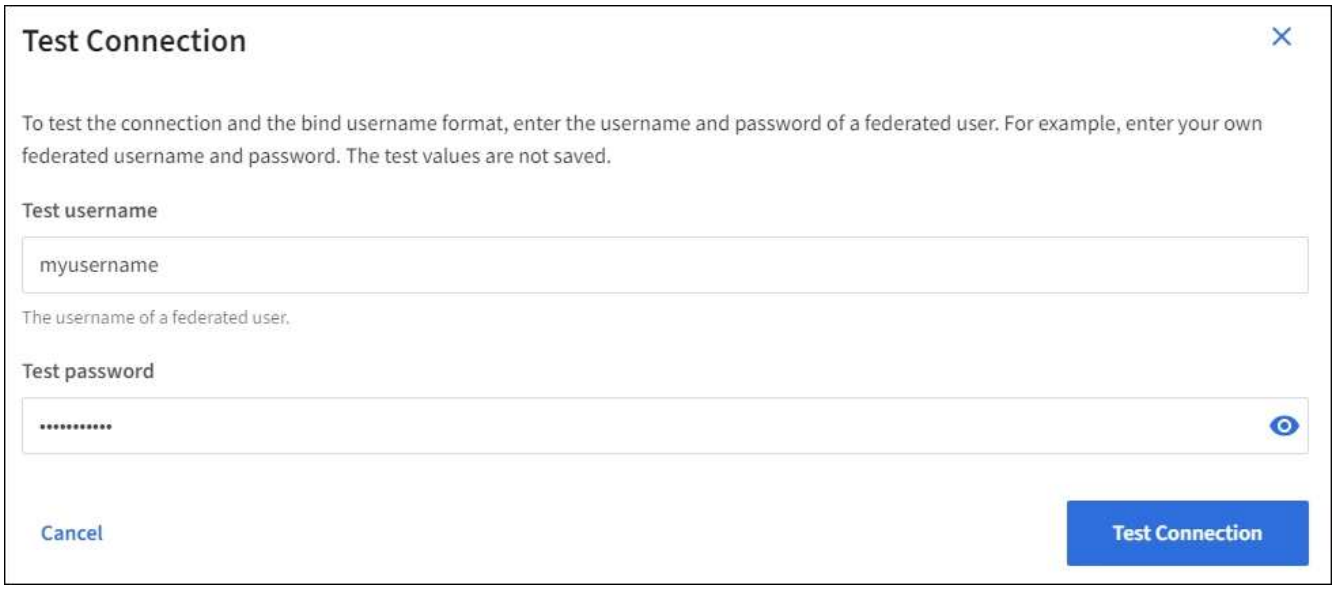
Pruebe la conexión y guarde la configuración

Después de introducir todos los valores, es necesario probar la conexión para poder guardar la configuración. StorageGRID verifica la configuración de conexión del servidor LDAP y el formato de nombre de usuario de enlace, si proporcionó uno.

Pasos

1. Seleccione **probar conexión**.
2. Si no se proporciona un formato de nombre de usuario de enlace:
   - Si la configuración de conexión es válida, aparecerá un mensaje que indica que la conexión se ha realizado correctamente. Seleccione **Guardar** para guardar la configuración.
   - Si la configuración de conexión no es válida, aparecerá un mensaje que indica que no se ha podido establecer la conexión de prueba. Seleccione **Cerrar**. Luego, resuelva cualquier problema y vuelva a probar la conexión.
3. Si proporcionó un formato de nombre de usuario de enlace, introduzca el nombre de usuario y la contraseña de un usuario federado válido.

   Por ejemplo, introduzca su propio nombre de usuario y contraseña. No incluya ningún carácter especial en el nombre de usuario, como @ o /.



- Si la configuración de conexión es válida, aparecerá un mensaje que indica que la conexión se ha realizado correctamente. Seleccione **Guardar** para guardar la configuración.
- Aparecerá un mensaje de error si las opciones de conexión, el formato de nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva los problemas y vuelva a probar la conexión.

Forzar la sincronización con el origen de identidades

El sistema StorageGRID sincroniza periódicamente grupos federados y usuarios del origen de identidades. Puede forzar el inicio de la sincronización si desea habilitar o restringir los permisos de usuario lo antes posible.

Pasos

1. Vaya a la página federación de identidades.
2. Seleccione **servidor de sincronización** en la parte superior de la página.

   El proceso de sincronización puede tardar bastante tiempo en función del entorno.

   La alerta **fallo de sincronización de la federación de identidades** se activa si hay un problema al sincronizar grupos federados y usuarios del origen de identidades.

Deshabilitar la federación de identidades

Puede deshabilitar temporalmente o de forma permanente la federación de identidades para grupos y usuarios. Cuando la federación de identidades está deshabilitada, no existe comunicación entre StorageGRID y el origen de identidades. Sin embargo, cualquier configuración que haya configurado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidades en el futuro.

Acerca de esta tarea

Antes de deshabilitar la federación de identidades, debe tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que hayan iniciado sesión en ese momento, retendrán el acceso al sistema StorageGRID hasta que caduque la sesión, pero no podrán iniciar sesión después de que caduque la

sesión.

- No se realizará la sincronización entre el sistema StorageGRID y el origen de identidad, y no se realizarán alertas ni alarmas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Habilitar federación de identidad** está desactivada si el inicio de sesión único (SSO) está configurado en **enabled** o **Sandbox Mode**. El estado de SSO de la página Single Sign-On debe ser **Desactivado** antes de poder deshabilitar la federación de identidades. Consulte "Desactive el inicio de sesión único".

Pasos

1. Vaya a la página federación de identidades.
2. Desmarque la casilla de verificación **Habilitar federación de identidad**.

Instrucciones para configurar un servidor OpenLDAP

Si desea utilizar un servidor OpenLDAP para la federación de identidades, debe configurar ajustes específicos en el servidor OpenLDAP.

> En el caso de fuentes de identidad que no sean ActiveDirectory ni Azure, StorageGRID no bloqueará automáticamente el acceso S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine cualquier clave S3 para el usuario o elimine al usuario de todos los grupos.

Revestimientos memberOf y reft

Se deben habilitar las superposiciones memberof y reft. Para obtener más información, consulte las instrucciones para el mantenimiento de miembros del grupo inverso en "Documentación de OpenLDAP: Guía del administrador de la versión 2.4".

Indización

Debe configurar los siguientes atributos OpenLDAP con las palabras clave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Además, asegúrese de que los campos mencionados en la ayuda para Nombre de usuario estén indexados para un rendimiento óptimo.

Consulte la información sobre el mantenimiento de pertenencia a grupos inversa en la "Documentación de OpenLDAP: Guía del administrador de la versión 2.4".

Gestione los grupos de administradores

Es posible crear grupos de administración para gestionar los permisos de seguridad de uno o más usuarios de administrador. Los usuarios deben pertenecer a un grupo para tener acceso al sistema StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Si planea importar un grupo federado, ha configurado la federación de identidades y el grupo federado ya existe en el origen de identidades configurado.

Cree un grupo de administración

Los grupos de administración permiten determinar a qué usuarios se puede acceder a qué características y operaciones en Grid Manager y en la API de gestión de grid.

Acceda al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **grupos de administración**.
2. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

- Cree un grupo local si desea asignar permisos a los usuarios locales.
- Cree un grupo federado para importar usuarios desde el origen de identidades.

Grupo local

Pasos

1. Seleccione **Grupo local**.
2. Introduzca un nombre para mostrar para el grupo, que puede actualizar más adelante si es necesario. Por ejemplo, «Usuarios de mantenimiento» o «Administradores de ILM».
3. Introduzca un nombre único para el grupo, que no podrá actualizar más tarde.
4. Seleccione **continuar**.

Grupo federado

Pasos

1. Seleccione **Grupo federado**.
2. Introduzca el nombre del grupo que desea importar, exactamente como aparece en el origen de identidad configurado.
   - Para Active Directory y Azure, utilice sAMAccountName.
   - Para OpenLDAP, utilice CN (Nombre común).
   - Para otro LDAP, utilice el nombre exclusivo adecuado para el servidor LDAP.
3. Seleccione **continuar**.

Administrar permisos de grupo

Pasos

1. En **modo de acceso**, seleccione si los usuarios del grupo pueden cambiar la configuración y realizar operaciones en Grid Manager y la API de gestión de grid o si sólo pueden ver la configuración y las

características.

- **Read-write** (predeterminado): Los usuarios pueden cambiar la configuración y realizar las operaciones permitidas por sus permisos de administración.
- **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden realizar cambios ni realizar ninguna operación en Grid Manager o la API de administración de grid. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

> Si un usuario pertenece a varios grupos y cualquier grupo está establecido en **sólo lectura**, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

2. Seleccione uno o varios "permisos de grupo de administración".

   Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios que pertenezcan al grupo no podrán iniciar sesión en StorageGRID.

3. Si está creando un grupo local, seleccione **continuar**. Si está creando un grupo federado, seleccione **Crear grupo** y **Finalizar**.

Añadir usuarios (sólo grupos locales)

Pasos

1. Opcionalmente, seleccione uno o varios usuarios locales para este grupo.

   Si todavía no ha creado usuarios locales, puede guardar el grupo sin agregar usuarios. Puede agregar este grupo al usuario en la página usuarios. Consulte "Gestionar usuarios" para obtener más detalles.

2. Seleccione **Crear grupo** y **Finalizar**.

Consulte y edite los grupos de administración

Puede ver los detalles de los grupos existentes, modificar un grupo o duplicar un grupo.

- Para ver información básica de todos los grupos, revise la tabla de la página grupos.
- Para ver todos los detalles de un grupo específico o editar un grupo, utilice el menú **acciones** o la página de detalles.

Tarea	Menú Actions	Detalles
Ver detalles del grupo	a. Seleccione la casilla de verificación para el grupo. b. Seleccione **acciones** > **Ver detalles del grupo**.	Seleccione el nombre del grupo en la tabla.

Tarea	Menú Actions	Detalles
Editar nombre para mostrar (sólo grupos locales)	a. Seleccione la casilla de verificación para el grupo. b. Seleccione **acciones** > **Editar nombre de grupo**. c. Introduzca el nuevo nombre. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del grupo para mostrar los detalles. b. Seleccione el icono de edición . c. Introduzca el nuevo nombre. d. Seleccione **Guardar cambios**.
Edite el modo de acceso o los permisos	a. Seleccione la casilla de verificación para el grupo. b. Seleccione **acciones** > **Ver detalles del grupo**. c. Si lo desea, cambie el modo de acceso del grupo. d. Opcionalmente, seleccione o desactive "permisos de grupo de administración". e. Seleccione **Guardar cambios**.	a. Seleccione el nombre del grupo para mostrar los detalles. b. Si lo desea, cambie el modo de acceso del grupo. c. Opcionalmente, seleccione o desactive "permisos de grupo de administración". d. Seleccione **Guardar cambios**.

Duplicar un grupo

Pasos

1. Seleccione la casilla de verificación para el grupo.
2. Seleccione **acciones** > **Duplicar grupo**.
3. Complete el asistente para grupos duplicados.

Eliminar un grupo

Es posible eliminar un grupo de administración cuando se desea quitar el grupo del sistema y quitar todos los permisos asociados con el grupo. Al eliminar un grupo de administración, se quitan todos los usuarios del grupo, pero no se eliminan los usuarios.

Pasos

1. En la página Groups, seleccione la casilla de comprobación de cada grupo que desea quitar.
2. Seleccione **acciones** > **Eliminar grupo**.
3. Seleccione **Eliminar grupos**.

Permisos de grupo de administradores

Al crear grupos de usuarios de administrador, debe seleccionar uno o más permisos para controlar el acceso a funciones específicas de Grid Manager. A continuación, puede asignar cada usuario a uno o varios de estos grupos de administración para determinar qué tareas puede realizar el usuario.

Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios pertenecientes a ese grupo no

podrán iniciar sesión en Grid Manager o en la API de gestión de grid.

De forma predeterminada, cualquier usuario que pertenezca a un grupo que tenga al menos un permiso puede realizar las siguientes tareas:

- Inicie sesión en Grid Manager
- Vea la consola
- Puede ver las páginas Nodes
- Supervise la topología de grid
- Ver las alertas actuales y resueltas
- Ver alarmas actuales e históricas (sistema heredado)
- Cambiar su propia contraseña (sólo usuarios locales)
- Ver cierta información proporcionada en las páginas de configuración y mantenimiento

Interacción entre permisos y modo de acceso

Para todos los permisos, la configuración del **modo de acceso** del grupo determina si los usuarios pueden cambiar la configuración y realizar operaciones o si sólo pueden ver la configuración y las características relacionadas. Si un usuario pertenece a varios grupos y cualquier grupo está establecido en **sólo lectura**, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

En las siguientes secciones se describen los permisos que se pueden asignar al crear o editar un grupo de administradores. Cualquier funcionalidad que no se haya mencionado explícitamente requiere el permiso **acceso raíz**.

Acceso raíz

Este permiso proporciona acceso a todas las funciones de administración de grid.

Confirmar alarmas (heredadas)

Este permiso proporciona acceso para reconocer y responder a alarmas (sistema heredado). Todos los usuarios que han iniciado sesión pueden ver las alarmas actuales e históricas.

Si desea que un usuario supervise la topología de la cuadrícula y reconozca únicamente las alarmas, debe asignar este permiso.

Cambiar la contraseña raíz del inquilino

Este permiso proporciona acceso a la opción **Cambiar contraseña raíz** de la página arrendatarios, lo que le permite controlar quién puede cambiar la contraseña del usuario raíz local del arrendatario. Este permiso también se usa para migrar claves S3 cuando se habilita la función de importación de claves S3. Los usuarios que no tienen este permiso no pueden ver la opción **Cambiar contraseña raíz**.

> Para conceder acceso a la página arrendatarios, que contiene la opción **Cambiar contraseña root**, también asigne el permiso **Cuentas de arrendatario**.

Configuración de la página de topología de grid

Este permiso permite acceder a las fichas Configuración de la página **SUPPORT** > **Tools** > **Topología de cuadrícula**.

ILM

Este permiso permite acceder a las siguientes opciones del menú **ILM**:

- Bases de datos
- Normativas
- Codificación de borrado
- Regiones
- Pools de almacenamiento

> Los usuarios deben tener los permisos **Other grid Configuration** y **Grid Topology page Configuration** para administrar los grados de almacenamiento.

Mantenimiento

Los usuarios deben tener permiso de mantenimiento para utilizar estas opciones:

- **CONFIGURACIÓN** > **Control de acceso**:
  - Contraseñas de grid
- **CONFIGURACIÓN** > **Red**:
  - Nombres de dominio de punto final S3
- **MANTENIMIENTO** > **tareas**:
  - Retirada
  - Expansión
  - Comprobación de existencia de objeto
  - Recuperación
- **MANTENIMIENTO** > **sistema**:
  - Paquete de recuperación
  - Actualización de software
- **SOPORTE** > **Herramientas**:
  - Registros

Los usuarios que no tienen el permiso de mantenimiento pueden ver, pero no editar, estas páginas:

- **MANTENIMIENTO** > **Red**:
  - Servidores DNS
  - Red Grid
  - Servidores NTP
- **MANTENIMIENTO** > **sistema**:
  - Licencia
- **CONFIGURACIÓN** > **Red**:
  - Nombres de dominio de punto final S3
- **CONFIGURACIÓN** > **Seguridad**:

    - Certificados
- **CONFIGURACIÓN** > **Supervisión**:
    - Servidor de auditoría y syslog

Gestionar alertas

Este permiso proporciona acceso a opciones para gestionar alertas. Los usuarios deben tener este permiso para gestionar las silencios, las notificaciones de alerta y las reglas de alerta.

Consulta de métricas

Este permiso proporciona acceso a:

- **SOPORTE** > **Herramientas** > **Métricas** página
- Consultas personalizadas de métricas de Prometheus utilizando la sección **Metrics** de la API de administración de grid
- Tarjetas del panel de control de Grid Manager que contienen métricas

Búsqueda de metadatos de objetos

Este permiso proporciona acceso a la página **ILM** > **Búsqueda de metadatos de objetos**.

Otra configuración de cuadrícula

Este permiso proporciona acceso a opciones de configuración de cuadrícula adicionales.

> Para ver estas opciones adicionales, los usuarios también deben tener el permiso **Configuración de página de topología de cuadrícula**.

- **ILM**:
    - Grados de almacenamiento
- **CONFIGURACIÓN** > **sistema**:
    - Opciones de almacenamiento
- **SOPORTE** > **Alarmas (heredado)**:
    - Eventos personalizados
    - Alarmas globales
    - Configuración de correo electrónico heredado
- **SOPORTE** > **OTRO**:
    - Coste del enlace

Administrador de dispositivos de almacenamiento

Este permiso proporciona:

- Acceso al SANtricity System Manager de E-Series en dispositivos de almacenamiento a través de Grid Manager.
- La capacidad de realizar tareas de solución de problemas y mantenimiento en la pestaña Gestionar unidades para los dispositivos que admiten estas operaciones.

Cuentas de inquilino

Este permiso permite:

- Acceda a la página Tenedores, donde puede crear, editar y eliminar cuentas de arrendatario
- Ver las políticas de clasificación de tráfico existentes
- Ver tarjetas de consola de Grid Manager que contienen detalles de arrendatario

Gestionar usuarios

Es posible ver usuarios locales y federados. También puede crear usuarios locales y asignarles grupos de administración locales para determinar a qué funciones de Grid Manager pueden acceder estos usuarios.

Antes de empezar

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

Cree un usuario local

Es posible crear uno o varios usuarios locales y asignar cada usuario a uno o varios grupos locales. Los permisos del grupo controlan a qué funciones de Grid Manager y la API de gestión de grid puede acceder el usuario.

Solo es posible crear usuarios locales. Utilice el origen de identidades externo para administrar grupos y usuarios federados.

Grid Manager incluye un usuario local predefinido, denominado «root». No puede eliminar el usuario root.

> Si el inicio de sesión único (SSO) está activado, los usuarios locales no pueden iniciar sesión en StorageGRID.

Acceda al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **usuarios de administración**.
2. Seleccione **Crear usuario**.

Introduzca las credenciales de usuario

Pasos

1. Introduzca el nombre completo del usuario, un nombre de usuario único y una contraseña.
2. Opcionalmente, seleccione **Sí** si este usuario no debe tener acceso a Grid Manager o a la API de gestión de grid.
3. Seleccione **continuar**.

Asignar a grupos

Pasos

1. Opcionalmente, asigne el usuario a uno o más grupos para determinar los permisos del usuario.

Si aún no ha creado grupos, puede guardar el usuario sin seleccionar grupos. Puede agregar este usuario a un grupo en la página grupos.

Si un usuario pertenece a varios grupos, los permisos son acumulativos. Consulte "Gestione los grupos de administradores" para obtener más detalles.

2. Seleccione **Crear usuario** y seleccione **Finalizar**.

Ver y editar usuarios locales

Es posible ver detalles de los usuarios locales y federados existentes. Es posible modificar un usuario local para cambiar el nombre completo, la contraseña o la pertenencia a grupos del usuario. También puede impedir temporalmente que un usuario acceda a Grid Manager y a la API de gestión de grid.

Solo puede editar usuarios locales. Utilice el origen de identidad externo para administrar usuarios federados.

- Para ver la información básica de todos los usuarios locales y federados, revise la tabla en la página Users.
- Para ver todos los detalles de un usuario específico, editar un usuario local o cambiar la contraseña de un usuario local, utilice el menú **acciones** o la página de detalles.

  Las modificaciones se aplican la próxima vez que el usuario cierre sesión y vuelva a acceder al Gestor de cuadrícula.

> Los usuarios locales pueden cambiar sus propias contraseñas usando la opción **Cambiar contraseña** en el banner de Grid Manager.

Tarea	Menú Actions	Detalles
Ver los detalles del usuario	a. Seleccione la casilla de control para el usuario. b. Seleccione **acciones** > **Ver detalles del usuario**.	Seleccione el nombre del usuario en la tabla.
Editar nombre completo (sólo usuarios locales)	a. Seleccione la casilla de control para el usuario. b. Seleccione **acciones** > **Editar nombre completo**. c. Introduzca el nuevo nombre. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione el icono de edición . c. Introduzca el nuevo nombre. d. Seleccione **Guardar cambios**.

Tarea	Menú Actions	Detalles
Denegar o permitir el acceso a StorageGRID	a. Seleccione la casilla de control para el usuario. b. Seleccione **acciones** > **Ver detalles del usuario**. c. Seleccione la pestaña Access. d. Seleccione **Sí** para evitar que el usuario inicie sesión en Grid Manager o en la API de gestión de grid, o seleccione **no** para permitir que el usuario inicie sesión. e. Seleccione **Guardar cambios**.	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la pestaña Access. c. Seleccione **Sí** para evitar que el usuario inicie sesión en Grid Manager o en la API de gestión de grid, o seleccione **no** para permitir que el usuario inicie sesión. d. Seleccione **Guardar cambios**.
Cambiar contraseña (solo usuarios locales)	a. Seleccione la casilla de control para el usuario. b. Seleccione **acciones** > **Ver detalles del usuario**. c. Seleccione la ficha Contraseña. d. Introduzca una contraseña nueva. e. Seleccione **Cambiar contraseña**.	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la ficha Contraseña. c. Introduzca una contraseña nueva. d. Seleccione **Cambiar contraseña**.
Cambiar grupos (sólo usuarios locales)	a. Seleccione la casilla de control para el usuario. b. Seleccione **acciones** > **Ver detalles del usuario**. c. Seleccione la ficha grupos. d. Opcionalmente, seleccione el vínculo después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del explorador. e. Seleccione **Editar grupos** para seleccionar diferentes grupos. f. Seleccione **Guardar cambios**.	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la ficha grupos. c. Opcionalmente, seleccione el vínculo después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del explorador. d. Seleccione **Editar grupos** para seleccionar diferentes grupos. e. Seleccione **Guardar cambios**.

Duplique un usuario

Puede duplicar un usuario existente para crear un nuevo usuario con los mismos permisos.

Pasos

1. Seleccione la casilla de control para el usuario.
2. Seleccione **acciones** > **Duplicar usuario**.
3. Complete el asistente Duplicar usuario.

Eliminar un usuario

Puede eliminar un usuario local para eliminar de forma permanente ese usuario del sistema.

No puede eliminar el usuario root.

Pasos

1. En la página Usuarios, seleccione la casilla de verificación de cada usuario que desee eliminar.
2. Seleccione **acciones** > **Eliminar usuario**.
3. Seleccione **Eliminar usuario**.

Utilizar inicio de sesión único (SSO)

Configurar el inicio de sesión único

Cuando se habilita el inicio de sesión único (SSO), los usuarios solo pueden acceder a Grid Manager, al arrendatario Manager, a la API de gestión de grid o a la API de gestión de inquilinos si sus credenciales están autorizadas mediante el proceso de inicio de sesión SSO implementado por la organización. Los usuarios locales no pueden iniciar sesión en StorageGRID.

Cómo funciona el inicio de sesión único

El sistema StorageGRID admite el inicio de sesión único (SSO) con el estándar de lenguaje de marcado de aserción de seguridad 2.0 (SAML 2.0).

Antes de habilitar el inicio de sesión único (SSO), revise cómo se ven afectados los procesos de inicio de sesión y cierre de sesión de StorageGRID cuando se habilita SSO.

Inicie sesión cuando SSO esté habilitado

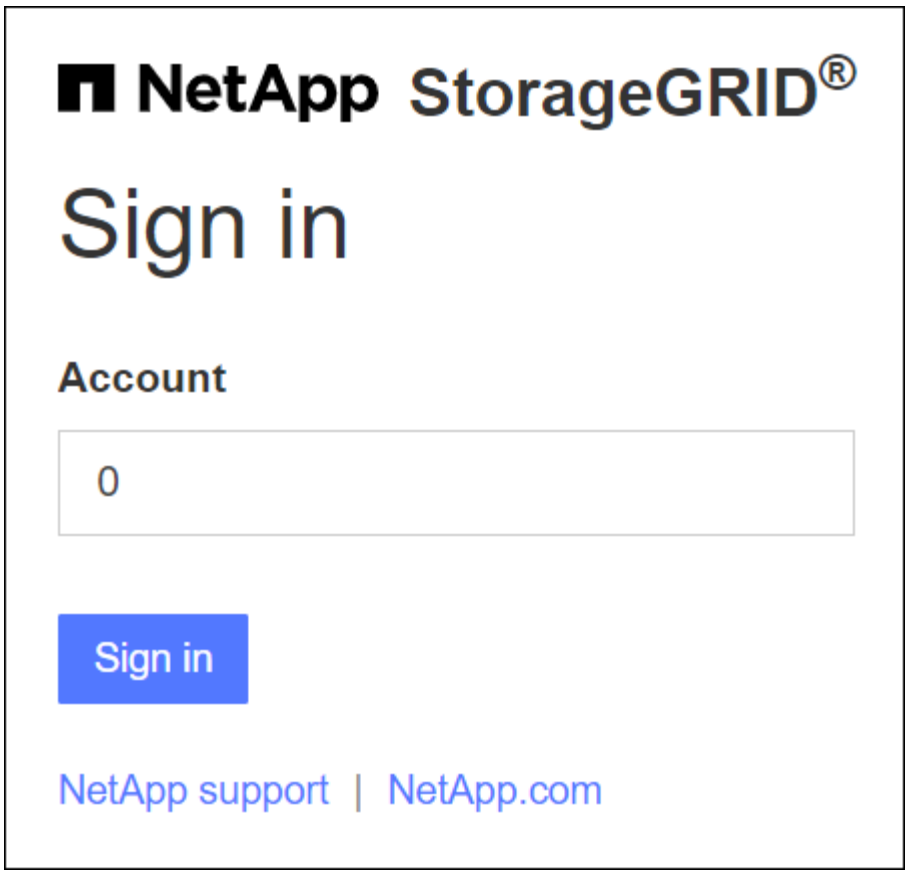
Cuando se habilita SSO y usted inicia sesión en StorageGRID, se le redirigirá a la página SSO de su organización para validar sus credenciales.

Pasos

1. Introduzca el nombre de dominio o la dirección IP completos de cualquier nodo de administración de StorageGRID en un navegador web.

   Aparece la página Inicio de sesión de StorageGRID.

   - Si es la primera vez que accede a la URL en este navegador, se le pedirá un ID de cuenta:

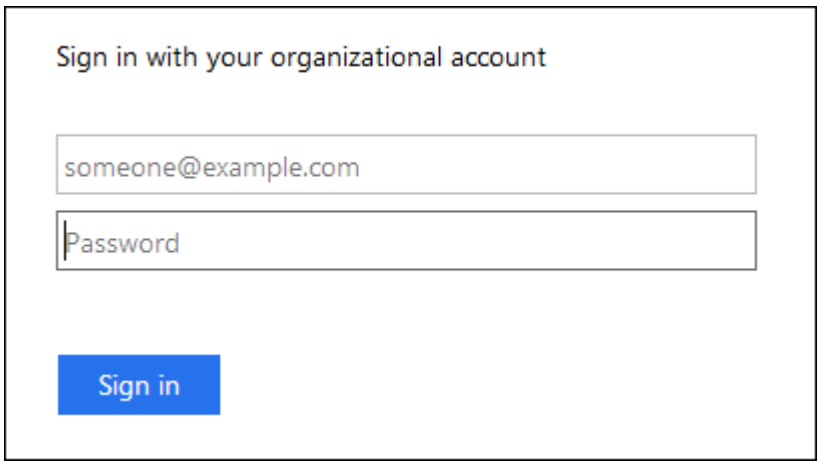


- Si anteriormente ha accedido al administrador de grid o al administrador de inquilinos, se le pedirá que seleccione una cuenta reciente o que introduzca un ID de cuenta:

La página de inicio de sesión de StorageGRID no se muestra cuando introduce la URL completa de una cuenta de inquilino (es decir, un nombre de dominio completo o una dirección IP seguida de `/?accountId=20-digit-account-id`). En su lugar, se le redirige inmediatamente a la página de inicio de sesión con SSO de su organización, en la que puede hacerlo Inicie sesión con sus credenciales de SSO.

2. Indique si desea acceder al administrador de grid o al responsable de inquilinos:
   - Para acceder a Grid Manager, deje el campo **ID de cuenta** en blanco, introduzca **0** como ID de cuenta o seleccione **Gestor de cuadrícula** si aparece en la lista de cuentas recientes.
   - Para acceder al Administrador de arrendatarios, introduzca el ID de cuenta de arrendatario de 20 dígitos o seleccione un arrendatario por nombre si aparece en la lista de cuentas recientes.
3. Seleccione **Iniciar sesión**

   StorageGRID le redirige a la página de inicio de sesión con SSO de su organización. Por ejemplo:



4. inicia sesión con sus credenciales de SSO.

   Si sus credenciales de SSO son correctas:

   a. El proveedor de identidades (IDP) ofrece una respuesta de autenticación a StorageGRID.
   b. StorageGRID valida la respuesta de autenticación.
   c. Si la respuesta es válida y pertenece a un grupo federado con permisos de acceso a StorageGRID, se ha iniciado sesión en el Gestor de grid o el Gestor de inquilinos, según la cuenta seleccionada.

   Si no se puede acceder a la cuenta de servicio, puede iniciar sesión siempre que sea un usuario existente que pertenezca a un grupo federado con permisos de acceso StorageGRID.

5. Opcionalmente, acceda a otros nodos de administración o acceda al administrador de grid o al administrador de inquilinos, si dispone de los permisos adecuados.

   No es necesario volver a introducir las credenciales de SSO.

Cierre sesión cuando SSO esté habilitado

Cuando se habilita SSO en StorageGRID, lo que sucede cuando se inicia sesión depende de lo que se haya iniciado sesión y del lugar en el que se está cerrando sesión.

Pasos

1. Localice el enlace **Sign Out** en la esquina superior derecha de la interfaz de usuario.
2. Selecciona **Cerrar sesión**.

   Aparece la página Inicio de sesión de StorageGRID. La lista desplegable **Cuentas recientes** se actualiza para incluir **Grid Manager** o el nombre del inquilino, por lo que puede acceder a estas interfaces de usuario más rápidamente en el futuro.

Si ha iniciado sesión en…	Y salir de…	Se ha cerrado sesión en…
Grid Manager en uno o varios nodos de administrador	Grid Manager en cualquier nodo de administrador	Grid Manager en todos los nodos de administración **Nota:** Si utiliza Azure para SSO, es posible que tarde unos minutos en salir de todos los nodos de administración.
Administrador de inquilinos en uno o varios nodos de administrador	Inquilino Manager en cualquier nodo de administrador	Administrador de inquilinos en todos los nodos de administrador
Tanto Grid Manager como Inquilino Manager	Administrador de grid	Sólo Grid Manager. También debe cerrar sesión en el Administrador de inquilinos para cerrar la sesión de SSO.

> La tabla resume lo que sucede cuando se inicia sesión si está utilizando una sola sesión del navegador. Si ha iniciado sesión en StorageGRID en varias sesiones de explorador, debe cerrar la sesión en todas las sesiones de explorador por separado.

Requisitos y consideraciones para el inicio de sesión único

Antes de activar el inicio de sesión único (SSO) para un sistema StorageGRID, revise los requisitos y consideraciones.

Requisitos del proveedor de identidades

StorageGRID admite los siguientes proveedores de identidad de SSO (IDP):

- Servicio de Federación de Active Directory (AD FS)
- Azure Active Directory (Azure AD)
- PingFederate

Debe configurar la federación de identidades para el sistema StorageGRID antes de poder configurar un proveedor de identidades SSO. El tipo de servicio LDAP que utiliza para controlar la federación de identidades qué tipo de SSO puede implementar.

Se ha configurado el tipo de servicio LDAP	Opciones para el proveedor de identidades SSO
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

Requisitos DE AD FS

Puede utilizar cualquiera de las siguientes versiones de AD FS:

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016 debe utilizar "Actualización KB3201845", o superior.

Requisitos adicionales

- Seguridad de la capa de transporte (TLS) 1.2 ó 1.3
- Microsoft .NET Framework, versión 3.5.1 o posterior

Consideraciones para Azure

Si usa Azure como tipo SSO y los usuarios tienen nombres principales de usuario que no usan sAMAccountName como prefijo, pueden producirse problemas de inicio de sesión si StorageGRID pierde su conexión con el servidor LDAP. Para permitir que los usuarios inicien sesión, debe restaurar la conexión con el servidor LDAP.

Requisitos de certificado de servidor

De forma predeterminada, StorageGRID utiliza un certificado de interfaz de gestión en cada nodo de administración para garantizar el acceso a Grid Manager, al Gestor de inquilinos, a la API de gestión de grid y a la API de gestión de inquilinos. Cuando configura confianzas de partes confiadas (AD FS), aplicaciones empresariales (Azure) o conexiones de proveedores de servicio (PingFederate) para StorageGRID, utilizará el certificado de servidor como certificado de firma para las solicitudes StorageGRID.

Si aún no lo ha hecho "se configuró un certificado personalizado para la interfaz de gestión", usted debe hacerlo ahora. Cuando instala un certificado de servidor personalizado, se utiliza para todos los nodos de administrador y puede usarlo en todas las confianzas de parte que dependen de StorageGRID, aplicaciones de empresa o conexiones del SP.

> No se recomienda utilizar el certificado de servidor predeterminado de un nodo de administración en la confianza de una parte que confía, la aplicación de empresa o la conexión de SP. Si el nodo falla y lo recupera, se genera un nuevo certificado de servidor predeterminado. Antes de iniciar sesión en el nodo recuperado, debe actualizar la confianza de la parte que confía, la aplicación de empresa o la conexión del SP con el nuevo certificado.

Para acceder a la certificación de servidor de un nodo de administrador, inicie sesión en el shell de comandos

del nodo y vaya al `/var/local/mgmt-api` directorio. Se denomina certificado de servidor personalizado `custom-server.crt`. El certificado de servidor predeterminado del nodo se denomina `server.crt`.

Requisitos de puertos

El inicio de sesión único (SSO) no está disponible en los puertos de administrador de grid restringido o de administrador de inquilinos. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autentiquen con inicio de sesión único. Consulte "Controle el acceso a un firewall externo".

Confirmar que los usuarios federados pueden iniciar sesión

Antes de habilitar el inicio de sesión único (SSO), debe confirmar que al menos un usuario federado puede iniciar sesión en Grid Manager y en el Gestor de inquilinos para cualquier cuenta de inquilino existente.

Antes de empezar

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

Pasos

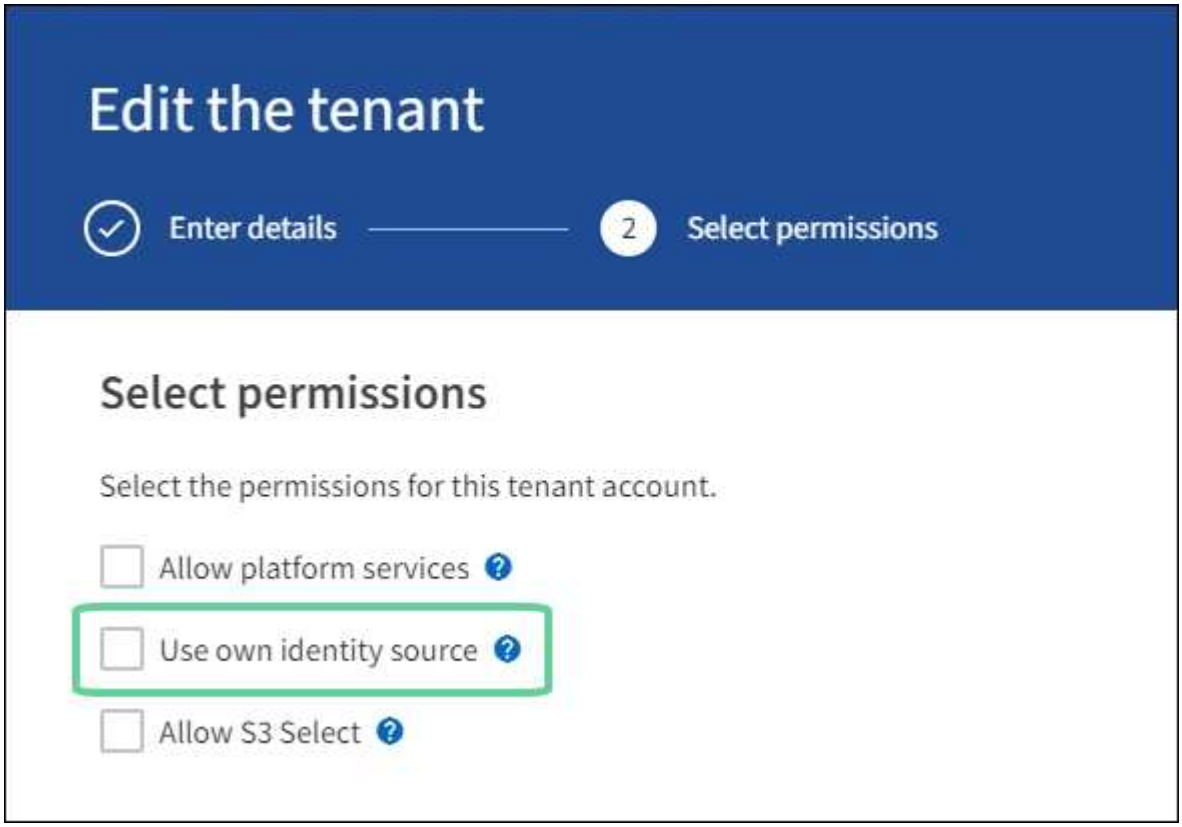
1. Si hay cuentas de inquilino existentes, confirme que ninguno de los inquilinos utiliza su propio origen de identidad.

   > Al habilitar SSO, el origen de identidad configurado en el Administrador de inquilinos se anula mediante el origen de identidades configurado en Grid Manager. Los usuarios que pertenezcan al origen de identidad del arrendatario ya no podrán iniciar sesión a menos que tengan una cuenta con el origen de identidad de Grid Manager.

   a. Inicie sesión en el Administrador de arrendatarios para cada cuenta de arrendatario.
   b. Seleccione **ADMINISTRACIÓN de ACCESO** > **federación de identidades**.
   c. Confirme que la casilla de verificación **Habilitar federación de identidad** no está seleccionada.
   d. Si lo es, confirme que los grupos federados que puedan estar en uso para esta cuenta de inquilino ya no son necesarios, desactive la casilla de verificación y seleccione **Guardar**.

2. Confirme que un usuario federado puede acceder a Grid Manager:
   a. En Grid Manager, seleccione **CONFIGURACIÓN** > **Control de acceso** > **grupos de administración**.
   b. Asegúrese de que al menos un grupo federado se ha importado del origen de identidad de Active Directory y de que se le ha asignado el permiso acceso raíz.
   c. Cierre la sesión.
   d. Confirme que puede volver a iniciar sesión en Grid Manager como usuario en el grupo federado.
3. Si hay cuentas de inquilino existentes, confirme que un usuario federado con permiso de acceso raíz puede iniciar sesión:
   a. En Grid Manager, seleccione **ARRENDATARIOS**.
   b. Seleccione la cuenta de arrendatario y seleccione **acciones** > **Editar**.
   c. En la ficha introducir detalles, seleccione **continuar**.

d. Si la casilla de verificación **Usar fuente de identidad propia** está seleccionada, desmarque la casilla y seleccione **Guardar**.



Aparece la página inquilino.

a. Seleccione la cuenta de arrendatario, seleccione **Iniciar sesión** e inicie sesión en la cuenta de arrendatario como usuario raíz local.
b. En el Administrador de inquilinos, seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
c. Asegúrese de que al menos un grupo federado de Grid Manager ha sido asignado el permiso de acceso raíz para este arrendatario.
d. Cierre la sesión.
e. Confirme que puede volver a iniciar sesión en el inquilino como usuario en el grupo federado.

Información relacionada

- "Requisitos y consideraciones para el inicio de sesión único"
- "Gestione los grupos de administradores"
- "Usar una cuenta de inquilino"

Utilizar el modo de recinto de seguridad

Es posible utilizar el modo de recinto de seguridad para configurar y probar el inicio de sesión único (SSO) antes de habilitarlo para todos los usuarios de StorageGRID. Una vez que se habilita SSO, es posible volver al modo Sandbox cada vez que sea necesario cambiar o volver a probar la configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".
- Configuró la federación de identidades para el sistema StorageGRID.
- Para la federación de identidades **Tipo de servicio LDAP**, ha seleccionado Active Directory o Azure, basándose en el proveedor de identidades SSO que planea utilizar.

Se ha configurado el tipo de servicio LDAP	Opciones para el proveedor de identidades SSO
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

Acerca de esta tarea

Cuando se habilita el inicio de sesión único y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación al proveedor de identidades de SSO. A su vez, el proveedor de identidades SSO envía una respuesta de autenticación a StorageGRID para indicar si la solicitud de autenticación se ha realizado correctamente. Para solicitudes correctas:

- La respuesta de Active Directory o PingFederate incluye un identificador único universal (UUID) para el usuario.
- La respuesta de Azure incluye un nombre principal de usuario (UPN).

Para permitir que StorageGRID (el proveedor de servicios) y el proveedor de identidades SSO se comuniquen de forma segura acerca de las solicitudes de autenticación de usuarios, debe configurar determinados ajustes en StorageGRID. A continuación, debe utilizar el software del proveedor de identidades SSO para crear una confianza de parte fiable (AD FS), una aplicación empresarial (Azure) o un proveedor de servicios (PingFederate) para cada nodo de administración. Por último, debe volver a StorageGRID para habilitar SSO.

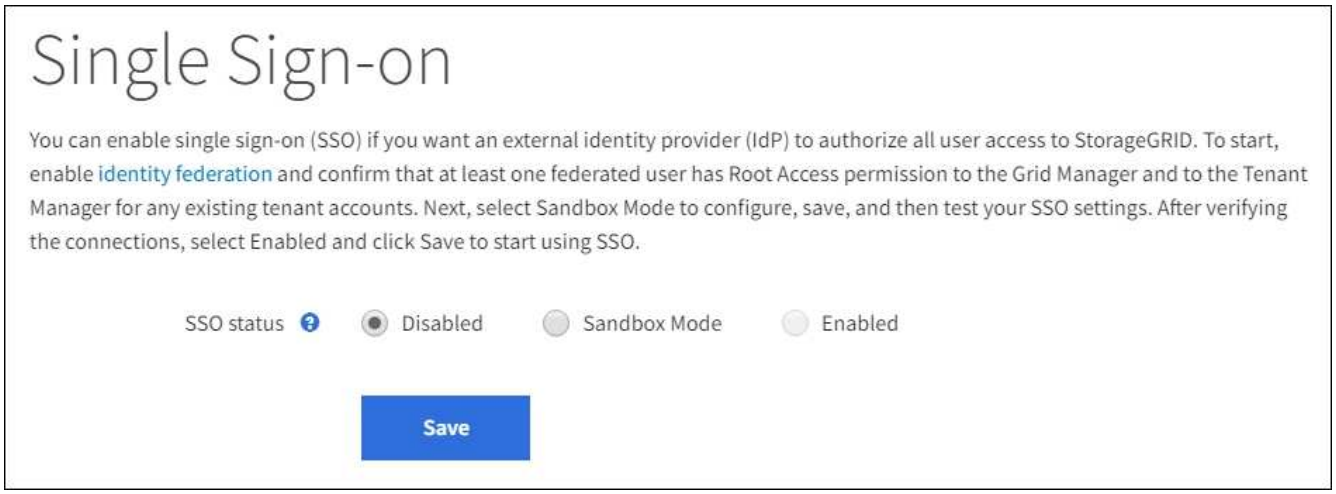
El modo de recinto de seguridad facilita la realización de esta configuración de fondo y la realización de pruebas de todos los ajustes antes de habilitar SSO. Al utilizar el modo sandbox, los usuarios no pueden iniciar sesión con SSO.

Acceder al modo de recinto de seguridad

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.

   Aparece la página Inicio de sesión único, con la opción **Desactivado** seleccionada.



Si las opciones de estado de SSO no aparecen, confirme que ha configurado el proveedor de identidad como origen de identidad federado. Consulte "Requisitos y consideraciones para el inicio de sesión único".

2. Seleccione **modo Sandbox**.

   Aparece la sección Proveedor de identidades.

Introduzca los detalles del proveedor de identidades

Pasos

1. Seleccione **Tipo SSO** en la lista desplegable.
2. Complete los campos de la sección Proveedor de identidades según el tipo de SSO seleccionado.

Active Directory

1. Introduzca el **nombre del servicio de Federación** para el proveedor de identidades, exactamente como aparece en el Servicio de Federación de Active Directory (AD FS).

   Para buscar el nombre del servicio de federación, vaya al Administrador de Windows Server. Seleccione **Herramientas** > **Administración AD FS**. En el menú Acción, seleccione **Editar propiedades del servicio de Federación**. El nombre del servicio de Federación se muestra en el segundo campo.

2. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidades envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID.
   - **Utilizar certificado CA** del sistema operativo: Utilice el certificado CA predeterminado instalado en el sistema operativo para asegurar la conexión.
   - **Utilizar certificado de CA personalizado**: Utilice un certificado de CA personalizado para proteger la conexión.

     Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.
   - **No utilice TLS**: No utilice un certificado TLS para garantizar la conexión.

     Si cambia el certificado de CA, inmediatamente "Reinicie el servicio mgmt-api en los nodos de administración" Y probar si se ha realizado correctamente un inicio de sesión único en Grid Manager.

3. En la sección parte que confía, especifique el identificador * de parte que confía* para StorageGRID. Este valor controla el nombre que utiliza para cada confianza de parte que confía en AD FS.
   - Por ejemplo, si el grid solo tiene un nodo de administración y no cree que agregue más nodos de administración en el futuro, introduzca `SG` o. `StorageGRID`.
   - Si el grid incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo: `SG-[HOSTNAME]`. De este modo, se genera una tabla que muestra el identificador de la parte que confía para cada nodo de administrador del sistema en función del nombre de host del nodo.

   Debe crear una confianza de parte de confianza para cada nodo de administrador en el sistema StorageGRID. Tener una confianza de parte que confía en cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura desde y hacia cualquier nodo de administración.

4. Seleccione **Guardar**.

   Aparece una Marca de verificación verde en el botón **Guardar** durante unos segundos.

Azure

1. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidades envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID.
   - **Utilizar certificado CA** del sistema operativo: Utilice el certificado CA predeterminado instalado en el sistema operativo para asegurar la conexión.
   - **Utilizar certificado de CA personalizado**: Utilice un certificado de CA personalizado para proteger la conexión.

     Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.
   - **No utilice TLS**: No utilice un certificado TLS para garantizar la conexión.

   > Si cambia el certificado de CA, inmediatamente "Reinicie el servicio mgmt-api en los nodos de administración" Y probar si se ha realizado correctamente un inicio de sesión único en Grid Manager.

2. En la sección aplicación de empresa, especifique **Nombre de aplicación de empresa** para StorageGRID. Este valor controla el nombre que se utiliza para cada aplicación empresarial en Azure AD.
   - Por ejemplo, si el grid solo tiene un nodo de administración y no cree que agregue más nodos de administración en el futuro, introduzca `SG` o. `StorageGRID`.
   - Si el grid incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo: `SG-[HOSTNAME]`. De este modo, se genera una tabla que muestra el nombre de una aplicación empresarial para cada nodo de administrador del sistema en función del nombre de host del nodo.

   > Debe crear una aplicación empresarial para cada nodo administrador en el sistema StorageGRID. Disponer de una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura en cualquier nodo de administración.

3. Siga los pasos de "Cree aplicaciones empresariales en Azure AD" Para crear una aplicación de empresa para cada nodo de administración que se muestra en la tabla.
4. Desde Azure AD, copie la URL de metadatos de federación para cada aplicación empresarial. A continuación, pegue esta URL en el campo **URL** de metadatos de Federación correspondiente de StorageGRID.
5. Después de copiar y pegar una dirección URL de metadatos de federación para todos los nodos de administración, seleccione **Guardar**.

   Aparece una Marca de verificación verde en el botón **Guardar** durante unos segundos.

PingFederate

1. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidades envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID.

- **Utilizar certificado CA** del sistema operativo: Utilice el certificado CA predeterminado instalado en el sistema operativo para asegurar la conexión.
- **Utilizar certificado de CA personalizado**: Utilice un certificado de CA personalizado para proteger la conexión.

  Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

- **No utilice TLS**: No utilice un certificado TLS para garantizar la conexión.

> Si cambia el certificado de CA, inmediatamente "Reinicie el servicio mgmt-api en los nodos de administración" Y probar si se ha realizado correctamente un inicio de sesión único en Grid Manager.

2. En la sección Proveedor de servicios (SP), especifique **ID de conexión SP** para StorageGRID. Este valor controla el nombre que utiliza para cada conexión SP en PingFederate.
   - Por ejemplo, si el grid solo tiene un nodo de administración y no cree que agregue más nodos de administración en el futuro, introduzca `SG` o. `StorageGRID`.
   - Si el grid incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo: `SG-[HOSTNAME]`. De este modo, se genera una tabla que muestra el ID de conexión del SP para cada nodo de administrador del sistema, según el nombre de host del nodo.

> Debe crear una conexión de SP para cada nodo de administrador en el sistema StorageGRID. Tener una conexión de SP para cada nodo de administrador garantiza que los usuarios puedan iniciar sesión de forma segura en cualquier nodo de administrador.

3. Especifique la dirección URL de metadatos de federación para cada nodo de administración en el campo **URL de metadatos de Federación**.

   Utilice el siguiente formato:

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection
ID>
```

4. Seleccione **Guardar**.

   Aparece una Marca de verificación verde en el botón **Guardar** durante unos segundos.

Configurar las confianzas de partes de confianza, las aplicaciones de la empresa o las conexiones de SP

Cuando se guarde la configuración, aparecerá el aviso de confirmación del modo Sandbox. Este aviso confirma que el modo de recinto de seguridad está ahora activado y proporciona instrucciones de descripción general.

StorageGRID puede permanecer en modo de recinto limitado siempre que sea necesario. Sin embargo, cuando se selecciona **modo Sandbox** en la página Single Sign-On, SSO está desactivado para todos los usuarios de StorageGRID. Solo los usuarios locales pueden iniciar sesión.

Siga estos pasos para configurar trusting Party trusts (Active Directory), completar aplicaciones empresariales (Azure) o configurar conexiones SP (PingFederate).

Active Directory

Pasos

1. Vaya a Servicios de Federación de Active Directory (AD FS).
2. Cree una o varias confianzas de parte que dependan para StorageGRID, utilizando cada identificador de parte que dependa que se muestra en la tabla de la página StorageGRID Single Sign-On.

   Debe crear una confianza para cada nodo de administrador que se muestra en la tabla.

   Para obtener instrucciones, vaya a. "Crear confianzas de parte de confianza en AD FS".

Azure

Pasos

1. En la página Single Sign-On del nodo de administrador al que ha iniciado sesión actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. A continuación, para cualquier otro nodo de administrador en el grid, repita estos pasos:
   a. Inicie sesión en el nodo.
   b. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.
   c. Descargue y guarde los metadatos de SAML de ese nodo.
3. Vaya al portal de Azure.
4. Siga los pasos de "Cree aplicaciones empresariales en Azure AD" Para cargar el archivo de metadatos SAML para cada nodo de administrador en la aplicación empresarial de Azure correspondiente.

PingFederate

Pasos

1. En la página Single Sign-On del nodo de administrador al que ha iniciado sesión actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. A continuación, para cualquier otro nodo de administrador en el grid, repita estos pasos:
   a. Inicie sesión en el nodo.
   b. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.
   c. Descargue y guarde los metadatos de SAML de ese nodo.
3. Vaya a PingFederate.
4. "Cree una o varias conexiones de proveedor de servicios (SP) para StorageGRID". Utilice el ID de conexión del SP para cada nodo de administrador (que se muestra en la tabla de la página StorageGRID Single Sign-On) y los metadatos SAML que ha descargado para ese nodo de administrador.

   Debe crear una conexión de SP para cada nodo de administrador que se muestra en la tabla.

Probar conexiones SSO

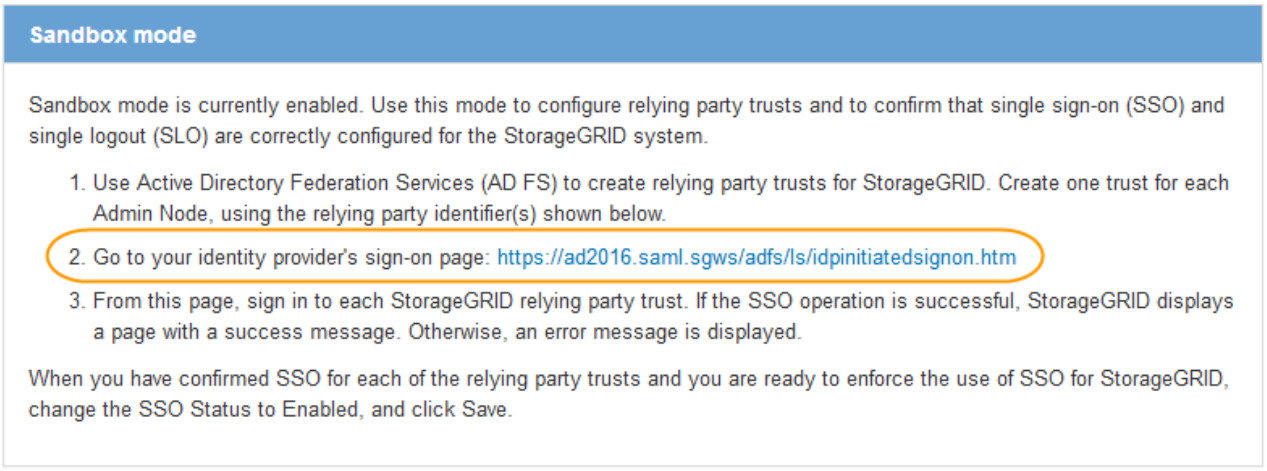
Antes de aplicar el uso del inicio de sesión único para todo el sistema StorageGRID, debe confirmar que el inicio de sesión único y el cierre de sesión único están correctamente configurados para cada nodo de administración.

Active Directory

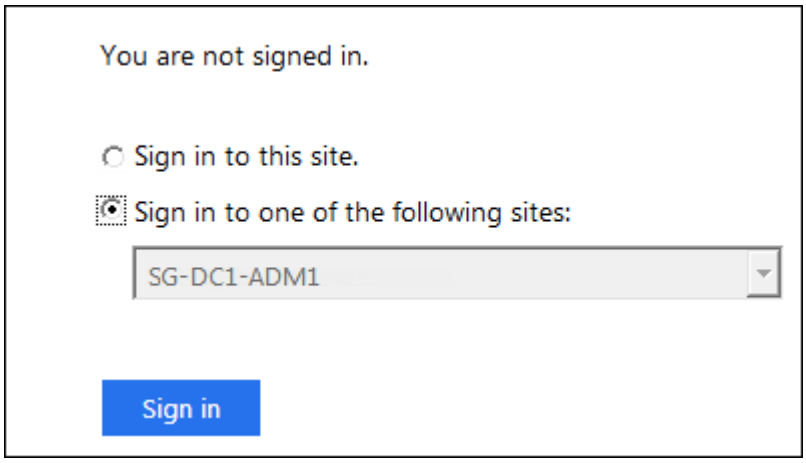
Pasos

1. En la página Inicio de sesión único de StorageGRID, localice el vínculo en el mensaje modo Sandbox.

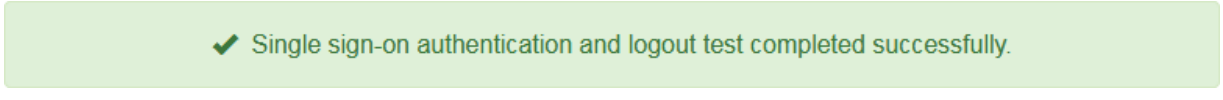
   La dirección URL se deriva del valor introducido en el campo **Nombre de servicio de Federación**.



2. Seleccione el enlace, o copie y pegue la URL en un navegador para acceder a la página de inicio de sesión del proveedor de identidades.
3. Para confirmar que puede utilizar SSO para iniciar sesión en StorageGRID, seleccione **Iniciar sesión en uno de los siguientes sitios**, seleccione el identificador de la parte que confía para su nodo de administración principal y seleccione **Iniciar sesión**.



4. Introduzca el nombre de usuario y la contraseña federados.
   - Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.



   - Si la operación de SSO se realiza sin errores, se muestra un mensaje de error. Solucione el problema, borre las cookies del navegador e inténtelo de nuevo.
5. Repita estos pasos para verificar la conexión SSO para cada nodo de administrador en el grid.

Azure

Pasos

1. Vaya a la página Single Sign-On del portal de Azure.
2. Seleccione **probar esta aplicación**.
3. Introduzca las credenciales de un usuario federado.
   - Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.

     ✔ Single sign-on authentication and logout test completed successfully.

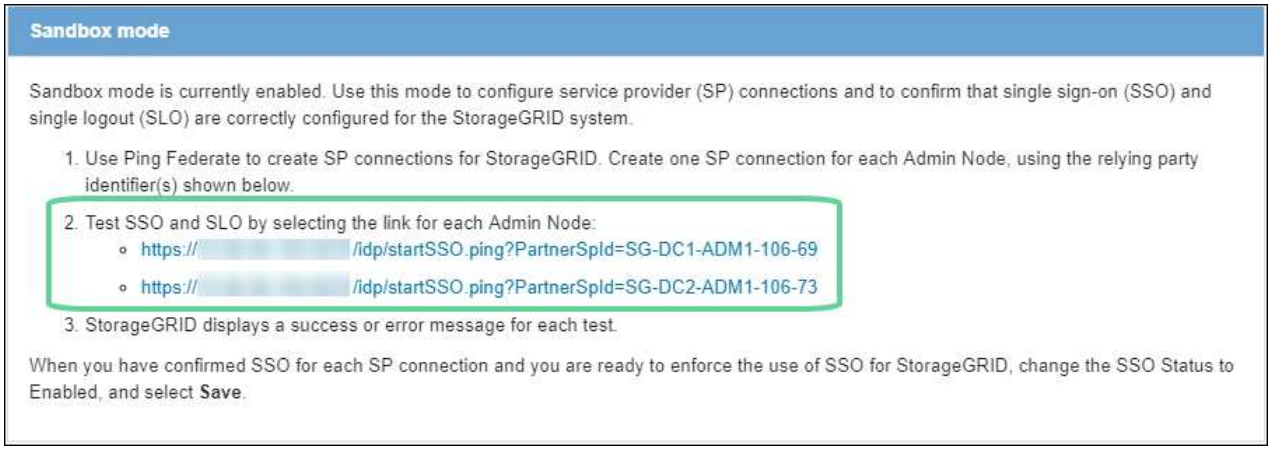
   - Si la operación de SSO se realiza sin errores, se muestra un mensaje de error. Solucione el problema, borre las cookies del navegador e inténtelo de nuevo.
4. Repita estos pasos para verificar la conexión SSO para cada nodo de administrador en el grid.

PingFederate

Pasos

1. En la página Inicio de sesión único de StorageGRID, seleccione el primer enlace en el mensaje modo Sandbox.

   Seleccione y pruebe un enlace cada vez.

2. Introduzca las credenciales de un usuario federado.
   - Si las operaciones de inicio de sesión y cierre de sesión SSO se realizan correctamente, se muestra un mensaje de éxito.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Si la operación de SSO se realiza sin errores, se muestra un mensaje de error. Solucione el problema, borre las cookies del navegador e inténtelo de nuevo.
3. Seleccione el siguiente enlace para verificar la conexión de SSO para cada nodo de administrador de la cuadrícula.

   Si ve un mensaje Página caducada, seleccione el botón **Atrás** de su explorador y vuelva a enviar sus credenciales.

Active el inicio de sesión único

Una vez que haya confirmado que puede usar SSO para iniciar sesión en cada nodo de administración, puede habilitar SSO en todo el sistema StorageGRID.

> Cuando SSO está habilitado, todos los usuarios deben utilizar SSO para acceder a Grid Manager, al arrendatario Manager, a la API de gestión de grid y a la API de gestión de inquilinos. Los usuarios locales ya no pueden acceder a StorageGRID.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.
2. Cambie el estado de SSO a **habilitado**.
3. Seleccione **Guardar**.
4. Revise el mensaje de advertencia y seleccione **Aceptar**.

   El inicio de sesión único ahora está activado.

> Si utiliza el portal de Azure y accede a StorageGRID desde el mismo equipo que utiliza para acceder a Azure, asegúrese de que el usuario del portal de Azure también sea un usuario de StorageGRID autorizado (un usuario de un grupo federado que se ha importado a StorageGRID) O cierre la sesión en Azure Portal antes de intentar iniciar sesión en StorageGRID.

Crear confianzas de parte de confianza en AD FS

Debe utilizar los Servicios de Federación de Active Directory (AD FS) para crear una confianza de parte de confianza para cada nodo de administración del sistema. Puede crear confianzas de parte confiando mediante comandos de PowerShell, importando los metadatos de SAML desde StorageGRID o introduciendo los datos manualmente.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y ha seleccionado **AD FS** como tipo SSO.
- **Modo Sandbox** está seleccionado en la página Single Sign-On de Grid Manager. Consulte "Utilizar el modo de recinto de seguridad".
- Conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte que confía para cada nodo de administración del sistema. Puede encontrar estos valores en la tabla de detalles Admin Nodes en la página StorageGRID Single Sign-On.

  > Debe crear una confianza de parte de confianza para cada nodo de administrador en el sistema StorageGRID. Tener una confianza de parte que confía en cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura desde y hacia cualquier nodo de administración.

- Tiene experiencia en la creación de confianzas de parte de confianza en AD FS o tiene acceso a la documentación de Microsoft AD FS.
- Está utilizando el complemento Administración de AD FS y pertenece al grupo Administradores.
- Si crea la confianza de la parte de confianza manualmente, tiene el certificado personalizado que se cargó para la interfaz de gestión de StorageGRID, o sabe cómo iniciar sesión en un nodo de administrador

desde el shell de comandos.

Acerca de esta tarea

Estas instrucciones se aplican a Windows Server 2016 AD FS. Si está utilizando una versión diferente de AD FS, notará ligeras diferencias en el procedimiento. Consulte la documentación de Microsoft AD FS si tiene alguna pregunta.

Cree una confianza de parte de confianza mediante Windows PowerShell

Puede utilizar Windows PowerShell para crear rápidamente una o más confianzas de parte que dependan.

Pasos

1. En el menú de inicio de Windows, seleccione con el botón derecho el icono de PowerShell y seleccione **Ejecutar como administrador**.
2. En el símbolo del sistema de PowerShell, introduzca el siguiente comando:

   `Add-AdfsRelyingPartyTrust -Name 'Admin_Node_Identifer' -MetadataURL "https://Admin_Node_FQDN/api/saml-metadata"

   - Para *`Admin_Node_Identifier`*, Escriba el identificador de parte que confía para el nodo de administración, exactamente como aparece en la página Single Sign-On. Por ejemplo: `SG-DC1-ADM1`.
   - Para *`Admin_Node_FQDN`*, Escriba el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)
3. En Windows Server Manager, seleccione **Herramientas** > **Administración de AD FS**.

   Aparece la herramienta de administración de AD FS.

4. Seleccione **AD FS** > **fideicomisos de la parte**.

   Aparece la lista de confianzas de parte de confianza.

5. Agregar una directiva de control de acceso a la confianza de parte de confianza recién creada:
   a. Busque la parte de confianza que acaba de crear.
   b. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar directiva de control de acceso**.
   c. Seleccione una Política de control de acceso.
   d. Seleccione **aplicar** y seleccione **Aceptar**
6. Agregar una política de emisión de reclamaciones a la nueva confianza de parte de confianza creada:
   a. Busque la parte de confianza que acaba de crear.
   b. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar política de emisión de reclamaciones**.
   c. Seleccione **Agregar regla**.
   d. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.
   e. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID to Name ID** o **UPN to Name ID**.

f. Para el almacén de atributos, seleccione **Active Directory**.

g. En la columna Atributo LDAP de la tabla de asignación, escriba **objectGUID** o seleccione **User-Principal-Name**.

h. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.

i. Seleccione **Finalizar** y seleccione **Aceptar**.

7. Confirme que los metadatos se han importado correctamente.

a. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.

b. Confirme que los campos de las fichas **puntos finales**, **identificadores** y **firma** se han rellenado.

Si faltan los metadatos, confirme que la dirección de metadatos de federación es correcta o introduzca los valores manualmente.

8. Repita estos pasos para configurar una confianza de parte que confía para todos los nodos de administración del sistema StorageGRID.

9. Cuando haya terminado, vuelva a StorageGRID y pruebe todos los fideicomisos de las partes que dependan para confirmar que están configurados correctamente. Consulte "Utilice el modo Sandbox" si desea obtener instrucciones.

Cree una confianza de parte de confianza importando metadatos de federación

Puede importar los valores de cada una de las partes que confía mediante el acceso a los metadatos de SAML de cada nodo de administrador.

Pasos

1. En Windows Server Manager, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.

2. En acciones, seleccione **Agregar confianza de parte de confianza**.

3. En la página de bienvenida, elija **Claims aware** y seleccione **Start**.

4. Seleccione **Importar datos sobre la parte que confía publicada en línea o en una red local**.

5. En **Dirección de metadatos de Federación (nombre de host o URL)**, escriba la ubicación de los metadatos SAML para este nodo de administración:

`https://Admin_Node_FQDN/api/saml-metadata`

Para *`Admin_Node_FQDN`*, Escriba el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)

6. Complete el asistente Trust Party Trust, guarde la confianza de la parte que confía y cierre el asistente.

Al introducir el nombre para mostrar, utilice el identificador de parte de confianza para el nodo de administración, exactamente como aparece en la página Single Sign-On en Grid Manager. Por ejemplo: `SG-DC1-ADM1`.

7. Agregar una regla de reclamación:
   a. Haga clic con el botón derecho del ratón en la confianza y seleccione **Editar política de emisión de reclamaciones**.
   b. Seleccione **Agregar regla**:
   c. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.
   d. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

      Por ejemplo, **ObjectGUID to Name ID** o **UPN to Name ID**.

   e. Para el almacén de atributos, seleccione **Active Directory**.
   f. En la columna Atributo LDAP de la tabla de asignación, escriba **objectGUID** o seleccione **User-Principal-Name**.
   g. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.
   h. Seleccione **Finalizar** y seleccione **Aceptar**.
8. Confirme que los metadatos se han importado correctamente.
   a. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.
   b. Confirme que los campos de las fichas **puntos finales**, **identificadores** y **firma** se han rellenado.

      Si faltan los metadatos, confirme que la dirección de metadatos de federación es correcta o introduzca los valores manualmente.

9. Repita estos pasos para configurar una confianza de parte que confía para todos los nodos de administración del sistema StorageGRID.
10. Cuando haya terminado, vuelva a StorageGRID y pruebe todos los fideicomisos de las partes que dependan para confirmar que están configurados correctamente. Consulte "Utilice el modo Sandbox" si desea obtener instrucciones.

Cree una confianza de parte de confianza manualmente

Si elige no importar los datos de las confianzas de la pieza de confianza, puede introducir los valores manualmente.

Pasos

1. En Windows Server Manager, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En acciones, seleccione **Agregar confianza de parte de confianza**.
3. En la página de bienvenida, elija **Claims aware** y seleccione **Start**.
4. Seleccione **introducir datos sobre la parte que confía manualmente** y seleccione **Siguiente**.
5. Complete el asistente Trust Party Trust:
   a. Introduzca un nombre de visualización para este nodo de administración.

      Para obtener coherencia, utilice el identificador de parte de confianza para el nodo de administración, exactamente como aparece en la página de inicio de sesión único en Grid Manager. Por ejemplo: `SG-`

`DC1-ADM1`.

b. Omitir el paso para configurar un certificado de cifrado de token opcional.

c. En la página Configurar URL, seleccione la casilla de verificación **Habilitar soporte para el protocolo WebSSO de SAML 2,0**.

d. Escriba la URL del extremo de servicio SAML para el nodo de administración:

`https://Admin_Node_FQDN/api/saml-response`

Para *`Admin_Node_FQDN`*, Escriba el nombre de dominio completo para el nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)

e. En la página Configurar identificadores, especifique el identificador de parte que confía para el mismo nodo de administración:

`Admin_Node_Identifier`

Para *`Admin_Node_Identifier`*, Escriba el identificador de parte que confía para el nodo de administración, exactamente como aparece en la página Single Sign-On. Por ejemplo: `SG-DC1-ADM1`.

f. Revise la configuración, guarde la confianza de la parte que confía y cierre el asistente.

Aparecerá el cuadro de diálogo Editar directiva de emisión de reclamaciones.

> Si el cuadro de diálogo no aparece, haga clic con el botón derecho del ratón en la confianza y seleccione **Editar directiva de emisión de reclamaciones**.

6. Para iniciar el asistente para reglas de reclamación, seleccione **Agregar regla**:

a. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** en la lista y seleccione **Siguiente**.

b. En la página Configurar regla, introduzca un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID to Name ID** o **UPN to Name ID**.

c. Para el almacén de atributos, seleccione **Active Directory**.

d. En la columna Atributo LDAP de la tabla de asignación, escriba **objectGUID** o seleccione **User-Principal-Name**.

e. En la columna Tipo de reclamación saliente de la tabla asignación, seleccione **ID de nombre** en la lista desplegable.

f. Seleccione **Finalizar** y seleccione **Aceptar**.

7. Haga clic con el botón derecho del ratón en la confianza de la parte que confía para abrir sus propiedades.

8. En la ficha **endpoints**, configure el extremo para un único cierre de sesión (SLO):

a. Seleccione **Añadir SAML**.

b. Seleccione **Tipo de extremo** > **SAML Logout**.

c. Seleccione **enlace** > **Redirigir**.

d. En el campo **Trusted URL**, introduzca la dirección URL utilizada para cerrar sesión único (SLO) desde este nodo de administración:

`https://Admin_Node_FQDN/api/saml-logout`

Para *`Admin_Node_FQDN`*, Escriba el nombre de dominio completo del nodo de administración. (Si es necesario, puede usar la dirección IP del nodo en su lugar. Sin embargo, si introduce una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear la confianza de esta parte que confía si esa dirección IP cambia alguna vez.)

a. Seleccione **OK**.

9. En la ficha **firma**, especifique el certificado de firma para esta confianza de parte de confianza:
   a. Agregue el certificado personalizado:
      - Si posee el certificado de gestión personalizado cargado en StorageGRID, seleccione ese certificado.
      - Si no tiene el certificado personalizado, inicie sesión en el nodo de administración, vaya a. `/var/local/mgmt-api` directorio del nodo Admin y añada el `custom-server.crt` archivo de certificado.

        Nota: utilizando el certificado predeterminado del nodo de administración (`server.crt`) no es recomendable. Si falla el nodo de administración, el certificado predeterminado se regenerará al recuperar el nodo y deberá actualizar la confianza de la parte de confianza.

   b. Seleccione **aplicar** y seleccione **Aceptar**.

      Las propiedades de la parte de confianza se guardan y cierran.

10. Repita estos pasos para configurar una confianza de parte que confía para todos los nodos de administración del sistema StorageGRID.
11. Cuando haya terminado, vuelva a StorageGRID y pruebe todos los fideicomisos de las partes que dependan para confirmar que están configurados correctamente. Consulte "Utilizar el modo de recinto de seguridad" si desea obtener instrucciones.

Cree aplicaciones empresariales en Azure AD

Puede usar Azure AD para crear una aplicación empresarial para cada nodo de administrador del sistema.

Antes de empezar

- Ha empezado a configurar el inicio de sesión único para StorageGRID y ha seleccionado **Azure** como tipo de SSO.
- **Modo Sandbox** está seleccionado en la página Single Sign-On de Grid Manager. Consulte "Utilizar el modo de recinto de seguridad".
- Tiene el **Nombre de la aplicación de empresa** para cada nodo de administración de su sistema. Se pueden copiar estos valores de la tabla de detalles Admin Node en la página StorageGRID Single Sign-On.

Debe crear una aplicación empresarial para cada nodo administrador en el sistema StorageGRID. Disponer de una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión de forma segura en cualquier nodo de administración.

- Tiene experiencia en la creación de aplicaciones empresariales en Azure Active Directory.
- Tiene una cuenta de Azure con una suscripción activa.
- Tiene uno de los siguientes roles en la cuenta de Azure: Administrador global, administrador de aplicaciones de cloud, administrador de aplicaciones o propietario del director del servicio.

Acceda a Azure AD

Pasos

1. Inicie sesión en la "Portal de Azure".
2. Vaya a. "Active Directory para Azure".
3. Seleccione "Aplicaciones de negocio".

Creación de aplicaciones empresariales y guardado de la configuración de SSO de StorageGRID

Para guardar la configuración de SSO para Azure en StorageGRID, debe usar Azure para crear una aplicación empresarial para cada nodo de administración. Copiará las URL de metadatos de federación de Azure y las pegará en los campos de la URL* de metadatos de Federación correspondientes de la página de inicio de sesión único de StorageGRID.

Pasos

1. Repita los siguientes pasos para cada nodo de administrador.
   a. En el panel aplicaciones de Azure Enterprise, seleccione **Nueva aplicación**.
   b. Seleccione **Crear su propia aplicación**.
   c. Para el nombre, introduzca el **Nombre de la aplicación de empresa** que ha copiado de la tabla de detalles del nodo de administración en la página Inicio de sesión único de StorageGRID.
   d. Deje seleccionada la opción **integrar cualquier otra aplicación que no encuentre en la galería (no galería)**.
   e. Seleccione **Crear**.
   f. Seleccione el enlace **Get Started** en **2. Configure el cuadro de inicio de sesión único en** o seleccione el enlace **Single Sign-On** en el margen izquierdo.
   g. Seleccione la casilla **SAML**.
   h. Copie la URL * metadatos de Federación de aplicaciones*, que puede encontrar en **Paso 3 Certificado de firma SAML**.
   i. Vaya a la página Inicio de sesión único de StorageGRID y pegue la dirección URL en el campo **URL** de metadatos de Federación que corresponda al **Nombre de aplicación de empresa** que ha utilizado.
2. Una vez que haya pegado una URL de metadatos de federación para cada nodo de administración y realizado todos los demás cambios necesarios en la configuración de SSO, seleccione **Guardar** en la página Inicio de sesión único de StorageGRID.

Descargue los metadatos de SAML para cada nodo de administración

Una vez guardada la configuración de SSO, puede descargar un archivo de metadatos SAML para cada nodo de administrador del sistema StorageGRID.

Pasos

1. Repita estos pasos para cada nodo de administración.
   a. Inicie sesión en StorageGRID desde el nodo de administrador.
   b. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.
   c. Seleccione el botón para descargar los metadatos de SAML de ese nodo de administración.
   d. Guarde el archivo, que cargará en Azure AD.

Cargue metadatos de SAML en cada aplicación empresarial

Después de descargar un archivo de metadatos SAML para cada nodo de administrador de StorageGRID, siga estos pasos en Azure AD:

Pasos

1. Vuelva al portal de Azure.
2. Repita estos pasos con cada aplicación de empresa:

   > Es posible que deba actualizar la página aplicaciones de empresa para ver las aplicaciones que ha agregado anteriormente en la lista.

   a. Vaya a la página Propiedades de la aplicación de empresa.
   b. Establezca **asignación requerida** en **no** (a menos que desee configurar las asignaciones por separado).
   c. Vaya a la página Single Sign-On.
   d. Complete la configuración de SAML.
   e. Seleccione el botón **Upload metadata file** y seleccione el archivo de metadatos SAML que descargó para el nodo de administración correspondiente.
   f. Después de cargar el archivo, seleccione **Guardar** y, a continuación, seleccione **X** para cerrar el panel. Volverá a la página Set up Single Sign-On with SAML.
3. Siga los pasos de "Utilizar el modo de recinto de seguridad" para probar cada aplicación.

Cree conexiones de proveedores de servicios (SP) en PingFederate

Puede utilizar PingFederate para crear una conexión de proveedor de servicios (SP) para cada nodo de administración del sistema. Para acelerar el proceso, importe los metadatos SAML de StorageGRID.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y ha seleccionado **Ping federate** como tipo de SSO.
- **Modo Sandbox** está seleccionado en la página Single Sign-On de Grid Manager. Consulte "Utilizar el modo de recinto de seguridad".
- Tiene el **ID de conexión SP** para cada nodo de administración de su sistema. Puede encontrar estos

valores en la tabla de detalles Admin Nodes en la página StorageGRID Single Sign-On.

- Ha descargado los **metadatos SAML** de cada nodo de administración del sistema.
- Tiene experiencia en la creación de conexiones SP en PingFederate Server.
- Usted tiene la "Guía de referencia del administrador" Para PingFederate Server. La documentación de PingFederate proporciona instrucciones detalladas paso a paso y explicaciones.
- Usted tiene la "Permiso de administrador" Para PingFederate Server.

Acerca de esta tarea

Estas instrucciones resumen cómo configurar PingFederate Server versión 10.3 como un proveedor SSO para StorageGRID. Si está utilizando otra versión de PingFederate, puede que necesite adaptar estas instrucciones. Consulte la documentación de PingFederate Server para obtener instrucciones detalladas para su publicación.

Complete los requisitos previos en PingFederate

Antes de poder crear las conexiones SP que utilizará para StorageGRID, debe completar las tareas previas en PingFederate. Utilizará la información de estos requisitos previos al configurar las conexiones del SP.

Crear almacén de datos

Si aún no lo ha hecho, cree un almacén de datos para conectar PingFederate al servidor LDAP de AD FS. Utilice los valores que utilizó cuando "configurando la federación de identidades" En StorageGRID.

- **Tipo**: Directorio (LDAP)
- **Tipo LDAP**: Active Directory
- **Nombre del atributo binario**: Introduzca **objectGUID** en la ficha atributos binarios LDAP exactamente como se muestra.

Crear validador de credenciales de contraseña

Si todavía no lo ha hecho, cree un validador de credencial de contraseña.

- **Tipo**: Validador de credenciales de nombre de usuario de LDAP
- **Almacén de datos**: Seleccione el almacén de datos que creó.
- **Search base**: Introduzca la información de LDAP (por ejemplo, DC=saml,DC=sgws).
- **Filtro de búsqueda**: SAMAccountName=${username}
- **Ámbito**: Subárbol

Crear instancia de adaptador IDP[[instancia de adaptador]]

Si todavía no lo ha hecho, cree una instancia de adaptador de IDP.

Pasos

1. Vaya a **autenticación** > **integración** > **Adaptadores IDP**.
2. Seleccione **Crear nueva instancia**.
3. En la ficha Tipo, seleccione **adaptador IDP de formulario HTML**.
4. En la ficha adaptador IDP, seleccione **Agregar una nueva fila a 'Validadores de credenciales'**.

5. Seleccione la validador de credenciales de contraseña que haya creado.
6. En la ficha atributos del adaptador, seleccione el atributo **nombre de usuario** para **seudónimo**.
7. Seleccione **Guardar**.

Crear o importar un certificado de firma[[certificado de firma]]

Si todavía no lo ha hecho, cree o importe el certificado de firma.

Pasos

1. Vaya a **Seguridad** > **claves y certificados de firma y descifrado**.
2. Cree o importe el certificado de firma.

Cree una conexión SP en PingFederate

Cuando crea una conexión del SP en PingFederate, importe los metadatos SAML que ha descargado de StorageGRID para el nodo de administración. El archivo de metadatos contiene muchos de los valores específicos necesarios.

Debe crear una conexión de SP para cada nodo de administrador en su sistema de StorageGRID, de modo que los usuarios puedan iniciar sesión desde y hacia cualquier nodo de forma segura. Utilice estas instrucciones para crear la primera conexión del SP. A continuación, vaya a. Cree conexiones adicionales del SP para crear las conexiones adicionales que necesite.

Elija el tipo de conexión del SP

Pasos

1. Vaya a **aplicaciones** > **integración** > **conexiones SP**.
2. Seleccione **Crear conexión**.
3. Seleccione **no utilice una plantilla para esta conexión**.
4. Seleccione **Examinador SSO Profiles** y **SAML 2.0** como protocolo.

Importe los metadatos de SP

Pasos

1. En la ficha Importar metadatos, seleccione **Archivo**.
2. Seleccione el archivo de metadatos de SAML que descargó de la página de inicio de sesión único de StorageGRID para el nodo de administrador.
3. Revise el resumen de metadatos y la información proporcionada en la pestaña Información general.

   El ID de entidad del partner y el nombre de conexión se establecen en el ID de conexión de StorageGRID SP. (Por ejemplo, 10.96.105.200-DC1-ADM1-105-200). La URL base es la IP del nodo de administrador de StorageGRID.

4. Seleccione **Siguiente**.

Configure el SSO del explorador IDP

Pasos

1. En la ficha SSO del explorador, seleccione **Configurar SSO del explorador**.
2. En la ficha Perfiles de SAML, seleccione las opciones **SSO iniciado por el SP**, **SLO inicial de SP**, **SSO iniciado por IDP** y **SLO iniciado por IDP**.
3. Seleccione **Siguiente**.
4. En la ficha ciclo de vida de las aserción, no realice cambios.
5. En la ficha creación de aserción, seleccione **Configurar creación de aserción**.
   a. En la ficha asignación de identidades, seleccione **Estándar**.
   b. En la ficha Contrato de atributo, utilice el formato **SAML_SUBJECT** como atributo Contract y el formato de nombre no especificado que se importó.
6. Para extender el contrato, seleccione **Eliminar** para eliminar `urn:oid`, que no se utiliza.

Asigne la instancia del adaptador

Pasos

1. En la ficha asignación de origen de autenticación, seleccione **asignar nueva instancia de adaptador**.
2. En la ficha instancias del adaptador, seleccione instancia del adaptador que haya creado.
3. En la ficha método de asignación, seleccione **recuperar atributos adicionales de un almacén de datos**.
4. En la ficha origen del atributo y Búsqueda del usuario, seleccione **Agregar origen del atributo**.
5. En la ficha almacén de datos, proporcione una descripción y seleccione almacén de datos usted agregó.
6. En la ficha Búsqueda de directorios LDAP:
   - Introduzca el **DN base**, que debe coincidir exactamente con el valor especificado en StorageGRID para el servidor LDAP.
   - Para el ámbito de búsqueda, seleccione **Subtree**.
   - Para la clase de objeto raíz, busque y agregue cualquiera de estos atributos: **ObjectGUID** o **userPrincipalName**.
7. En la ficha tipos de codificación de atributos binarios LDAP , seleccione **Base64** para el atributo **objectGUID** .
8. En la ficha filtro LDAP, introduzca **sAMAccountName=${username}**.
9. En la pestaña Cumplimiento de contrato de atributo, seleccione **LDAP (atributo)** en la lista desplegable Origen y seleccione **objectGUID** o **userPrincipalName** en la lista desplegable Valor.
10. Revise y, a continuación, guarde el origen del atributo.
11. En la ficha origen del atributo Failsave, seleccione **Anular la transacción SSO**.
12. Revise el resumen y seleccione **hecho**.
13. Seleccione **Listo**.

Configure los ajustes de protocolo

Pasos

1. En la ficha **Conexión SP** > **SSO del navegador** > **Configuración de protocolo**, seleccione **Configurar ajustes de protocolo**.
2. En la ficha URL del servicio de consumidor de aserción , acepte los valores predeterminados que se importaron desde los metadatos SAML de StorageGRID (**POST** para el enlace y. `/api/saml-response` Para la URL del extremo).

3. En la ficha direcciones URL del servicio SLO , acepte los valores predeterminados, que se importaron desde los metadatos SAML de StorageGRID (**REDIRECT** para el enlace y. `/api/saml-logout` Para la dirección URL del extremo.
4. En la pestaña Enlaces SAML permitidos, desactive **ARTEFACTO** y **SOAP**. Sólo se requieren **POST** y **REDIRECT**.
5. En la pestaña Política de firma, deje las casillas de verificación **Requerir que se firmen las solicitudes AUTHN** y **Siempre firmar afirmación** seleccionadas.
6. En la ficha Directiva de cifrado, seleccione **Ninguno**.
7. Revise el resumen y seleccione **hecho** para guardar la configuración del protocolo.
8. Revise el resumen y seleccione **hecho** para guardar la configuración de SSO del explorador.

Configurar credenciales

Pasos

1. En la ficha Conexión SP, seleccione **credenciales**.
2. En la ficha credenciales, seleccione **Configurar credenciales**.
3. Seleccione la certificado de firma ha creado o importado.
4. Seleccione **Siguiente** para ir a **gestionar ajustes de verificación de firma**.
   a. En la ficha Modelo de confianza, seleccione **sin anclar**.
   b. En la pestaña Certificado de verificación de firma, revise la información de certificación de firma, que se importó de los metadatos SAML de StorageGRID.
5. Revise las pantallas de resumen y seleccione **Guardar** para guardar la conexión SP.

Cree conexiones adicionales del SP

Puede copiar la primera conexión de SP para crear las conexiones de SP que necesita para cada nodo de administrador de su grid. Se cargan metadatos nuevos para cada copia.

> Las conexiones SP para diferentes nodos de administración utilizan valores idénticos, a excepción del ID de entidad del partner, la URL base, el ID de conexión, el nombre de conexión, la verificación de firma, Y URL de respuesta de SLO.

Pasos

1. Seleccione **Acción** > **Copiar** para crear una copia de la conexión SP inicial para cada nodo de administración adicional.
2. Introduzca el ID de conexión y el nombre de conexión para la copia y seleccione **Guardar**.
3. Elija el archivo de metadatos que corresponde al nodo de administración:
   a. Seleccione **Acción** > **Actualizar con metadatos**.
   b. Seleccione **elegir archivo** y cargue los metadatos.
   c. Seleccione **Siguiente**.
   d. Seleccione **Guardar**.
4. Resuelva el error debido al atributo no utilizado:
   a. Seleccione la nueva conexión.
   b. Seleccione **Configurar SSO del explorador > Configurar creación de aserción > Contrato de**

atributo.

c. Elimine la entrada para **urn:oid**.

d. Seleccione **Guardar**.

Desactive el inicio de sesión único

Si ya no desea usar esta funcionalidad, puede deshabilitar el inicio de sesión único (SSO). Debe deshabilitar el inicio de sesión único antes de poder deshabilitar la federación de identidades.

Antes de empezar

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

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.

   Aparece la página Single Sign-On.

2. Seleccione la opción **Desactivado**.
3. Seleccione **Guardar**.

   Aparece un mensaje de advertencia que indica que los usuarios locales podrán iniciar sesión.

4. Seleccione **OK**.

   La próxima vez que inicie sesión en StorageGRID, aparecerá la página Inicio de sesión en StorageGRID, donde deberá introducir el nombre de usuario y la contraseña de un usuario de StorageGRID local o federado.

Desactive y vuelva a habilitar temporalmente el inicio de sesión único para un nodo de administración

Es posible que no pueda iniciar sesión en Grid Manager si se desactiva el sistema de inicio de sesión único (SSO). En este caso, puede deshabilitar y volver a habilitar SSO para un nodo de administración. Para deshabilitar y, a continuación, volver a habilitar SSO, debe acceder al shell de comandos del nodo.

Antes de empezar

- Ya tienes "permisos de acceso específicos".
- Usted tiene la `Passwords.txt` archivo.
- Conoce la contraseña del usuario raíz local.

Acerca de esta tarea

Después de deshabilitar SSO para un nodo de administración, puede iniciar sesión en Grid Manager como usuario raíz local. Para proteger el sistema StorageGRID, tiene que utilizar el shell de comandos del nodo para volver a habilitar SSO en el nodo de administración tan pronto como cierre la sesión.

La deshabilitación de SSO para un nodo de administrador no afecta la configuración de SSO para ningún otro nodo de administrador que esté en el grid. La casilla de verificación **Enable SSO** en la página Single Sign-On en Grid Manager permanece seleccionada y se mantienen todas las configuraciones de SSO existentes a menos que las actualice.

Pasos

1. Inicie sesión en un nodo de administrador:
   a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Ejecute el siguiente comando:`disable-saml`

   Un mensaje indica que el comando se aplica únicamente a este nodo de administrador.

3. Confirme que desea deshabilitar SSO.

   Un mensaje indica que el inicio de sesión único está deshabilitado en el nodo.

4. Desde un explorador web, acceda a Grid Manager en el mismo nodo de administración.

   Ahora se muestra la página de inicio de sesión de Grid Manager porque SSO se ha desactivado.

5. Inicie sesión con la raíz del nombre de usuario y la contraseña del usuario raíz local.
6. Si deshabilitó temporalmente SSO debido a que debe corregir la configuración de SSO:
   a. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.
   b. Cambie la configuración incorrecta o obsoleta de SSO.
   c. Seleccione **Guardar**.

   Al seleccionar **Guardar** en la página de inicio de sesión único, se vuelve a activar SSO automáticamente para toda la cuadrícula.

7. Si ha desactivado SSO temporalmente porque necesita acceder a Grid Manager por algún otro motivo:
   a. Realice cualquier tarea o tarea que necesite realizar.
   b. Seleccione **Cerrar sesión** y cierre Grid Manager.
   c. Vuelva a habilitar SSO en el nodo de administrador. Puede realizar cualquiera de los siguientes pasos:

      - Ejecute el siguiente comando: `enable-saml`

        Un mensaje indica que el comando se aplica únicamente a este nodo de administrador.

      Confirme que desea habilitar SSO.

   Un mensaje indica que el inicio de sesión único está habilitado en el nodo.

- Reinicie el nodo de cuadrícula: `reboot`

8. Desde un explorador web, acceda a Grid Manager desde el mismo nodo de administración.
9. Confirme que aparece la página de inicio de sesión de StorageGRID y que debe introducir sus credenciales de SSO para acceder a Grid Manager.

Usar federación de grid

¿Qué es GRID federation?

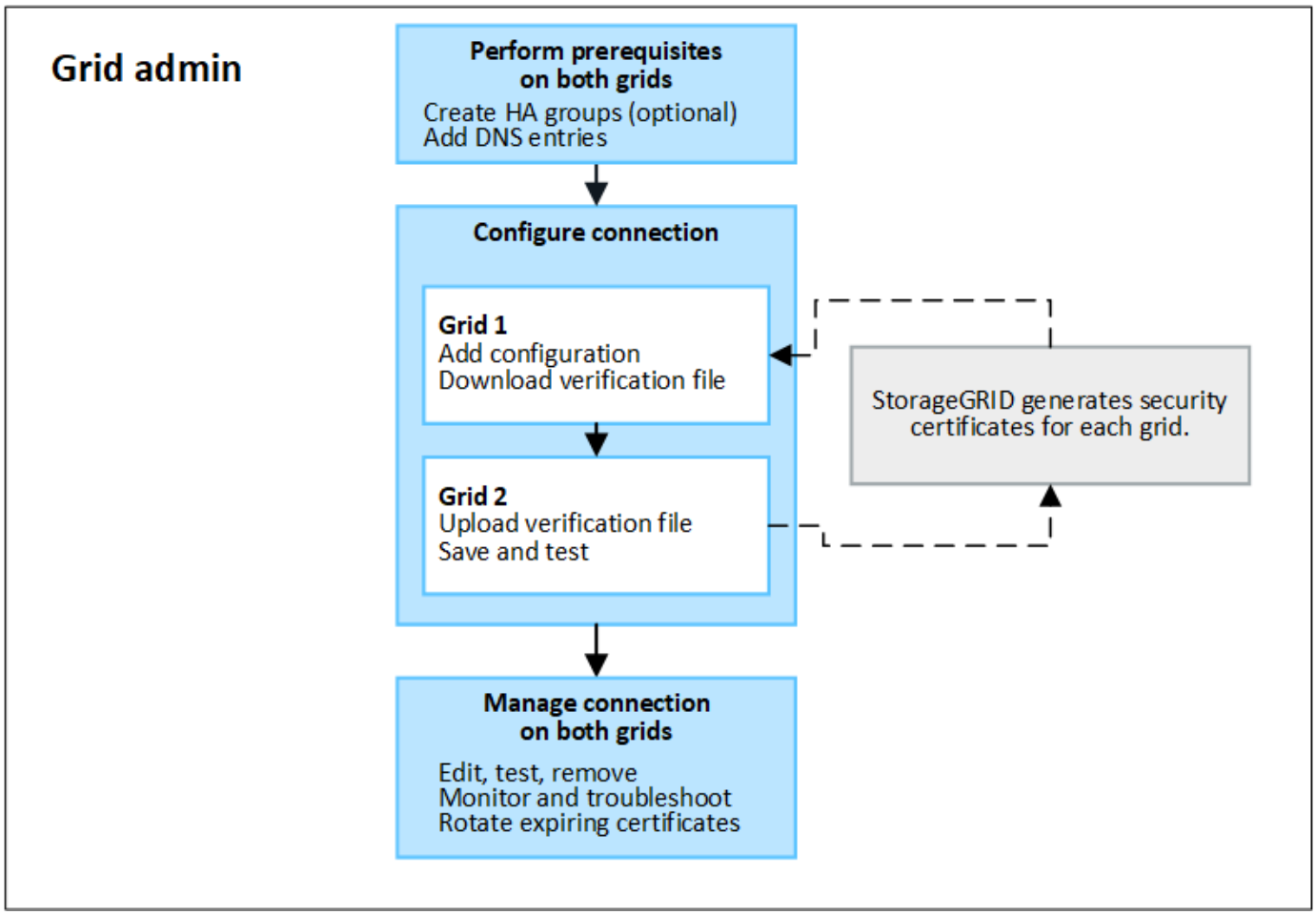
Puede utilizar la federación de grid para clonar inquilinos y replicar sus objetos entre dos sistemas StorageGRID para la recuperación ante desastres.

¿Qué es una conexión de federación de grid?

Una conexión de federación de grid es una conexión bidireccional, de confianza y segura entre los nodos de administración y puerta de enlace en dos sistemas StorageGRID.

Flujo de trabajo de federación de grid

El diagrama de flujo de trabajo resume los pasos para configurar una conexión de federación de grid entre dos cuadrículas.



Consideraciones y requisitos para las conexiones de federación de grid

- Los dos grids utilizados para la federación de grid deben ejecutar StorageGRID 11,7 o una versión posterior.
- Un grid puede tener una o más conexiones de federación de grid a otras grids. Cada conexión de federación de grid es independiente de cualquier otra conexión. Por ejemplo, si Grid 1 tiene una conexión con Grid 2 y una segunda conexión con Grid 3, no hay ninguna conexión implícita entre Grid 2 y Grid 3.
- Las conexiones de federación de grid son bidireccionales. Una vez establecida la conexión, puede supervisar y gestionar la conexión desde cualquiera de las dos redes.
- Debe existir al menos una conexión de federación de grid para poder utilizarla "clon de cuenta" o. "replicación entre grid".

Requisitos de redes y dirección IP

- Las conexiones de federación de grid se pueden producir en la red de grid, la red de administración o la red de cliente.
- Una conexión de federación de grid conecta un grid a otro. La configuración de cada grid especifica un extremo de federación de grid en el otro grid que consta de nodos de administración, nodos de puerta de enlace o ambos.
- La práctica recomendada es conectar "Grupos de alta disponibilidad" De nodos de puerta de enlace y administración en cada grid. El uso de grupos de alta disponibilidad ayuda a garantizar que las conexiones de federación de grid permanecerán en línea en caso de que los nodos dejen de estar disponibles. Si la interfaz activa en cualquiera de los grupos de alta disponibilidad falla, la conexión puede usar una interfaz de backup.
- No se recomienda crear una conexión de federación de grid que utilice la dirección IP de un único nodo de administración o nodo de pasarela. Si el nodo deja de estar disponible, la conexión de federación de grid también no estará disponible.
- "Replicación entre grid" De objetos requiere que los nodos de almacenamiento de cada grid puedan acceder a los nodos de administración y puerta de enlace configurados en el otro grid. En cada grid, confirme que todos los nodos de almacenamiento tienen una ruta de ancho de banda alto a los nodos de administración o puerta de enlace utilizados para la conexión.

Utilice FQDN para equilibrar la carga de la conexión

En un entorno de producción, utilice nombres de dominio completamente cualificados (FQDN) para identificar cada cuadrícula en la conexión. A continuación, cree las entradas DNS apropiadas, de la siguiente manera:

- El FQDN para Grid 1 se asignó a una o más direcciones IP virtuales (VIP) para grupos de alta disponibilidad en Grid 1, o a la dirección IP de uno o más nodos de administración o puerta de enlace en Grid 1.
- El FQDN para Grid 2 asignado a una o más direcciones VIP para Grid 2 o a la dirección IP de uno o más nodos de administración o puerta de enlace en Grid 2.

Cuando utiliza varias entradas DNS, las solicitudes para utilizar la conexión se equilibran de carga, de la siguiente manera:

- Las entradas de DNS que se asignan a las direcciones VIP de varios grupos de alta disponibilidad se equilibran la carga entre los nodos activos de los grupos de alta disponibilidad.
- Las entradas de DNS que se asignan a las direcciones IP de varios nodos de administración o nodos de pasarela se equilibran la carga entre los nodos asignados.

Requisitos de puertos

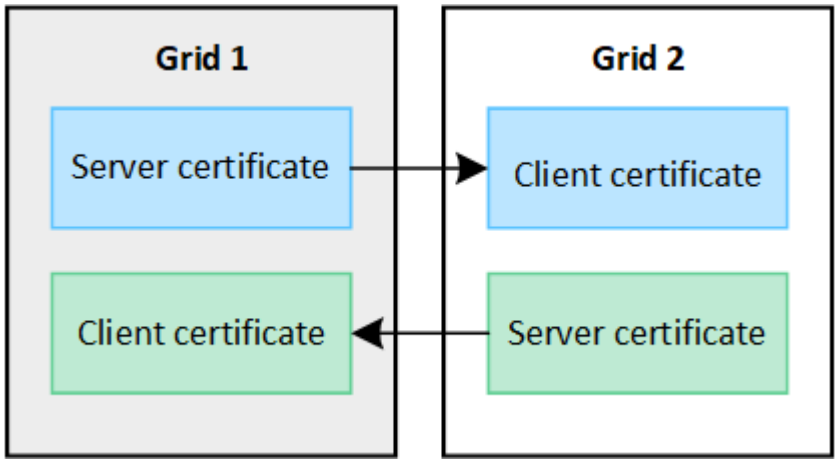
Al crear una conexión de federación de grid, puede especificar cualquier número de puerto no utilizado de 23000 a 23999. Ambas rejillas de esta conexión utilizarán el mismo puerto.

Debe asegurarse de que ningún nodo de ninguno de los grid utilice este puerto para otras conexiones.

Requisitos de certificado

Cuando se configura una conexión de federación de grid, StorageGRID genera automáticamente cuatro certificados SSL:

- Certificados de servidor y cliente para autenticar y cifrar la información enviada desde la cuadrícula 1 a la cuadrícula 2
- Certificados de servidor y cliente para autenticar y cifrar la información enviada desde la cuadrícula 2 a la cuadrícula 1



Por defecto, los certificados son válidos durante 730 días (2 años). Cuando estos certificados se acerquen a su fecha de vencimiento,
La alerta **Expiración del certificado de federación de cuadrícula** le recuerda que debe rotar los certificados, lo que puede hacer con el Administrador de cuadrícula.

> Si los certificados en cualquiera de los extremos de la conexión caducan, la conexión dejará de funcionar. La replicación de datos estará pendiente hasta que se actualicen los certificados.

Leer más

- "Crear conexiones de federación de grid"
- "Gestionar conexiones de federación de grid"
- "Solucionar errores de federación de grid"

¿Qué es el clon de cuenta?

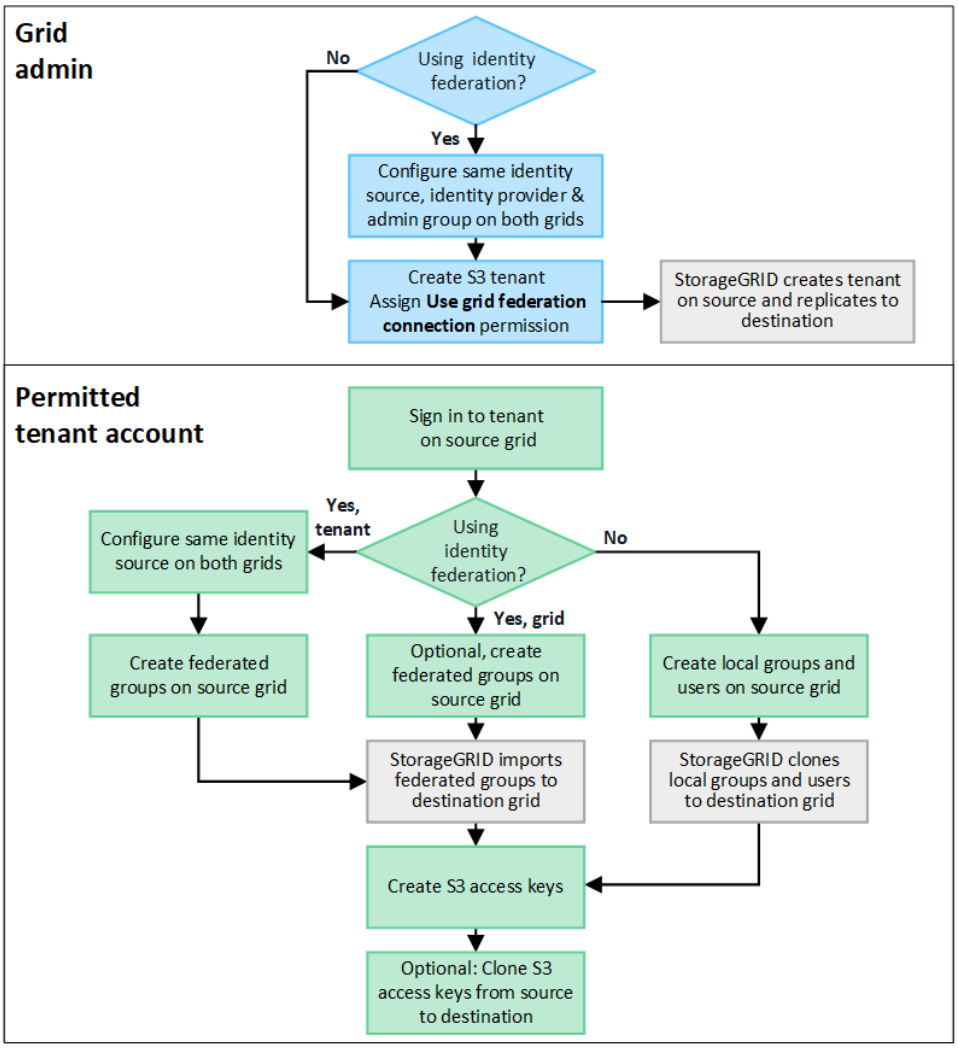
El clon de la cuenta es la replicación automática de una cuenta de inquilino, grupos de inquilinos, usuarios de inquilinos y, opcionalmente, S3 claves de acceso entre los sistemas StorageGRID en un "conexión de federación de grid".

La clonación de cuenta es necesaria para "replicación entre grid". Al clonar la información de la cuenta desde un sistema StorageGRID de origen a un sistema StorageGRID de destino se garantiza que los usuarios y

grupos inquilinos puedan acceder a los bloques y objetos correspondientes en cualquiera de los grid.

Flujo de trabajo del clon de cuenta

El diagrama de flujo de trabajo muestra los pasos que realizarán los administradores de grid y los inquilinos permitidos para configurar el clon de cuenta. Estos pasos se realizan después del "la conexión de federación de grid está configurada".



Flujo de trabajo del administrador de grid

Los pasos que realizan los administradores de grid dependen de si los sistemas StorageGRID del "conexión de federación de grid" Utilice el inicio de sesión único (SSO) o la federación de identidades.

Configurar SSO para el clon de cuenta (opcional)

Si alguno de los sistemas StorageGRID de la conexión de federación de grid utiliza SSO, ambos grids deben utilizar SSO. Antes de crear las cuentas de inquilino para la federación de grid, los administradores de grid de origen y destino del inquilino deben realizar estos pasos.

Pasos

1. Configure el mismo origen de identidad para ambas cuadrículas. Consulte "Usar la federación de identidades".

2. Configure el mismo proveedor de identidad de SSO (IdP) para ambas cuadrículas. Consulte "Configurar el inicio de sesión único".
3. "Cree el mismo grupo de administración" en ambas cuadrículas importando el mismo grupo federado.

   Al crear el inquilino, seleccionará este grupo para que tenga el permiso inicial de acceso raíz para las cuentas de inquilino de origen y de destino.

   > Si este grupo de administración no existe en ambas cuadrículas antes de crear el arrendatario, el arrendatario no se replica en el destino.

Configurar federación de identidades a nivel de cuadrícula para el clon de cuenta (opcional)

Si alguno de los sistemas StorageGRID utiliza la federación de identidades sin SSO, ambas cuadrículas deben utilizar la federación de identidades. Antes de crear las cuentas de inquilino para la federación de grid, los administradores de grid de origen y destino del inquilino deben realizar estos pasos.

Pasos

1. Configure el mismo origen de identidad para ambas cuadrículas. Consulte "Usar la federación de identidades".
2. Opcionalmente, si un grupo federado tendrá permiso inicial de acceso root para las cuentas de arrendatario de origen y destino, "cree el mismo grupo de administración" en ambas cuadrículas importando el mismo grupo federado.

   > Si asigna permiso de acceso raíz a un grupo federado que no existe en ambas cuadrículas, el inquilino no se replica en la cuadrícula de destino.

3. Si no desea que un grupo federado tenga permiso de acceso raíz inicial para ambas cuentas, especifique una contraseña para el usuario raíz local.

Cree una cuenta de inquilino de S3 permitida

Después de configurar, de manera opcional, el inicio de sesión único o la federación de identidades, un administrador de grid lleva a cabo estos pasos para determinar qué inquilinos pueden replicar objetos del bloque en otros sistemas StorageGRID.

Pasos

1. Determine qué grid desea que sea la cuadrícula de origen del inquilino para las operaciones de clonación de cuentas.

   La cuadrícula donde se creó originalmente el inquilino se conoce como *source grid* del inquilino. La cuadrícula donde se replica el inquilino se conoce como *grid de destino* del inquilino.

2. En esa cuadrícula, cree una nueva cuenta de inquilino de S3 o edite una cuenta existente.
3. Asigne el permiso **Use grid federation connection**.
4. Si la cuenta de inquilino administrará sus propios usuarios federados, asigne el permiso **Usar propia fuente de identidad**.

   Si se asigna este permiso, tanto las cuentas de arrendatario de origen como las de destino deben configurar el mismo origen de identidad antes de crear grupos federados. Los grupos federados agregados al inquilino de origen no se pueden clonar en el inquilino de destino a menos que ambas cuadrículas utilicen el mismo origen de identidad.

5. Seleccione una conexión de federación de cuadrícula específica.
6. Guarde el inquilino nuevo o modificado.

   Cuando se guarda un nuevo inquilino con el permiso **Usar conexión de federación de grid**, StorageGRID crea automáticamente una réplica de ese inquilino en la otra cuadrícula, de la siguiente manera:

   - Ambas cuentas de inquilino tienen el mismo ID de cuenta, nombre, cuota de almacenamiento y permisos asignados.
   - Si seleccionó un grupo federado para tener permiso de acceso raíz para el inquilino, ese grupo se clona en el inquilino de destino.
   - Si seleccionó un usuario local para que tenga permiso de acceso raíz para el inquilino, ese usuario se clona en el inquilino de destino. Sin embargo, la contraseña para ese usuario no está clonada.

Para obtener más información, consulte "Gestionar inquilinos permitidos para la federación de grid".

Flujo de trabajo de cuenta de inquilino permitido

Después de que un inquilino con el permiso **Usar conexión de federación de grid** se replica en la cuadrícula de destino, las cuentas de inquilino permitidas pueden realizar estos pasos para clonar grupos de inquilinos, usuarios y claves de acceso S3.

Pasos

1. Inicie sesión en la cuenta de inquilino en la cuadrícula de origen del inquilino.
2. Si está permitido, configure Identify federation tanto en las cuentas de arrendatario de origen como en las de destino.
3. Cree grupos y usuarios en el arrendatario de origen.

   Cuando se crean nuevos grupos o usuarios en el inquilino de origen, StorageGRID los clona automáticamente en el inquilino de destino, pero no se produce ningún clonado del destino al origen.

4. Crear claves de acceso S3.
5. Opcionalmente, clone las claves de acceso S3 del inquilino de origen al inquilino de destino.

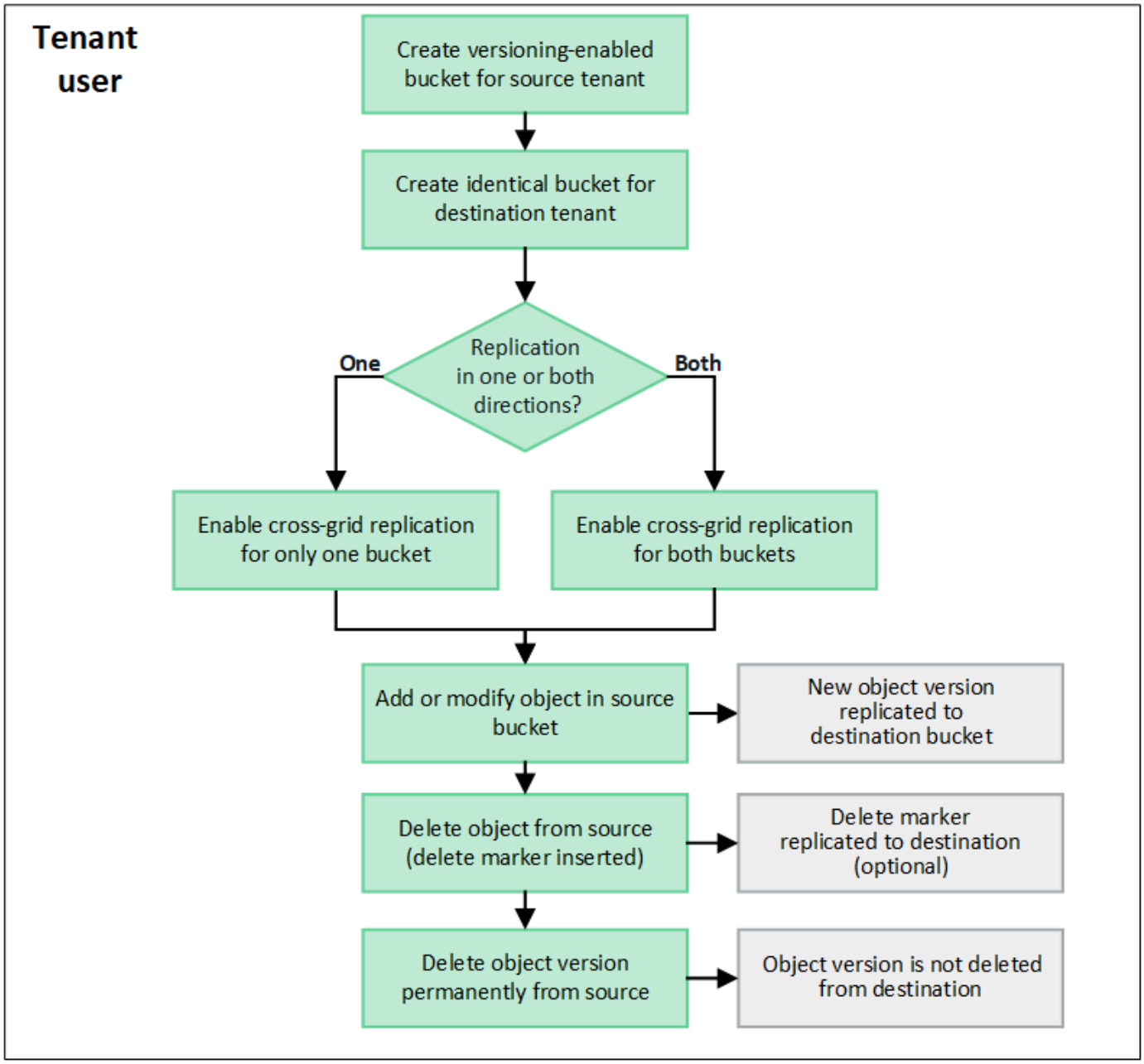
Para obtener detalles sobre el flujo de trabajo permitido de la cuenta de inquilino y saber cómo se clonan los grupos, los usuarios y las claves de acceso S3, consulte "Clone los usuarios y los grupos de inquilinos" y.. "Clone las claves de acceso S3 mediante la API".

¿Qué es la replicación entre grid?

La replicación entre grid es la replicación automática de objetos entre buckets de S3 seleccionados en dos sistemas StorageGRID conectados en un "conexión de federación de grid". "Clon de cuenta" es necesario para la replicación entre grid.

Flujo de trabajo de replicación entre grid

El diagrama de flujo de trabajo resume los pasos para configurar la replicación entre bloques en dos cuadrículas.



Requisitos de la replicación entre grid

Si una cuenta de inquilino tiene el permiso **Use grid federation connection** para usar uno o más "conexiones de federación de grid", Un usuario inquilino con permiso de acceso root puede crear cubos idénticos en las cuentas de inquilino correspondientes en cada cuadrícula. Estos bloques:

- Debe tener el mismo nombre pero puede tener regiones diferentes
- Debe tener el control de versiones activado
- Debe tener S3 Object Lock desactivado
- Debe estar vacío

Una vez creados ambos bloques, la replicación entre grid se puede configurar para uno o ambos bloques.

Leer más

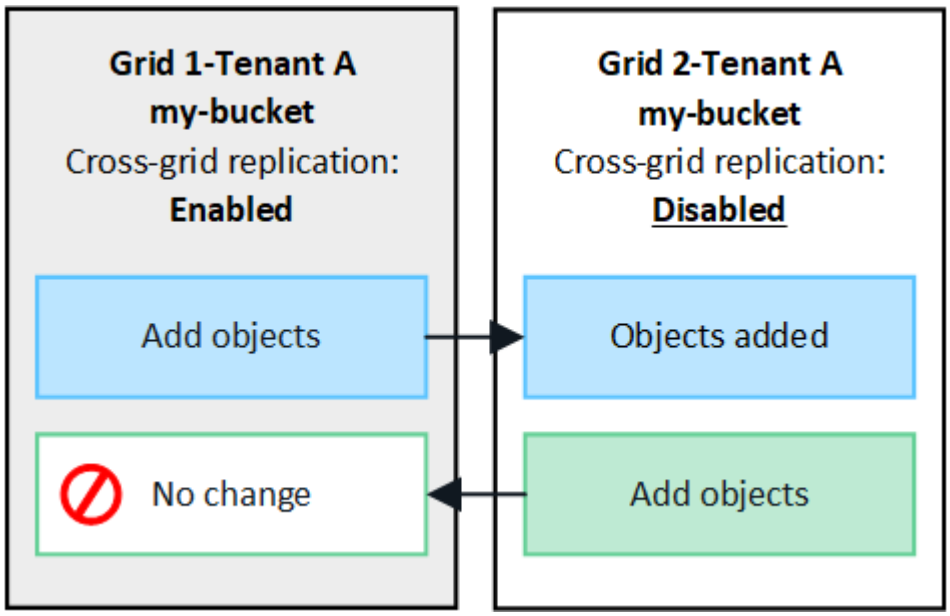
"Gestionar la replicación entre grid"

Funcionamiento de la replicación entre grid

La replicación entre grid puede configurarse para que ocurra en una dirección o en ambas direcciones.

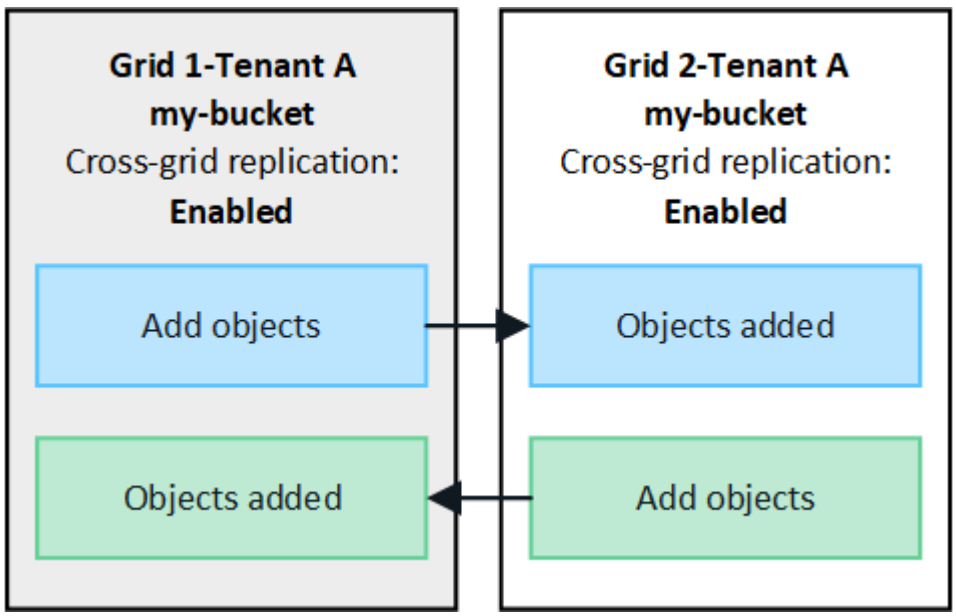
Replicación en una dirección

Si habilita la replicación entre grid para un bucket en solo una grid, los objetos agregados a ese bucket (el bucket de origen) se replican en el bucket correspondiente en la otra grid (el bucket de destino). Sin embargo, los objetos añadidos al depósito de destino no se vuelven a replicar en el origen. En la figura, la replicación entre grid está activada para `my-bucket` De la cuadrícula 1 a la cuadrícula 2, pero no está activada en la otra dirección.



Replicación en ambas direcciones

Si habilita la replicación entre grid para el mismo bucket en ambos grids, los objetos agregados a cada bucket se replican en el otro grid. En la figura, la replicación entre grid está activada para `my-bucket` en ambas direcciones.



¿Qué sucede cuando se ingieren objetos?

Cuando un cliente S3 agrega un objeto a un bloque que tiene habilitada la replicación entre grid, sucede lo siguiente:

1. StorageGRID replica automáticamente el objeto del bloque de origen al de destino. El tiempo para realizar esta operación de replicación en segundo plano depende de varios factores, incluidos la cantidad de otras operaciones de replicación pendientes.

   El cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud GetObject o HeadObject. La respuesta incluye un recurso específico de StorageGRID `x-ntap-sg-cgr-replication-status` cabecera de respuesta, que tendrá uno de los siguientes valores:
   El cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud GetObject o HeadObject. La respuesta incluye un recurso específico de StorageGRID `x-ntap-sg-cgr-replication-status` cabecera de respuesta, que tendrá uno de los siguientes valores:

Cuadrícula	Estado de replicación
Origen	• **ÉXITO**: La replicación fue exitosa para todas las conexiones a la red. • **PENDIENTE**: El objeto no ha sido replicado en al menos una conexión de red. • **FALLO**: La replicación no está pendiente para ninguna conexión a la red y al menos una falló con un fallo permanente. Un usuario debe resolver el error.
Destino	**REPLICA**: El objeto fue replicado desde la cuadrícula de origen.

   > ⓘ StorageGRID no admite el `x-amz-replication-status` encabezado.

2. StorageGRID utiliza las políticas de ILM activas de cada grid para gestionar los objetos, al igual que lo haría con cualquier otro objeto. Por ejemplo, el objeto A en Grid 1 se puede almacenar como dos copias replicadas y conservarse permanentemente, mientras que la copia del objeto A replicado en Grid 2 se puede almacenar con el código de borrado 2+1 y eliminarse después de tres años.

¿Qué sucede cuando se eliminan los objetos?

Como se describe en "Eliminar flujo de datos", StorageGRID puede eliminar un objeto por cualquiera de estos motivos:

- El cliente S3 emite una solicitud de eliminación.
- Un usuario del gestor de inquilinos selecciona el "Suprimir objetos del depósito" opción para eliminar todos los objetos de un depósito.
- El bloque tiene una configuración del ciclo de vida que caduca.
- El último periodo de tiempo de la regla de ILM para el objeto finaliza, y no se han especificado más ubicaciones.

Cuando StorageGRID elimina un objeto debido a una operación Eliminar objetos en el bloque, la caducidad del ciclo de vida del bloque o la caducidad de la ubicación de ILM, el objeto replicado nunca se elimina del otro grid en una conexión de la federación de grid. Sin embargo, los marcadores de borrado que se han añadido al

bloque de origen mediante eliminaciones de clientes de S3 se pueden replicar opcionalmente en el bloque de destino.

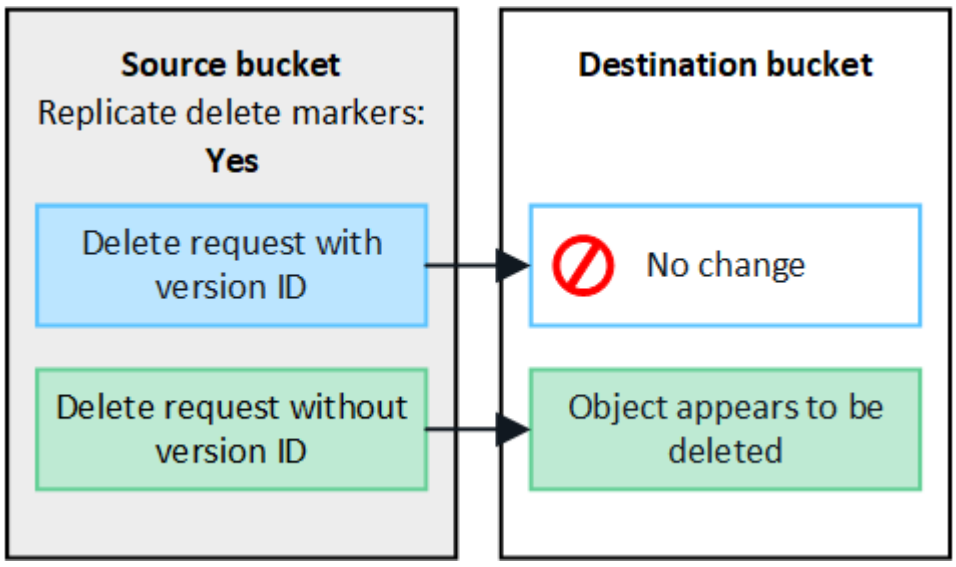
Para comprender qué sucede cuando un cliente S3 elimina objetos de un bloque que tiene habilitada la replicación entre grid, revise cómo los clientes S3 eliminan objetos de los bloques que tienen el control de versiones activado, de la siguiente manera:

- Si un cliente S3 emite una solicitud de eliminación que incluye un ID de versión, esa versión del objeto se elimina de forma permanente. No se ha añadido ningún marcador de borrado al depósito.
- Si un cliente S3 emite una solicitud de eliminación que no incluye un ID de versión, StorageGRID no elimina ninguna versión de objeto. En su lugar, agrega un marcador de borrado al cubo. El marcador de borrado hace que StorageGRID actúe como si el objeto se hubiera eliminado:
  - Una solicitud GetObject sin un identificador de versión fallará con `404 No Object Found`
  - Una solicitud GetObject con un identificador de versión válido se realizará correctamente y devolverá la versión del objeto solicitado.

Cuando un cliente S3 elimina un objeto de un bloque que tiene habilitada la replicación entre grid, StorageGRID determina si desea replicar la solicitud de eliminación en el destino, de la siguiente manera:

- Si la solicitud de eliminación incluye un ID de versión, esa versión de objeto se elimina permanentemente de la cuadrícula de origen. Sin embargo, StorageGRID no replica las solicitudes de eliminación que incluyan un ID de versión, por lo que la misma versión del objeto no se elimina del destino.
- Si la solicitud de eliminación no incluye un ID de versión, StorageGRID puede replicar opcionalmente el marcador de eliminación, en función de cómo se configure la replicación entre grid para el bloque:
  - Si decide replicar marcadores de eliminación (valor predeterminado), se agrega un marcador de eliminación al bloque de origen y se replica en el bloque de destino. De hecho, el objeto parece eliminarse en ambas cuadrículas.
  - Si decide no replicar marcadores de eliminación, se agrega un marcador de eliminación al depósito de origen, pero no se replica en el depósito de destino. De hecho, los objetos que se eliminan en la cuadrícula de origen no se eliminan en la cuadrícula de destino.

En la figura, **REPLY DELETE MARKERS** se estableció en **Yes** cuando "se ha activado la replicación entre grid". Las solicitudes de supresión para el bloque de origen que incluyan un identificador de versión no suprimirán los objetos del bloque de destino. Las solicitudes de supresión del depósito de origen que no incluyan un ID de versión aparecerán para suprimir objetos del depósito de destino.



Si desea mantener sincronizadas las eliminaciones de objetos entre las cuadrículas, cree las correspondientes "Configuraciones de ciclo de vida de S3" para los cucharones de ambas rejillas.

Cómo se replican los objetos cifrados

Cuando se utiliza la replicación entre grid para replicar objetos entre grids, se pueden cifrar objetos individuales, utilizar el cifrado de bucket predeterminado o configurar el cifrado de toda la grid. Puede agregar, modificar o eliminar la configuración de cifrado predeterminada de bloque o de grid antes o después de habilitar la replicación entre grid para un bloque.

Para cifrar objetos individuales, puede utilizar SSE (cifrado del lado del servidor con claves gestionadas por StorageGRID) al agregar los objetos al depósito de origen. Utilice la `x-amz-server-side-encryption` solicitar cabecera y especificar `AES256`. Consulte "Usar cifrado del servidor".

El uso de SSE-C (cifrado en el lado del servidor con claves proporcionadas por el cliente) no es compatible para la replicación entre grid. La operación de ingesta fallará.

Para utilizar el cifrado predeterminado para un depósito, utilice una solicitud PutBucketEncryption y establezca el `SSEAlgorithm` parámetro a. `AES256`. El cifrado de nivel de bloque se aplica a cualquier objeto ingerido sin `x-amz-server-side-encryption` solicite el encabezado. Consulte "Operaciones en bloques".

Para utilizar el cifrado a nivel de cuadrícula, establezca la opción **cifrado de objetos almacenados** en **AES-256**. El cifrado de nivel de grid se aplica a cualquier objeto que no esté cifrado en el nivel del bloque o que se ingiera sin `x-amz-server-side-encryption` solicite el encabezado. Consulte "Configure las opciones de red y objeto".

SSE no admite AES-128. Si la opción **cifrado de objetos almacenados** está habilitada para la cuadrícula de origen mediante la opción **AES-128**, el uso del algoritmo AES-128 no se propagará al objeto replicado. En su lugar, el objeto replicado utilizará la configuración de cifrado de nivel de grid o bloque predeterminada del destino, si está disponible.

Al determinar cómo cifrar los objetos de origen, StorageGRID aplica estas reglas:

1. Utilice la `x-amz-server-side-encryption` encabezado de ingesta, si existe.
2. Si no hay una cabecera de ingesta, utilice la configuración de cifrado predeterminado de depósito, si está configurada.
3. Si no se ha configurado una configuración de depósito, utilice la configuración de cifrado de toda la cuadrícula, si está configurada.
4. Si no hay una configuración para toda la cuadrícula, no cifre el objeto de origen.

Al determinar cómo cifrar los objetos replicados, StorageGRID aplica estas reglas en este orden:

1. Use el mismo cifrado que el objeto de origen, a menos que ese objeto utilice cifrado AES-128.
2. Si el objeto de origen no está cifrado o utiliza AES-128, utilice la configuración de cifrado predeterminada del depósito de destino, si está configurada.
3. Si el depósito de destino no tiene una configuración de cifrado, utilice la configuración de cifrado de toda la cuadrícula del destino, si está configurada.
4. Si no hay una configuración de toda la cuadrícula, no cifre el objeto de destino.

PutObjectTagging y DeleteObjectTagging no son compatibles

Las solicitudes PutObjectTagging y DeleteObjectTagging no están soportadas para los objetos de los depósitos que tienen activada la replicación entre grid.

Si un cliente S3 emite una solicitud PutObjectTagging o DeleteObjectTagging, `501 Not Implemented` se devuelve. El mensaje es `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured`.

Cómo se replican los objetos segmentados

El tamaño máximo del segmento de la cuadrícula de origen se aplica a los objetos replicados a la cuadrícula de destino. Cuando los objetos se replican en otra cuadrícula, el ajuste **Tamaño de segmento máximo** (**CONFIGURACIÓN** > **Sistema** > **Opciones de almacenamiento**) de la cuadrícula de origen se utilizará en ambas cuadrículas. Por ejemplo, supongamos que el tamaño máximo del segmento para la cuadrícula de origen es de 1 GB, mientras que el tamaño máximo del segmento de la cuadrícula de destino es de 50 MB. Si ingiere un objeto de 2 GB en la cuadrícula de origen, ese objeto se guarda como dos segmentos de 1 GB. También se replicará en la cuadrícula de destino como dos segmentos de 1 GB, aunque el tamaño máximo del segmento de esa cuadrícula sea de 50 MB.

Compare la replicación entre grid y la replicación de CloudMirror

A medida que comience a utilizar la federación de cuadrícula, revise las similitudes y diferencias entre "replicación entre grid" y la "Servicio de replicación CloudMirror de StorageGRID".

	Replicación entre grid	Servicio de replicación de CloudMirror
¿Cuál es el objetivo principal?	Un sistema StorageGRID actúa como sistema de recuperación ante desastres. Los objetos de un depósito se pueden replicar entre las cuadrículas en una o en ambas direcciones.	Permite que un inquilino replique automáticamente objetos de un bloque en StorageGRID (origen) a un bloque S3 externo (destino). La replicación de CloudMirror crea una copia independiente de un objeto en una infraestructura de S3 independiente. Esta copia independiente no se usa como backup, pero suele procesarse en el cloud.
¿Cómo se configura?	1. Configure una conexión de federación de grid entre dos cuadrículas. 2. Agregar nuevas cuentas de inquilino, que se clonan automáticamente en el otro grid. 3. Añadir usuarios y grupos de inquilinos nuevos que también se clonan. 4. Crea los bloques correspondientes en cada grid y permite que la replicación entre grid se realice en una o en ambas direcciones.	1. Un usuario de inquilino configura la replicación de CloudMirror definiendo un extremo de CloudMirror (dirección IP, credenciales, etc.) mediante el administrador de inquilinos o la API de S3. 2. Se puede configurar cualquier bloque que pertenezca a esa cuenta de inquilino para que apunte al extremo de CloudMirror.

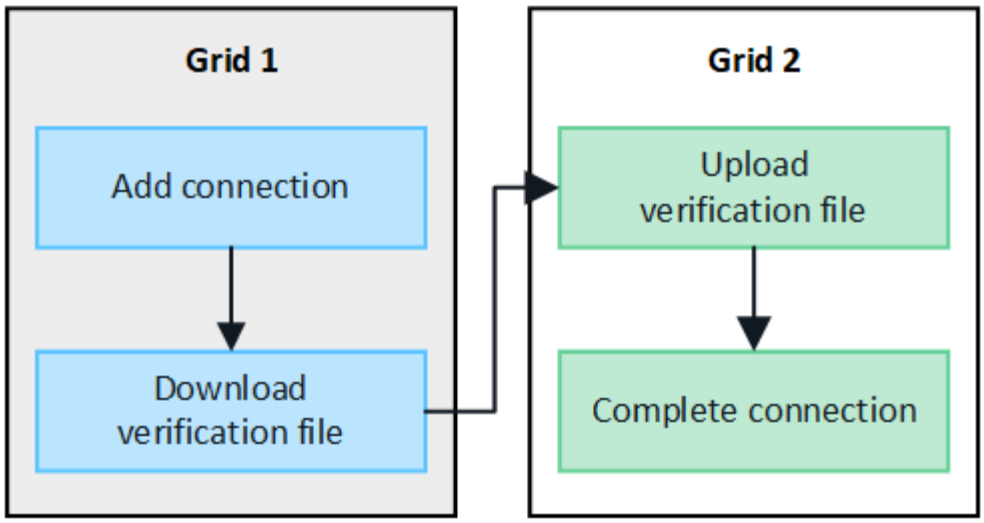
	Replicación entre grid	Servicio de replicación de CloudMirror
¿Quién es responsable de su configuración ?	• Un administrador de grid configura la conexión y los inquilinos. • Los usuarios inquilinos configuran los grupos, los usuarios, las claves y los buckets.	Normalmente, un usuario inquilino.
¿Cuál es el destino?	Un bloque de S3 correspondiente e idéntico en el otro sistema StorageGRID de la conexión de federación de grid.	• Cualquier infraestructura S3 compatible (incluido Amazon S3). • Google Cloud Platform (GCP)
¿Se requiere el control de versiones de objetos?	Sí, tanto los depósitos de origen como de destino deben tener activado el control de versiones de objetos.	No, la replicación de CloudMirror admite cualquier combinación de buckets sin versiones y con versiones tanto en el origen como en el destino.
¿Qué hace que los objetos se muevan al destino?	Los objetos se replican automáticamente cuando se añaden a un bloque que tiene habilitada la replicación entre grid.	Los objetos se replican automáticamente cuando se añaden a un bloque que se ha configurado con un extremo de CloudMirror. Los objetos que existían en el bloque de origen antes de que se configurara con el extremo de CloudMirror no se replican, a menos que se modifiquen.
¿Cómo se replican los objetos?	La replicación entre grid crea objetos con versiones y replica el identificador de versión del bloque de origen al bloque de destino. Esto permite mantener el orden de versión en ambas cuadrículas.	La replicación de CloudMirror no requiere buckets habilitados para el control de versiones, por lo que CloudMirror solo puede mantener el pedido de una clave dentro de un sitio. No hay garantías de que el pedido se mantendrá para las solicitudes a un objeto en un sitio diferente.
¿Qué pasa si un objeto no se puede replicar?	El objeto se pone en cola para la replicación, sujeto a los límites de almacenamiento de metadatos.	El objeto se pone en cola para la replicación, sujeto a los límites de servicios de la plataforma (consulte "Recomendaciones para el uso de servicios de plataformas").
¿Se replican los metadatos del sistema del objeto?	Sí, cuando un objeto se replica en la otra cuadrícula, sus metadatos del sistema también se replican. Los metadatos serán idénticos en ambas cuadrículas.	No, cuando un objeto se replica en el depósito externo, sus metadatos del sistema se actualizan. Los metadatos variarán entre ubicaciones, en función del tiempo de procesamiento y del comportamiento de la infraestructura S3 independiente.

	Replicación entre grid	Servicio de replicación de CloudMirror
¿Cómo se recuperan los objetos?	Las aplicaciones pueden recuperar o leer objetos mediante la realización de una solicitud al depósito en cualquier cuadrícula.	Las aplicaciones pueden recuperar o leer objetos realizando una solicitud en StorageGRID o en el destino de S3. Por ejemplo, supongamos que usa la replicación de CloudMirror para reflejar objetos en una organización asociada. El partner puede utilizar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario usar StorageGRID.
¿Qué sucede si se elimina un objeto?	• Las solicitudes de supresión que incluyan un ID de versión nunca se replican en la cuadrícula de destino. • Las solicitudes de eliminación que no incluyen un ID de versión agregan un marcador de eliminación al depósito de origen, que opcionalmente se puede replicar en la cuadrícula de destino. • Si la replicación entre grid se configura para una sola dirección, los objetos del bucket de destino se pueden eliminar sin afectar al origen.	Los resultados variarán en función del estado de control de versiones de los depósitos de origen y destino (que no necesitan ser los mismos): • Si ambos cubos están versionados, una solicitud de eliminación agregará un marcador de eliminación en ambas ubicaciones. • Si sólo se ha versionado el depósito de origen, una solicitud de supresión agregará un marcador de supresión al origen pero no al destino. • Si ninguno de los depósitos está versionado, una solicitud de supresión suprimirá el objeto del origen pero no del destino. Del mismo modo, los objetos del bloque de destino se pueden eliminar sin que ello afecte al origen.

Crear conexiones de federación de grid

Puede crear una conexión de federación de grid entre dos sistemas StorageGRID si desea clonar detalles de inquilinos y replicar datos de objetos.

Como se muestra en la figura, la creación de una conexión de federación de cuadrícula incluye pasos en ambas cuadrículas. Agrega la conexión en una cuadrícula y la completa en la otra. Puede empezar desde cualquiera de las dos cuadrículas.



Antes de empezar

- Ha revisado el "consideraciones y requisitos" para configurar conexiones de federación de grid.
- Si planea utilizar nombres de dominio completos (FQDN) para cada cuadrícula en lugar de direcciones IP o VIP, sabrá qué nombres utilizar y confirmará que el servidor DNS de cada cuadrícula tiene las entradas adecuadas.
- Está utilizando un "navegador web compatible".
- Dispone de permiso de acceso raíz y la frase de acceso de aprovisionamiento para ambas cuadrículas.

Agregar conexión

Realice estos pasos en cualquiera de los dos sistemas StorageGRID.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal de cualquiera de las cuadrículas.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. Selecciona **Añadir conexión**.
4. Introduzca los detalles de la conexión.

Campo	Descripción
Nombre de conexión	Un nombre único para ayudarle a reconocer esta conexión, por ejemplo, “Grid 1-Grid 2”.
FQDN o IP para este grid	Uno de los siguientes: • El FQDN del grid en el que está conectado actualmente • Dirección VIP de un grupo de alta disponibilidad en esta cuadrícula • La dirección IP de un nodo de administración o un nodo de pasarela en este grid. La IP puede estar en cualquier red a la que pueda acceder la cuadrícula de destino.

Campo	Descripción
Puerto	Puerto que desea utilizar para esta conexión. Puede introducir cualquier número de puerto no utilizado del 23000 al 23999. Ambas rejillas de esta conexión utilizarán el mismo puerto. Debe asegurarse de que ningún nodo de ninguno de los grid utilice este puerto para otras conexiones.
Días válidos de certificado para esta cuadrícula	El número de días que desea que los certificados de seguridad de esta cuadrícula de la conexión sean válidos. El valor predeterminado es 730 días (2 años), pero puede introducir cualquier valor de 1 a 762 días. StorageGRID genera automáticamente certificados de cliente y de servidor para cada grid al guardar la conexión.
Aprovisionamiento de la clave de acceso para este grid	La clave de acceso de aprovisionamiento para el grid en el que ha iniciado sesión.
FQDN o IP para el otro grid	Uno de los siguientes: • El FQDN del grid al que desea conectarse • Una dirección VIP de un grupo de alta disponibilidad en la otra cuadrícula • Una dirección IP de un nodo de administración o nodo de pasarela en el otro grid. La IP puede estar en cualquier red a la que pueda acceder la red de origen.

5. Selecciona **Guardar y continuar**.
6. Para el paso Descargar archivo de verificación, seleccione **Descargar archivo de verificación**.

   Una vez completada la conexión en la otra cuadrícula, ya no podrá descargar el archivo de verificación de ninguna de las dos.

7. Busque el archivo descargado (*`connection-name`*`.grid-federation`), y guárdelo en un lugar seguro.

   > ⚠ Este archivo contiene secretos (enmascarados como *****) y otros datos confidenciales y deben almacenarse y transmitirse de forma segura.

8. Selecciona **Cerrar** para volver a la página de Grid federation.
9. Confirme que se muestra la nueva conexión y que su **estado de conexión** está **esperando para conectarse**.
10. Proporcione el *`connection-name`*`.grid-federation` en el administrador de grid para el otro grid.

Conexión completa

Realice estos pasos en el sistema StorageGRID al que se está conectando (la otra cuadrícula).

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. Seleccione **Cargar archivo de verificación** para acceder a la página Cargar.
4. Seleccione **Cargar archivo de verificación**. A continuación, busque y seleccione el archivo que se descargó de la primera cuadrícula (*connection-name*`.grid-federation`).

   Se muestran los detalles de la conexión.

5. Opcionalmente, introduzca un Núm. Diferente de días válidos para los certificados de seguridad de esta cuadrícula. La entrada **Certificate Valid Days** establece por defecto el valor que ingresaste en la primera cuadrícula, pero cada cuadrícula puede usar diferentes fechas de vencimiento.

   En general, utilice el mismo número de días para los certificados en ambos lados de la conexión.

   > Si los certificados en cualquiera de los extremos de la conexión caducan, la conexión dejará de funcionar y las replicaciones estarán pendientes hasta que se actualicen los certificados.

6. Introduzca la clave de acceso de aprovisionamiento para la cuadrícula en la que está conectado actualmente.
7. Seleccione **Guardar y probar**.

   Los certificados se generan y se prueba la conexión. Si la conexión es válida, aparece un mensaje de éxito y la nueva conexión se muestra en la página federación de Cuadrícula. El **Estado de conexión** será **Conectado**.

   Si aparece un mensaje de error, solucione cualquier problema. Consulte "Solucionar errores de federación de grid".

8. Vaya a la página Grid federation en la primera cuadrícula y actualice el explorador. Confirme que el **Estado de conexión** es ahora **Conectado**.
9. Una vez establecida la conexión, elimine de forma segura todas las copias del archivo de verificación.

   Si edita esta conexión, se creará un nuevo archivo de verificación. No se puede volver a utilizar el archivo original.

Después de terminar

- Revise las consideraciones para "gestión de inquilinos permitidos".
- "Cree una o más cuentas de arrendatario nuevas", Asigne el permiso **Use grid federation connection** y seleccione la nueva conexión.
- "Gestionar la conexión" según sea necesario. Puede editar valores de conexión, probar una conexión, rotar certificados de conexión o eliminar una conexión.
- "Supervise la conexión" Como parte de sus actividades normales de monitoreo de StorageGRID.
- "Solucione los problemas de la conexión", incluyendo la resolución de alertas y errores relacionados con la clonación de cuentas y la replicación entre redes.

Gestionar conexiones de federación de grid

La gestión de las conexiones de federación de grid entre sistemas StorageGRID incluye editar detalles de conexión, girar los certificados, eliminar permisos de inquilinos y

eliminar conexiones que no se utilizan.

Antes de empezar

- Ha iniciado sesión en Grid Manager en cualquiera de las tablas mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz" para la cuadrícula en la que ha iniciado sesión.

Edite una conexión de federación de cuadrícula

Puede editar una conexión de federación de grid iniciando sesión en el nodo de administración principal en cualquier cuadrícula de la conexión. Después de realizar cambios en la primera cuadrícula, debe descargar un nuevo archivo de verificación y cargarlo en la otra cuadrícula.

> Mientras se edita la conexión, las solicitudes de clonación de cuentas o replicación entre cuadrículas seguirán utilizando la configuración de conexión existente. Las ediciones que realice en la primera cuadrícula se guardan localmente, pero no se utilizan hasta que se hayan cargado en la segunda cuadrícula, se hayan guardado y probado.

Comience a editar la conexión

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal de cualquiera de las cuadrículas.
2. Seleccione * NODOS * y confirme que todos los demás nodos de administración del sistema estén en línea.

   > Cuando edita una conexión de federación de grid, StorageGRID intenta guardar un archivo de configuración de candidato en todos los nodos de administración de la primera cuadrícula. Si este archivo no se puede guardar en todos los nodos de administración, aparecerá un mensaje de advertencia al seleccionar **Guardar y probar**.

3. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
4. Edite los detalles de la conexión utilizando el menú **Acciones** de la página de federación de cuadrícula o la página de detalles de una conexión específica. Consulte "Crear conexiones de federación de grid" para qué entrar.

   Menú Actions

   a. Seleccione el botón de opción para la conexión.
   b. Selecciona **Acciones** > **Editar**.
   c. Introduzca la nueva información.

   Detalles

   a. Seleccione un nombre de conexión para mostrar sus detalles.
   b. Seleccione **Editar**.
   c. Introduzca la nueva información.

5. Introduzca la clave de acceso de aprovisionamiento para la cuadrícula en la que ha iniciado sesión.
6. Selecciona **Guardar y continuar**.

Los nuevos valores se guardan, pero no se aplicarán a la conexión hasta que haya cargado el nuevo archivo de verificación en la otra cuadrícula.

7. Seleccione **Descargar archivo de verificación**.

   Para descargar este archivo más adelante, vaya a la página de detalles de la conexión.

8. Busque el archivo descargado (*connection-name*`.grid-federation`), y guárdelo en un lugar seguro.

   > El archivo de verificación contiene secretos y debe almacenarse y transmitirse de forma segura.

9. Selecciona **Cerrar** para volver a la página de Grid federation.
10. Confirme que el **Estado de conexión** es **Edición pendiente**.

    > Si el estado de la conexión no era **Connected** cuando comenzó a editar la conexión, no cambiará a **Pending edit**.

11. Proporcione el *connection-name*`.grid-federation` en el administrador de grid para el otro grid.

Termine de editar la conexión

Termine de editar la conexión cargando el archivo de verificación en la otra cuadrícula.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. Seleccione **Cargar archivo de verificación** para acceder a la página de carga.
4. Seleccione **Cargar archivo de verificación**. A continuación, busque y seleccione el archivo que se descargó de la primera cuadrícula.
5. Introduzca la clave de acceso de aprovisionamiento para la cuadrícula en la que está conectado actualmente.
6. Seleccione **Guardar y probar**.

   Si la conexión se puede establecer mediante los valores editados, aparece un mensaje de éxito. De lo contrario, aparecerá un mensaje de error. Revise el mensaje y resuelva cualquier problema.

7. Cierre el asistente para volver a la página Grid federation.
8. Confirme que el **Estado de conexión** es **Conectado**.
9. Vaya a la página Grid federation en la primera cuadrícula y actualice el explorador. Confirme que el **Estado de conexión** es ahora **Conectado**.
10. Una vez establecida la conexión, elimine de forma segura todas las copias del archivo de verificación.

Pruebe una conexión de federación de grid

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.

3. Pruebe la conexión utilizando el menú **Acciones** de la página de Grid federation o la página de detalles de una conexión específica.

   Menú Actions

   a. Seleccione el botón de opción para la conexión.

   b. Selecciona **Acciones** > **Prueba**.

   Detalles

   a. Seleccione un nombre de conexión para mostrar sus detalles.

   b. Seleccione **probar conexión**.

4. Revise el estado de conexión:

Estado de conexión	Descripción
Conectado	Ambas rejillas están conectadas y se comunican con normalidad.
Error	La conexión está en estado de error. Por ejemplo, un certificado ha caducado o un valor de configuración ya no es válido.
Edición pendiente	Ha editado la conexión en esta cuadrícula, pero la conexión sigue utilizando la configuración existente. Para completar la edición, cargue el nuevo archivo de verificación en la otra cuadrícula.
Esperando conexión	Ha configurado la conexión en esta cuadrícula, pero la conexión no se ha completado en la otra. Descargue el archivo de verificación de esta cuadrícula y cárguelo en la otra cuadrícula.
Desconocido	La conexión está en estado desconocido, posiblemente debido a un problema de red o a un nodo sin conexión.

5. Si el estado de la conexión es **Error**, resuelva cualquier problema. A continuación, seleccione **Probar conexión** de nuevo para confirmar que el problema se ha solucionado.

Girar certificados de conexión

Cada conexión de federación de grid utiliza cuatro certificados SSL generados automáticamente para proteger la conexión. Cuando los dos certificados para cada cuadrícula se acercan a su fecha de vencimiento, la alerta **Caducidad del certificado de federación de cuadrícula** le recuerda que debe rotar los certificados.

> Si los certificados en cualquiera de los extremos de la conexión caducan, la conexión dejará de funcionar y las replicaciones estarán pendientes hasta que se actualicen los certificados.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal de cualquiera de las cuadrículas.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. En cualquiera de los separadores de la página Grid federation, seleccione el nombre de la conexión para

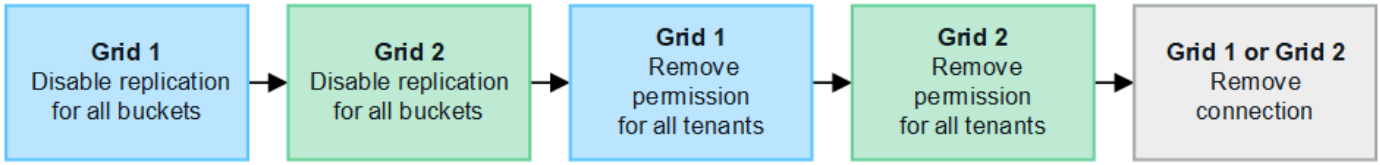
mostrar sus detalles.

4. Seleccione la ficha **certificados**.
5. Seleccione **Girar certificados**.
6. Especifique cuántos días deben ser válidos los certificados nuevos.
7. Introduzca la clave de acceso de aprovisionamiento para la cuadrícula en la que ha iniciado sesión.
8. Seleccione **Girar certificados**.
9. Si es necesario, repita estos pasos en la otra cuadrícula de la conexión.

   En general, utilice el mismo número de días para los certificados en ambos lados de la conexión.

Elimine una conexión de federación de cuadrícula

Puede eliminar una conexión de federación de cuadrícula de cualquiera de las dos cuadrículas de la conexión. Como se muestra en la figura, debe realizar los pasos de requisitos previos en ambas cuadrículas para confirmar que la conexión no está siendo utilizada por ningún inquilino en ninguna de las cuadrículas.



Antes de eliminar una conexión, tenga en cuenta lo siguiente:

- La eliminación de una conexión no elimina ningún elemento que ya se haya copiado entre las cuadrículas. Por ejemplo, los usuarios, grupos y objetos de arrendatarios que existen en ambas cuadrículas no se eliminan de ninguna de las cuadrículas cuando se elimina el permiso del arrendatario. Si desea eliminar estos elementos, debe eliminarlos manualmente de ambas cuadrículas.
- Al eliminar una conexión, cualquier objeto que esté pendiente de replicación (ingerido pero que aún no se haya replicado en la otra cuadrícula) tendrá un fallo permanente en su replicación.

Desactive la replicación para todos los bloques de inquilinos

Pasos

1. A partir de cualquier cuadrícula, inicie sesión en Grid Manager desde el nodo de administración principal.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. Seleccione el nombre de la conexión para mostrar sus detalles.
4. En la pestaña **Arrendatarios permitidos**, determine si la conexión está siendo utilizada por algún inquilino.
5. Si se muestra algún arrendatario, indique a todos los arrendatarios que "desactive la replicación entre grid" para todos sus cucharones en ambas rejillas de la conexión.

> No puede eliminar el permiso **Usar conexión de federación de grid** si algún depósito de inquilino tiene habilitada la replicación entre grid. Cada cuenta de inquilino debe deshabilitar la replicación entre grid en sus bloques en ambos grids.

Eliminar permiso para cada inquilino

Después de que la replicación entre redes se haya desactivado para todos los depósitos de inquilinos, elimine el permiso **Usar federación de grid** de todos los inquilinos en ambas cuadrículas.

Pasos

1. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
2. Seleccione el nombre de la conexión para mostrar sus detalles.
3. Para cada inquilino en la pestaña **Arrendatarios permitidos**, elimine el permiso **Usar conexión de federación de grid** de cada inquilino. Consulte "Gestionar inquilinos permitidos".
4. Repita estos pasos para los inquilinos permitidos en la otra cuadrícula.

Retire la conexión

Pasos

1. Cuando ningún inquilino de ninguna de las dos rejillas esté usando la conexión, seleccione **Eliminar**.
2. Revise el mensaje de confirmación y seleccione **Eliminar**.
   - Si se puede eliminar la conexión, se muestra un mensaje de éxito. La conexión de federación de cuadrícula se elimina ahora de ambas cuadrículas.
   - Si la conexión no se puede eliminar (por ejemplo, aún está en uso o hay un error de conexión), se muestra un mensaje de error. Puede realizar una de las siguientes acciones:
     - Resuelva el error (recomendado). Consulte "Solucionar errores de federación de grid".
     - Retire la conexión por la fuerza. Consulte la siguiente sección.

Elimine una conexión de federación de cuadrícula por fuerza

Si es necesario, puede forzar la eliminación de una conexión que no tiene el estado **CONECTADA**.

La eliminación forzada sólo elimina la conexión de la rejilla local. Para eliminar completamente la conexión, realice los mismos pasos en ambas rejillas.

Pasos

1. En el cuadro de diálogo de confirmación, selecciona **Forzar eliminación**.

   Aparece un mensaje de éxito. Esta conexión de federación de grid ya no se puede utilizar. Sin embargo, es posible que los bloques de inquilinos aún tengan habilitada la replicación entre grid, y es posible que algunas copias de objeto ya se hayan replicado entre los grids en la conexión.

2. Desde la otra cuadrícula de la conexión, inicie sesión en Grid Manager desde el nodo de administración principal.
3. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
4. Seleccione el nombre de la conexión para mostrar sus detalles.
5. Selecciona **Eliminar** y **Sí**.
6. Seleccione **Forzar eliminación** para eliminar la conexión de esta cuadrícula.

Gestione los inquilinos permitidos para la federación de grid

Puede permitir que las cuentas de inquilino de S3 usen una conexión de federación de

grid entre dos sistemas StorageGRID. Cuando se permite a los inquilinos utilizar una conexión, se requieren pasos especiales para editar los detalles del arrendatario o para eliminar permanentemente el permiso de un arrendatario para usar la conexión.

Antes de empezar

- Ha iniciado sesión en Grid Manager en cualquiera de las tablas mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz" para la cuadrícula en la que ha iniciado sesión.
- Ya tienes "se ha creado una conexión de federación de grid" entre dos cuadrículas.
- Ha revisado los flujos de trabajo para "clon de cuenta" y.. "replicación entre grid".
- Según sea necesario, ya ha configurado Single Sign-On (SSO) o Identify federation para ambas cuadrículas en la conexión. Consulte "Qué es el clon de cuenta".

Cree un inquilino permitido

Si desea permitir que una cuenta de inquilino nueva o existente utilice una conexión de federación de grid para la clonación de cuentas y la replicación entre grid, siga las instrucciones generales a. "Cree un nuevo inquilino S3" o. "edite una cuenta de inquilino" y tenga en cuenta lo siguiente:

- Puede crear el inquilino desde cualquier cuadrícula en la conexión. La cuadrícula donde se crea un inquilino es la cuadrícula de origen del *tenant*.
- El estado de la conexión debe ser **Conectado**.
- Cuando el inquilino se crea o edita para habilitar el permiso **Usar conexión de federación de grid** y luego se guarda en la primera cuadrícula, un inquilino idéntico se replica automáticamente en la otra cuadrícula. La cuadrícula en la que se replica el inquilino es la cuadrícula de destino del *tenant*.
- Los inquilinos de ambas cuadrículas tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos. Opcionalmente, puede utilizar el campo **Descripción** para ayudar a identificar cuál es el inquilino de origen y cuál es el inquilino de destino. Por ejemplo, esta descripción para un inquilino creado en Grid 1 también aparecerá para el inquilino replicado en Grid 2: «Este inquilino se creó en Grid 1».
- Por motivos de seguridad, la contraseña de un usuario raíz local no se copia en la cuadrícula de destino.

> Antes de que un usuario raíz local pueda iniciar sesión en el inquilino replicado en la cuadrícula de destino, un administrador de grid para ese grid debe "cambie la contraseña del usuario raíz local".

- Una vez que el arrendatario nuevo o editado esté disponible en ambas cuadrículas, los usuarios del arrendatario pueden realizar estas operaciones:
  - A partir del grid de origen del inquilino, cree grupos y usuarios locales que se clonan automáticamente en el grid de destino del inquilino. Consulte "Clone los usuarios y los grupos de inquilinos".
  - Crear nuevas claves de acceso S3, que se pueden clonar opcionalmente en el grid de destino del inquilino. Consulte "Clone las claves de acceso S3 mediante la API".
  - Cree depósitos idénticos en ambas cuadrículas de la conexión y habilite la replicación entre cuadrículas en una dirección o en ambas direcciones. Consulte "Gestionar la replicación entre grid".

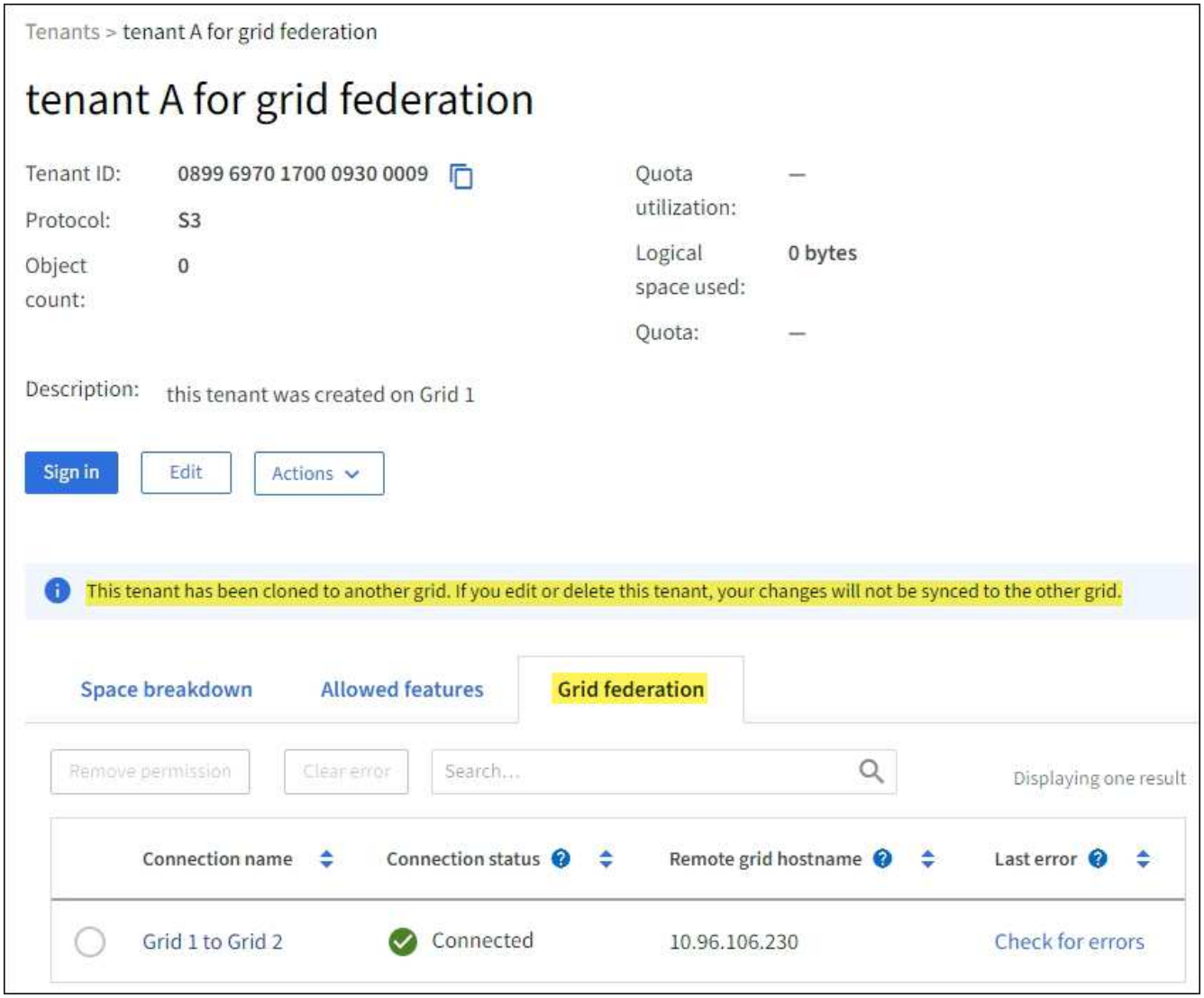
Ver un inquilino permitido

Puede ver los detalles de un inquilino con permiso para utilizar una conexión de federación de grid.

Pasos

1. Seleccione **ARRENDATARIOS**.
2. En la página Tenedores, seleccione el nombre del arrendatario para ver la página de detalles del arrendatario.

   Si se trata de la cuadrícula de origen del inquilino (es decir, si el inquilino se creó en esta cuadrícula), aparece un banner para recordarle que el inquilino se clonó en otra cuadrícula. Si edita o elimina este arrendatario, los cambios no se sincronizarán con la otra cuadrícula.



3. Opcionalmente, seleccione la pestaña **Grid federation** a. "supervise la conexión de federación de grid".

Editar un arrendatario permitido

Si necesita editar un inquilino que tiene el permiso **Usar conexión de federación de grid**, siga las instrucciones generales para "editar una cuenta de inquilino" y tenga en cuenta lo siguiente:

- Si un inquilino tiene el permiso **Usar conexión de federación de grid**, puede editar los detalles del inquilino desde cualquier cuadrícula en la conexión. Sin embargo, los cambios que realice no se copiarán en la otra cuadrícula. Si desea mantener sincronizados los detalles del arrendatario entre las cuadrículas, debe realizar las mismas modificaciones en ambas cuadrículas.
- No puede borrar el permiso **Usar conexión de federación de grid** cuando está editando un inquilino.

- No puede seleccionar una conexión de federación de grid diferente al editar un inquilino.

Suprimir un arrendatario permitido

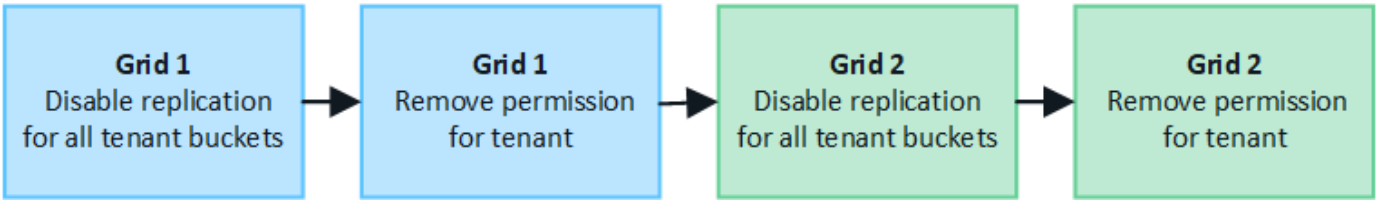
Si necesita eliminar un inquilino que tiene el permiso **Usar conexión de federación de grid**, siga las instrucciones generales para "eliminación de una cuenta de inquilino" y tenga en cuenta lo siguiente:

- Antes de poder eliminar el arrendatario original en la cuadrícula de origen, debe eliminar todos los depósitos de la cuenta en la cuadrícula de origen.
- Para poder quitar el inquilino clonado en la cuadrícula de destino, debe eliminar todos los buckets de la cuenta de la cuadrícula de destino.
- Si quita el inquilino original o el clonado, la cuenta ya no se puede usar para la replicación entre grid.
- Si va a eliminar el inquilino original en la cuadrícula de origen, los grupos de inquilinos, usuarios o las claves que se hayan clonado en el grid de destino no se verán afectados. Puede eliminar el inquilino clonado o permitir que gestione sus propios grupos, usuarios, claves de acceso y bloques.
- Si va a quitar el inquilino clonado en la cuadrícula de destino, se producirán errores de clonado si se añaden usuarios o grupos nuevos al inquilino original.

  Para evitar estos errores, elimine el permiso del inquilino para utilizar la conexión de federación de grid antes de eliminar el inquilino de esta cuadrícula.

Eliminar el permiso de conexión Usar federación de grid

Para evitar que un inquilino utilice una conexión de federación de grid, debe eliminar el permiso **Usar conexión de federación de grid**.



Antes de eliminar el permiso de un inquilino para utilizar una conexión de federación de grid, tenga en cuenta lo siguiente:

- No puede eliminar el permiso **Usar conexión de federación de grid** si alguno de los depósitos del inquilino tiene habilitada la replicación entre grid. La cuenta de inquilino debe deshabilitar primero la replicación entre grid en todos sus bloques.
- Eliminar el permiso **Usar conexión de federación de cuadrícula** no elimina ningún elemento que ya se haya replicado entre las cuadrículas. Por ejemplo, los usuarios, grupos y objetos de arrendatarios que existen en ambas cuadrículas no se eliminan de ninguna de las cuadrículas cuando se elimina el permiso del arrendatario. Si desea eliminar estos elementos, debe eliminarlos manualmente de ambas cuadrículas.
- Si desea volver a habilitar este permiso con la misma conexión de federación de grid, suprima primero este inquilino en la cuadrícula de destino; de lo contrario, si vuelve a habilitar este permiso, se producirá un error.

> Al volver a habilitar el permiso **Usar conexión de federación de grid**, la cuadrícula local se convierte en la cuadrícula de origen y activa la clonación en la cuadrícula remota especificada por la conexión de federación de grid seleccionada. Si la cuenta de inquilino ya existe en la cuadrícula remota, la clonación provocará un error de conflicto.

Antes de empezar

- Está utilizando un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz" para ambas cuadrículas.

Desactive la replicación para bloques de clientes

Como primer paso, deshabilite la replicación entre grid para todos los buckets de inquilinos.

Pasos

1. A partir de cualquier cuadrícula, inicie sesión en Grid Manager desde el nodo de administración principal.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. Seleccione el nombre de la conexión para mostrar sus detalles.
4. En la pestaña **Arrendatarios permitidos**, determine si el inquilino está usando la conexión.
5. Si el inquilino aparece en la lista, indíquele que lo haga "desactive la replicación entre grid" para todos sus cucharones en ambas rejillas de la conexión.

> No puede eliminar el permiso **Usar conexión de federación de grid** si algún depósito de inquilino tiene habilitada la replicación entre grid. El inquilino debe deshabilitar la replicación entre grid en sus buckets en ambas grids.

Eliminar permiso para arrendatario

Una vez deshabilitada la replicación entre grid para bloques de inquilinos, puede eliminar el permiso del inquilino para utilizar la conexión de federación de grid.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Elimine el permiso de las páginas Grid federation o Tenants.

Página de federación de grid

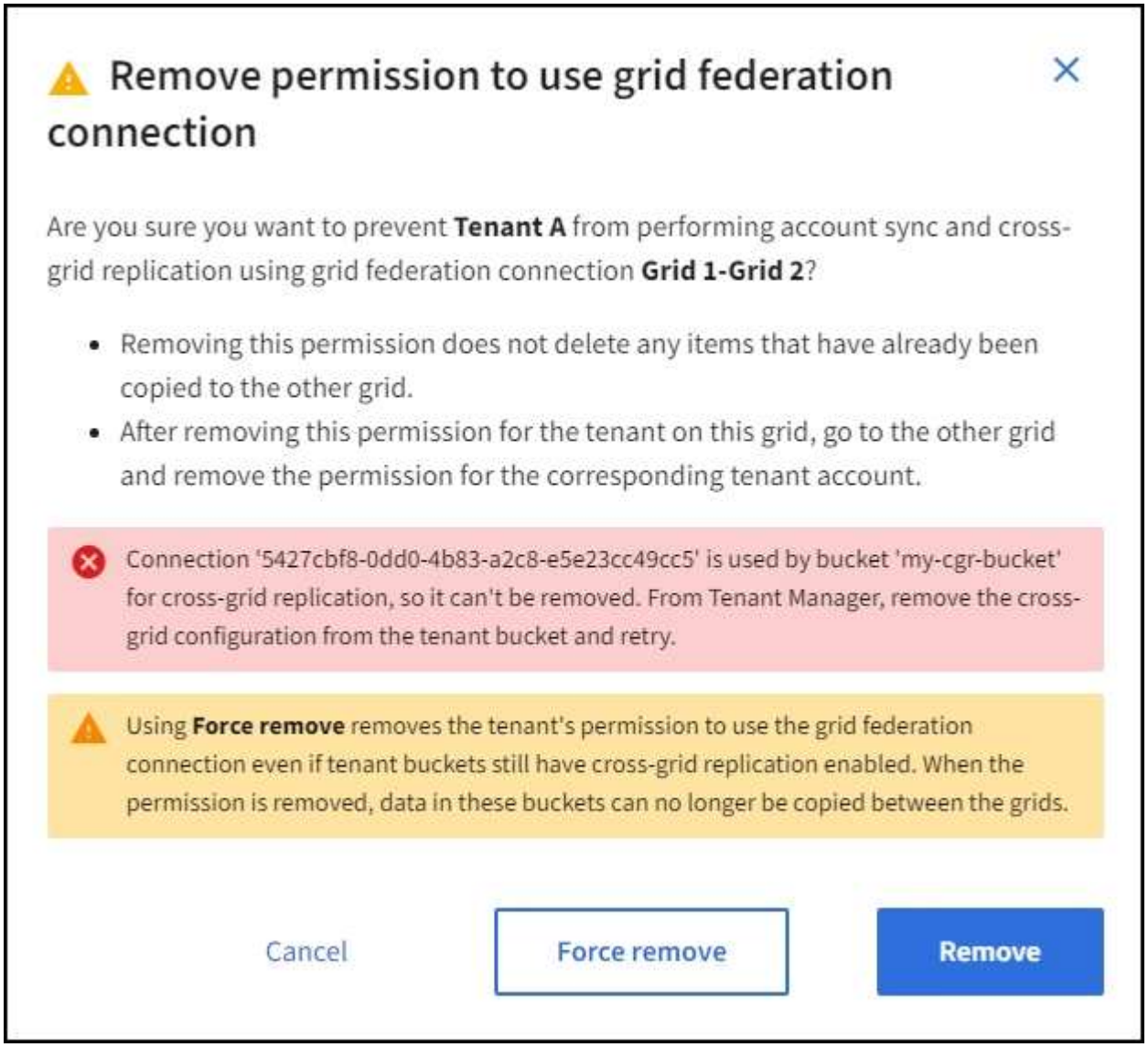
a. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
b. Seleccione el nombre de la conexión para mostrar su página de detalles.
c. En la pestaña **Arrendatarios permitidos**, seleccione el botón de radio para el inquilino.
d. Selecciona **Eliminar permiso**.

Inquilinos

a. Seleccione **ARRENDATARIOS**.
b. Seleccione el nombre del arrendatario para mostrar la página de detalles.
c. En la pestaña **Grid federation**, seleccione el botón de radio para la conexión.
d. Selecciona **Eliminar permiso**.

3. Revise las advertencias en el cuadro de diálogo de confirmación y seleccione **Eliminar**.
   - Si el permiso se puede eliminar, volverá a la página de detalles y aparecerá un mensaje de éxito. Este inquilino ya no puede utilizar la conexión de federación de grid.

◦ Si uno o más bloques de inquilinos aún tienen habilitada la replicación entre grid, se muestra un error.



Puede realizar una de las siguientes acciones:

- (Recomendado). Inicie sesión en el Gestor de inquilinos y deshabilite la replicación para cada uno de los buckets del inquilino. Consulte "Gestionar la replicación entre grid". Luego, repita los pasos para eliminar el permiso **Usar conexión a la cuadrícula**.
- Elimine el permiso por la fuerza. Consulte la siguiente sección.

4. Vaya a la otra cuadrícula y repita estos pasos para eliminar el permiso para el mismo inquilino en la otra cuadrícula.

Elimine el permiso por la fuerza

Si es necesario, puede forzar la eliminación del permiso de un inquilino para utilizar una conexión de federación de grid incluso si los buckets de inquilinos tienen habilitada la replicación entre grid.

Antes de eliminar el permiso de un inquilino por la fuerza, tenga en cuenta las consideraciones generales para eliminando el permiso así como estas consideraciones adicionales:

- Si elimina el permiso **Usar conexión de federación de grid** por fuerza, cualquier objeto que esté

pendiente de replicación en la otra cuadrícula (ingerido pero no replicado aún) seguirá siendo replicado. Para evitar que estos objetos en curso lleguen al depósito de destino, también debe eliminar el permiso del inquilino en la otra cuadrícula.

- Cualquier objeto ingerido en el depósito de origen después de eliminar el permiso **Usar conexión de federación de grid** nunca se replicará en el depósito de destino.

Pasos

1. Inicie sesión en Grid Manager desde el nodo de administración principal.
2. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.
3. Seleccione el nombre de la conexión para mostrar su página de detalles.
4. En la pestaña **Arrendatarios permitidos**, seleccione el botón de radio para el inquilino.
5. Selecciona **Eliminar permiso**.
6. Revise las advertencias en el cuadro de diálogo de confirmación y seleccione **Forzar eliminación**.

   Aparece un mensaje de éxito. Este inquilino ya no puede utilizar la conexión de federación de grid.

7. Según sea necesario, vaya a la otra cuadrícula y repita estos pasos para forzar la eliminación del permiso para la misma cuenta de inquilino en la otra cuadrícula. Por ejemplo, debe repetir estos pasos en la otra cuadrícula para evitar que los objetos en curso lleguen al depósito de destino.

Solucionar errores de federación de grid

Es posible que deba solucionar alertas y errores relacionados con las conexiones de federación de grid, el clon de cuenta y la replicación entre grid.

Alertas y errores de conexión de federación de grid

Es posible que reciba alertas o se produzcan errores con las conexiones de federación de grid.

Después de realizar cualquier cambio para resolver un problema de conexión, pruebe la conexión para asegurarse de que el estado de la conexión vuelva a **CONECTADA**. Para ver instrucciones, consulte "Gestionar conexiones de federación de grid".

Alerta de fallo de conexión de federación de grid

Problema

Se ha activado la alerta de error de conexión **Grid federation**.

Detalles

Esta alerta indica que la conexión de federación de rejilla entre las cuadrículas no funciona.

Acciones recomendadas

1. Revise la configuración en la página Grid Federation para ambas cuadrículas. Confirme que todos los valores son correctos. Consulte "Gestionar conexiones de federación de grid".
2. Revise los certificados utilizados para la conexión. Asegúrese de que no haya alertas para los certificados de federación de grid vencidos y que los detalles de cada certificado sean válidos. Consulte las instrucciones para girar los certificados de conexión en "Gestionar conexiones de federación de grid".
3. Confirme que todos los nodos ADMIN y Gateway de ambas cuadrículas están en línea y disponibles. Resuelva las alertas que puedan estar afectando a estos nodos y vuelva a intentarlo.

4. Si proporcionó un nombre de dominio completo (FQDN) para la cuadrícula local o remota, confirme que el servidor DNS esté en línea y disponible. Consulte "¿Qué es GRID federation?" Para los requisitos de redes, dirección IP y DNS.

La alerta de caducidad del certificado de federación de grid

Problema

Se activó la alerta **Expiración del certificado de federación de red**.

Detalles

Esta alerta indica que uno o más certificados de federación de grid están a punto de caducar.

Acciones recomendadas

Consulte las instrucciones para girar los certificados de conexión en "Gestionar conexiones de federación de grid".

Error al editar una conexión de federación de cuadrícula

Problema

Al editar una conexión de federación de grid, aparece el siguiente mensaje de advertencia cuando selecciona **Guardar y probar**: “No se pudo crear un archivo de configuración de candidato en uno o más nodos”.

Detalles

Cuando edita una conexión de federación de grid, StorageGRID intenta guardar un archivo de configuración de candidato en todos los nodos de administración de la primera cuadrícula. Aparece un mensaje de advertencia si este archivo no se puede guardar en todos los nodos de administración, por ejemplo, porque un nodo de administración está fuera de línea.

Acciones recomendadas

1. En la cuadrícula que está utilizando para editar la conexión, seleccione * NODOS *.
2. Confirmar que todos los nodos de administración de ese grid están en línea.
3. Si alguno de los nodos está sin conexión, vuelva a conectarlo e intente editar nuevamente la conexión.

Errores de clonación de cuenta

No se puede iniciar sesión en una cuenta de inquilino clonada

Problema

No puede iniciar sesión en una cuenta de inquilino clonada. El mensaje de error de la página de inicio de sesión del gestor de inquilinos indica que las credenciales de esta cuenta no son válidas. Inténtelo de nuevo.

Detalles

Por motivos de seguridad, cuando se clona una cuenta de inquilino desde la cuadrícula de origen del inquilino a la cuadrícula de destino del inquilino, la contraseña que configuró para el usuario raíz local del inquilino no se clona. De la misma forma, cuando un inquilino crea usuarios locales en su grid de origen, las contraseñas de usuario local no se clonan en el grid de destino.

Acciones recomendadas

Antes de que el usuario raíz pueda iniciar sesión en la cuadrícula de destino del inquilino, primero debe hacerlo un administrador de grid "cambie la contraseña del usuario raíz local" en la cuadrícula de destino.

Para que un usuario local clonado pueda iniciar sesión en la cuadrícula de destino del inquilino, el usuario raíz

del inquilino clonado debe agregar una contraseña para el usuario en la cuadrícula de destino. Para ver instrucciones, consulte "Gestionar usuarios locales" En las instrucciones de uso del Gestor de inquilinos.

Inquilino creado sin un clon

Problema

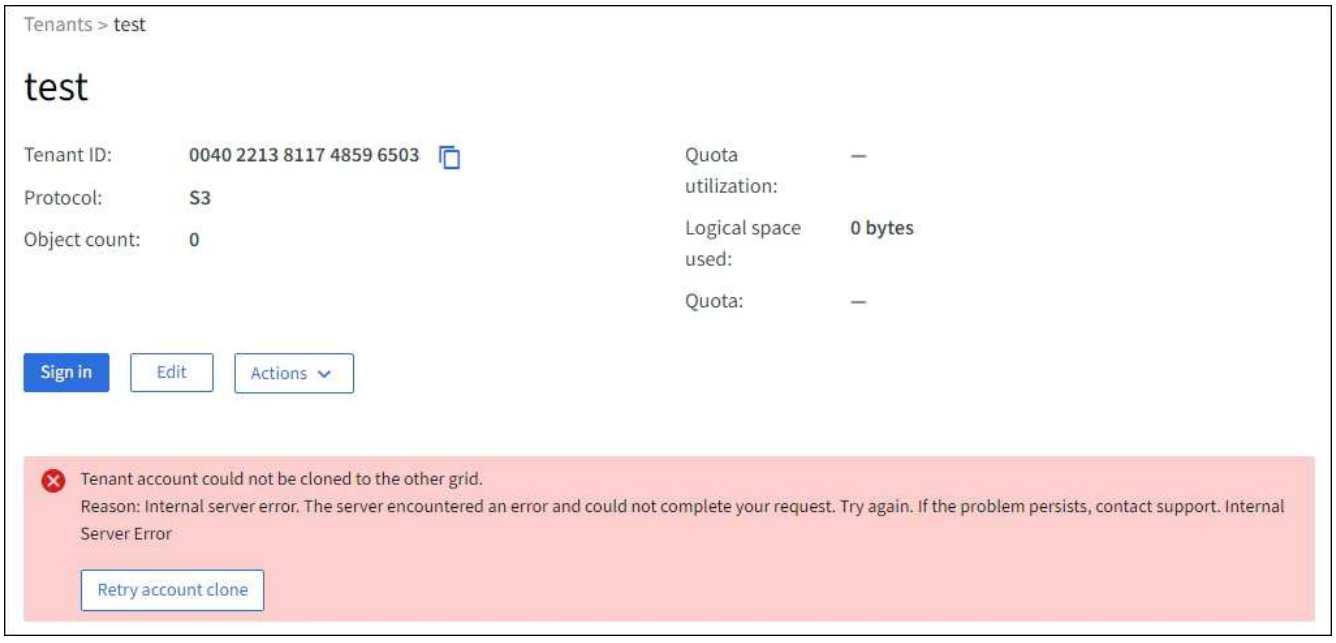
Puede ver el mensaje “Tenant created without a clone” después de crear un nuevo inquilino con el permiso **use grid federation connection**.

Detalles

Este problema puede ocurrir si las actualizaciones del estado de conexión se retrasan, lo que podría provocar que una conexión no saludable se listara como **Connected**.

Acciones recomendadas

1. Revise el motivo que aparece en el mensaje de error y resuelva cualquier problema de red u otros problemas que puedan impedir el funcionamiento de la conexión. Consulte Alertas y errores de conexión de federación de grid.
2. Siga las instrucciones para probar una conexión de federación de rejilla en "Gestionar conexiones de federación de grid" para confirmar que se ha solucionado el problema.
3. Desde la cuadrícula de origen del inquilino, seleccione **TENANTS**.
4. Localice la cuenta de inquilino que no se pudo clonar.
5. Seleccione el nombre del arrendatario para mostrar la página de detalles.
6. Seleccione **Reintentar clon de cuenta**.



Si se ha resuelto el error, la cuenta de inquilino se clonará ahora en la otra cuadrícula.

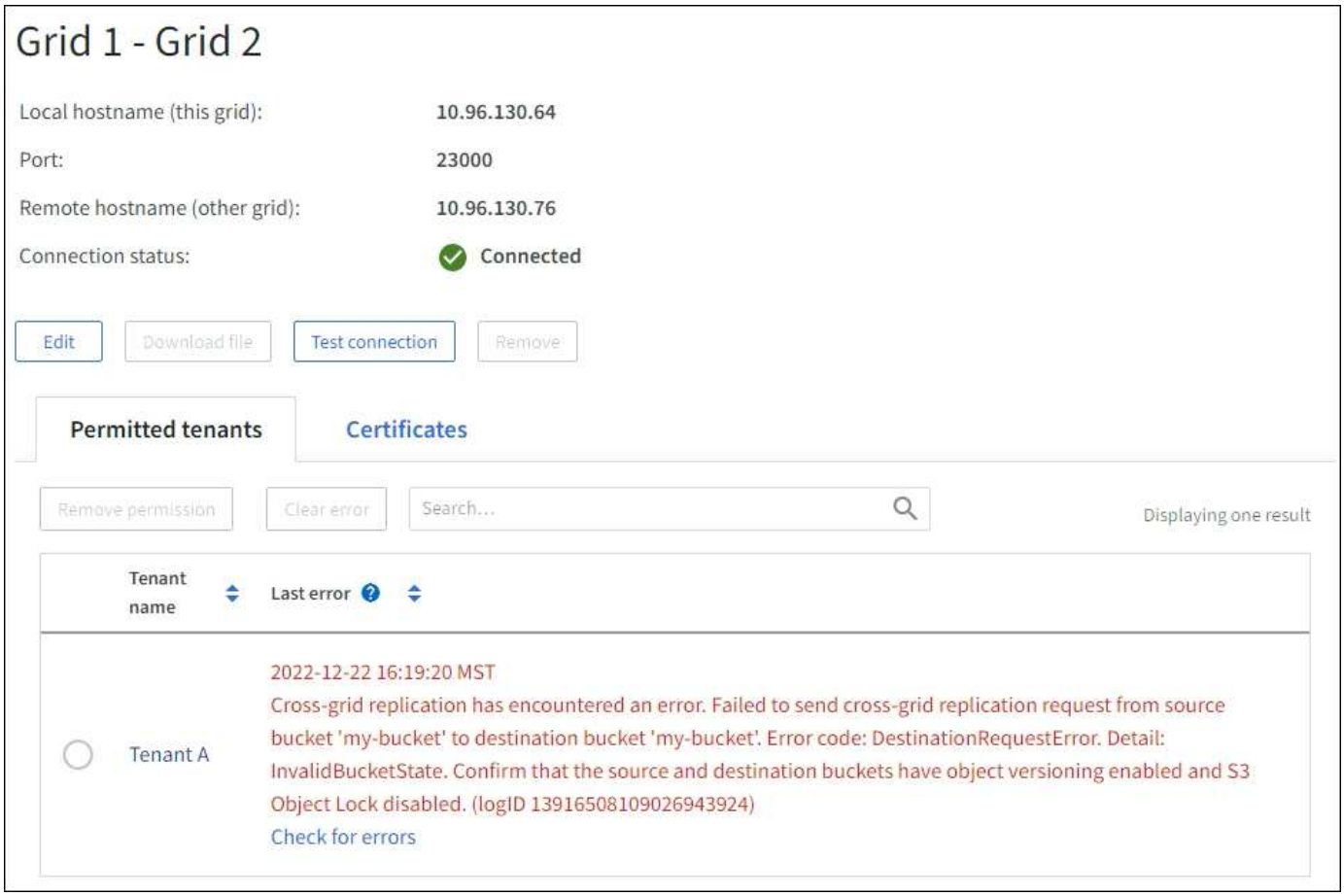
Alertas y errores de replicación entre grid

Último error mostrado para conexión o arrendatario

Problema

Cuando "visualización de una conexión de federación de grid" (o cuando "gestión de los inquilinos permitidos"

Para una conexión), usted nota un error en la columna **Último error** en la página de detalles de la conexión. Por ejemplo:



Detalles

Para cada conexión de federación de grid, la columna **last error** muestra el error más reciente que se producirá, si lo hubiera, cuando los datos de un inquilino se estaban replicando en la otra cuadrícula. Esta columna solo muestra el último error de replicación entre cuadrículas que se produce; no se mostrarán los errores anteriores que podrían haberse producido.
Un error en esta columna puede ocurrir por uno de estos motivos:

- No se ha encontrado la versión del objeto de origen.
- No se ha encontrado el depósito de origen.
- Se ha suprimido el depósito de destino.
- Una cuenta diferente ha vuelto a crear el bloque de destino.
- Se ha suspendido el control de versiones del bloque de destino.
- La misma cuenta ha vuelto a crear el depósito de destino, pero ahora no tiene versiones.

Acciones recomendadas

Si aparece un mensaje de error en la columna **Último error**, siga estos pasos:

1. Revise el texto del mensaje.
2. Realice las acciones recomendadas. Por ejemplo, si se suspendió el control de versiones en el bloque de destino para la replicación entre grid, vuelva a habilitar el control de versiones para ese bloque.

3. Seleccione la conexión o la cuenta de inquilino de la tabla.
4. Seleccione **Borrar error**.
5. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
6. Espere 5-6 minutos e incorpore un objeto nuevo en el bloque. Confirme que el mensaje de error no vuelve a aparecer.

> Para asegurarse de que el mensaje de error se borra, espere al menos 5 minutos después de la marca de tiempo del mensaje antes de introducir un nuevo objeto.

> Después de borrar el error, puede aparecer un nuevo **last error** si los objetos se ingieren en un depósito diferente que también tiene un error.

7. Para determinar si se ha producido un error en la replicación de algún objeto debido al error de depósito, consulte "Identifique y vuelva a intentar operaciones de replicación fallidas".

Alerta de error permanente de replicación entre grid

Problema

Se activó la alerta de error permanente de replicación cruzada de la red*.

Detalles

Esta alerta indica que los objetos de arrendatario no se pueden replicar entre los buckets de dos cuadrículas por un motivo que requiere la intervención del usuario para resolverlos. Esta alerta suele deberse a un cambio en el depósito de origen o de destino.

Acciones recomendadas

1. Inicie sesión en la cuadrícula donde se activó la alerta.
2. Vaya a **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula** y localice el nombre de la conexión que aparece en la alerta.
3. En la pestaña de inquilinos permitidos, mire la columna **Último error** para determinar qué cuentas de inquilino tienen errores.
4. Para obtener más información sobre el fallo, consulte las instrucciones en "Supervisar las conexiones de federación de grid" para revisar las métricas de replicación entre cuadrículas.
5. Para cada cuenta de inquilino afectada:
   a. Consulte las instrucciones en "Supervise la actividad de los inquilinos" para confirmar que el inquilino no ha superado su cuota en la cuadrícula de destino para la replicación entre grid.
   b. Según sea necesario, aumente la cuota del inquilino en la cuadrícula de destino para permitir guardar nuevos objetos.
6. Para cada inquilino afectado, inicie sesión en el Gestor de inquilinos en ambas cuadrículas, de modo que pueda comparar la lista de bloques.
7. Para cada bloque que tiene habilitada la replicación entre grid, confirme lo siguiente:
   - Hay un depósito correspondiente para el mismo inquilino en la otra cuadrícula (debe usar el nombre exacto).
   - Ambos cubos tienen activado el control de versiones de objetos (el control de versiones no se puede suspender en ninguna cuadrícula).
   - Ambos cubos tienen S3 Object Lock desactivado.

- Ninguno de los depósitos está en el estado **Deleting objects: Read-only**.

8. Para confirmar que el problema se ha resuelto, consulte las instrucciones de "Supervisar las conexiones de federación de grid" para revisar las métricas de replicación entre cuadrículas, o realice los siguientes pasos:

   a. Vuelva a la página Grid federation.
   b. Seleccione el inquilino afectado y seleccione **Borrar error** en la columna **Último error**.
   c. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
   d. Espere 5-6 minutos e incorpore un objeto nuevo en el bloque. Confirme que el mensaje de error no vuelve a aparecer.

   > Para asegurarse de que el mensaje de error se borra, espere al menos 5 minutos después de la marca de tiempo del mensaje antes de introducir un nuevo objeto.

   > Puede que la alerta tarde hasta un día en borrarse una vez que se resuelve.

   a. Vaya a. "Identifique y vuelva a intentar operaciones de replicación fallidas" para identificar objetos o eliminar marcadores que no se han podido replicar en la otra cuadrícula y volver a intentar la replicación según sea necesario.

Alerta no disponible del recurso de replicación entre grid

Problema

Se activó la alerta **Cross-grid replication resource unavailable**.

Detalles

Esta alerta indica que las solicitudes de replicación entre grid están pendientes porque un recurso no está disponible. Por ejemplo, puede haber un error de red.

Acciones recomendadas

1. Supervise la alerta para ver si el problema se resuelve por sí solo.
2. Si el problema persiste, determine si cualquiera de las redes tiene una alerta de **Error de conexión de federación de red** para la misma conexión o una alerta de **No se puede comunicar con el nodo** para un nodo. Es posible que esta alerta se resuelva al resolver esas alertas.
3. Para obtener más información sobre el fallo, consulte las instrucciones en "Supervisar las conexiones de federación de grid" para revisar las métricas de replicación entre cuadrículas.
4. Si no puede resolver la alerta, póngase en contacto con el soporte técnico.

La replicación entre cuadrículas continuará con normalidad una vez resuelto el problema.

Identifique y vuelva a intentar operaciones de replicación fallidas

Después de resolver la alerta de error permanente * de replicación entre redes, debe determinar si algún objeto o marcador de borrado no se pudo replicar en la otra cuadrícula. A continuación, puede volver a ingerir estos objetos o utilizar la API de administración de grid para volver a intentar la replicación.

La alerta de error permanente * de replicación cruzada de la red indica que los objetos del inquilino no se pueden replicar entre los depósitos en dos cuadrículas por una razón que requiere la intervención del usuario

para resolverlos. Esta alerta suele deberse a un cambio en el depósito de origen o de destino. Para obtener más información, consulte "Solucionar errores de federación de grid".

Determine si se ha producido un fallo en la replicación de algún objeto

Para determinar si algún objeto o marcador de borrado no se ha replicado en la otra cuadrícula, puede buscar en el registro de auditoría "CGRR (Solicitud de Replicación entre Grid)" mensajes. Este mensaje se agrega al registro cuando StorageGRID no puede replicar un objeto, un objeto multiparte o un marcador de eliminación en el bloque de destino.

Puede utilizar el "herramienta audit-explain" para traducir los resultados a un formato más fácil de leer.

Antes de empezar

- Tiene permiso de acceso raíz.
- Usted tiene la `Passwords.txt` archivo.
- Conoce la dirección IP del nodo de administración principal.

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Busque en audit.log mensajes CGRR y utilice la herramienta audit-explain para dar formato a los resultados.

   Por ejemplo, este comando greps para todos los mensajes CGRR en los últimos 30 minutos y utiliza la herramienta audit-explain.

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

Los resultados del comando se parecerán a este ejemplo, que tiene entradas para seis mensajes CGRR. En el ejemplo, todas las solicitudes de replicación entre grid devolvieron un error general porque el objeto no se pudo replicar. Los tres primeros errores son para las operaciones de «objeto de réplica», y los tres últimos errores son para las operaciones de «marcador de borrado de réplica».

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

Cada entrada contiene la siguiente información:

Campo	Descripción
Solicitud de Replicación de Cuadrícula Cruzada de CGRR	Nombre de la solicitud
inquilino	El ID de cuenta del inquilino
conexión	El ID de la conexión de federación de grid
funcionamiento	Tipo de operación de replicación que se intentó: • replicar objeto • replicar marcador de borrado • replicar objeto de varias partes
cucharón	El nombre del cubo
objeto	El nombre del objeto
versión	El ID de versión del objeto

Campo	Descripción
error	Tipo de error. Si se produce un error en la replicación entre cuadrículas, el error es Error general.

Vuelva a intentar las replicaciones fallidas

Después de generar una lista de objetos y de eliminar marcadores que no se han replicado en el depósito de destino y resolver los problemas subyacentes, puede volver a intentar la replicación de una de las dos formas siguientes:

- Vuelva a ingerir cada objeto en el bloque de origen.
- Utilice la API privada de Grid Management, tal y como se describe.

Pasos

1. En la parte superior de Grid Manager, selecciona el icono de ayuda y selecciona **Documentación de API**.
2. Seleccione **Ir a documentación privada de API**.

   > Los extremos de la API de StorageGRID marcados como «privados» están sujetos a cambios sin previo aviso. Los extremos privados de StorageGRID también ignoran la versión de API de la solicitud.

3. En la sección **cross-grid-replication-advanced**, seleccione el siguiente punto final:

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. Seleccione **probar**.
5. En el cuadro de texto **body**, reemplace la entrada de ejemplo para **versionID** por un ID de versión del audit.log que corresponda a una solicitud fallida de replicación cruzada.

   Asegúrese de conservar las comillas dobles alrededor de la cadena.

6. Seleccione **Ejecutar**.
7. Confirme que el código de respuesta del servidor es **204**, lo que indica que el objeto o marcador de borrado se ha marcado como pendiente para la replicación de cuadrícula cruzada a la otra cuadrícula.

   > Pendiente significa que la solicitud de replicación entre grid se ha agregado a la cola interna para su procesamiento.

Supervisar reintentos de replicación

Debe supervisar las operaciones de reintento de replicación para asegurarse de que se completen.

> Puede que un objeto o marcador de eliminación tarde varias horas o más en la otra cuadrícula.

Es posible supervisar las operaciones de reintento de dos maneras:

- Utilice un S3 "Objeto principal" o. "GetObject" solicitud. La respuesta incluye los recursos específicos de StorageGRID `x-ntap-sg-cgr-replication-status` cabecera de respuesta, que tendrá uno de los siguientes valores:

Cuadrícula	Estado de replicación
Origen	• **ÉXITO**: La replicación fue exitosa. • **PENDIENTE**: El objeto aún no ha sido replicado. • **FALLO**: La replicación falló con un fallo permanente. Un usuario debe resolver el error.
Destino	**REPLICA**: El objeto fue replicado desde la cuadrícula de origen.

- Utilice la API privada de Grid Management, tal y como se describe.

Pasos

1. En la sección **cross-grid-replication-advanced** de la documentación de la API privada, seleccione el siguiente punto final:

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. Seleccione **probar**.
3. En la sección Parámetro, introduzca el ID de versión que utilizó en el `cross-grid-replication-retry-failed` solicitud.
4. Seleccione **Ejecutar**.
5. Confirme que el código de respuesta del servidor es **200**.
6. Revise el estado de replicación, que será uno de los siguientes:
   - **PENDIENTE**: El objeto aún no ha sido replicado.
   - **COMPLETADO**: La replicación fue exitosa.
   - **ERROR**: La replicación falló con un fallo permanente. Un usuario debe resolver el error.

Gestionar la seguridad

Gestionar la seguridad: Información general

Puede configurar varias opciones de seguridad desde Grid Manager para ayudar a proteger el sistema StorageGRID.

Gestione el cifrado

StorageGRID ofrece varias opciones para el cifrado de datos. Usted debe "revise los métodos de cifrado disponibles" para determinar cuáles satisfacen sus requisitos de protección de datos.

Gestionar certificados

Puede hacerlo "configurar y gestionar los certificados de servidor" Se utiliza para las conexiones HTTP o los certificados de cliente utilizados para autenticar una identidad de cliente o usuario en el servidor.

Configuración de servidores de gestión de claves

Utilizar un "servidor de gestión de claves" Le permite proteger los datos de StorageGRID incluso si se ha quitado un dispositivo del centro de datos. Una vez que se han cifrado los volúmenes del dispositivo, no podrá

acceder a ningún dato del dispositivo a menos que el nodo se pueda comunicar con el KMS.

> Para utilizar la administración de claves de cifrado, debe activar el ajuste **cifrado de nodos** para cada dispositivo durante la instalación, antes de agregar el dispositivo a la cuadrícula.

Administrar la configuración de proxy

Si utiliza servicios de plataforma S3 o pools de almacenamiento en la nube, puede configurar un "servidor proxy de almacenamiento" Entre los nodos de almacenamiento y los extremos externos de S3. Si envía paquetes AutoSupport con HTTPS o HTTP, puede configurar un "servidor proxy de administración" Entre los nodos de administración y el soporte técnico.

Controle los firewalls

Para mejorar la seguridad de su sistema, puede controlar el acceso a los nodos de administración de StorageGRID abriendo o cerrando puertos específicos en la "firewall externo". También es posible controlar el acceso de la red a cada nodo configurando su "firewall interno". Puede evitar el acceso a todos los puertos, excepto a los necesarios para la implementación.

Consulte los métodos de cifrado de StorageGRID

StorageGRID ofrece varias opciones para el cifrado de datos. Debe revisar los métodos disponibles para determinar qué métodos cumplen sus requisitos de protección de datos.

La tabla proporciona un resumen de alto nivel de los métodos de cifrado disponibles en StorageGRID.

Opción de cifrado	Cómo funciona	Se aplica a.
Servidor de gestión de claves (KMS) en Grid Manager	Usted "configurar un servidor de gestión de claves" Para el sitio de StorageGRID y. "habilite el cifrado de nodos para el dispositivo". A continuación, un nodo de dispositivo se conecta al KMS para solicitar una clave de cifrado (KEK). Esta clave cifra y descifra la clave de cifrado de datos (DEK) en cada volumen.	Nodos de dispositivo con **cifrado de nodos** activado durante la instalación. Todos los datos del dispositivo están protegidos frente a la pérdida física o la eliminación del centro de datos. **Nota**: La gestión de claves de cifrado con un KMS solo es compatible con los nodos de almacenamiento y los dispositivos de servicios.

Opción de cifrado	Cómo funciona	Se aplica a.
Página de cifrado de unidades de Installer de dispositivos de StorageGRID	Si el dispositivo contiene unidades que admiten el cifrado de hardware, puede establecer una frase de acceso de la unidad durante la instalación. Cuando se configura una clave de acceso de la unidad, es imposible que nadie recupere datos válidos de las unidades que se han eliminado del sistema, a menos que conozcan la clave de acceso. Antes de iniciar la instalación, vaya a **Configurar hardware** > **Cifrado de unidades** para establecer una frase de contraseña de la unidad que se aplique a todas las unidades de cifrado automático gestionadas por StorageGRID en un nodo.	Dispositivos que contienen unidades de autocifrado. Todos los datos de las unidades seguras están protegidos frente a la pérdida física o eliminación del centro de datos. El cifrado de unidades no se aplica a las unidades gestionadas por SANtricity. Si tiene un dispositivo de almacenamiento con unidades de cifrado automático y controladoras SANtricity, puede habilitar la seguridad de unidades en SANtricity.
Drive Security en SANtricity System Manager	Si la función Drive Security está habilitada para un dispositivo de almacenamiento SG5700 o SG6000, es posible usar "System Manager de SANtricity" para crear y gestionar la clave de seguridad. Se requiere la clave para acceder a los datos en las unidades seguras.	Los dispositivos de almacenamiento que tienen unidades de cifrado de disco completo (FDE) o unidades de autocifrado. Todos los datos de las unidades seguras están protegidos frente a la pérdida física o eliminación del centro de datos. No se puede usar con algunos dispositivos de almacenamiento ni con ningún dispositivo de servicios.
Cifrado de objetos almacenados	Puede activar el "Cifrado de objetos almacenados" En Grid Manager. Cuando se habilita, todos los objetos nuevos que no se cifren a nivel de bucket o de objeto se cifran durante la ingesta.	Datos de objetos S3 y Swift recientemente procesados. Los objetos almacenados existentes no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados.

Opción de cifrado	Cómo funciona	Se aplica a.
Cifrado de bloques de S3	Emite una solicitud PutBucketEncryption para habilitar el cifrado para el depósito. Todos los objetos nuevos que no se cifren en el nivel de objeto se cifran durante la ingesta.	Solo datos de objetos S3 procesados recientemente. Debe especificarse el cifrado para el bloque. Los objetos de cubo existentes no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados. "Operaciones en bloques"
Cifrado del lado del servidor de objetos S3 (SSE)	Se emite una solicitud de S3 para almacenar un objeto e incluir el `x-amz-server-side-encryption` solicite el encabezado.	Solo datos de objetos S3 procesados recientemente. Se debe especificar el cifrado para el objeto. Los metadatos de los objetos y otros datos confidenciales no están cifrados. StorageGRID gestiona las claves. "Usar cifrado del servidor"
Cifrado del lado del servidor de objetos S3 con claves proporcionadas por el cliente (SSE-C)	Se emite una solicitud S3 para almacenar un objeto e incluir tres encabezados de solicitud. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Solo datos de objetos S3 procesados recientemente. Se debe especificar el cifrado para el objeto. Los metadatos de los objetos y otros datos confidenciales no están cifrados. Las claves se gestionan fuera de StorageGRID. "Usar cifrado del servidor"
Cifrado de volúmenes o almacenes de datos externos	Si la plataforma de implementación lo admite, puede utilizar un método de cifrado fuera de StorageGRID para cifrar un volumen o almacén de datos completo.	Todos los datos de objetos, metadatos y datos de configuración del sistema, suponiendo que se cifre cada volumen o almacén de datos. Un método de cifrado externo proporciona un control más estricto sobre los algoritmos y claves de cifrado. Se puede combinar con los otros métodos enumerados.

Opción de cifrado	Cómo funciona	Se aplica a.
Cifrado de objetos fuera de StorageGRID	Se utiliza un método de cifrado fuera de StorageGRID para cifrar los metadatos y los datos de objetos antes de que se ingieran en StorageGRID.	Solo datos de objetos y metadatos (los datos de configuración del sistema no están cifrados). Un método de cifrado externo proporciona un control más estricto sobre los algoritmos y claves de cifrado. Se puede combinar con los otros métodos enumerados. "Amazon simple Storage Service - Guía para desarrolladores: Protección de datos mediante cifrado en el cliente"

Utilice varios métodos de cifrado

En función de los requisitos, puede utilizar más de un método de cifrado a la vez. Por ejemplo:

- Se puede usar un KMS para proteger los nodos del dispositivo y también para usar la función de seguridad de la unidad en el administrador del sistema de SANtricity para «cifrar dos veces» los datos en las unidades de autocifrado del mismo dispositivo.
- Puede utilizar un KMS para proteger los datos en los nodos del dispositivo y también utilizar la opción de cifrado de objetos almacenados para cifrar todos los objetos cuando se ingieren.

Si solo una pequeña parte de los objetos requiere cifrado, considere la posibilidad de controlar el cifrado en el nivel de bloque o de objeto individual. Habilitar varios niveles de cifrado tiene un coste de rendimiento adicional.

Gestionar certificados

Gestionar certificados de seguridad: Información general

Los certificados de seguridad son archivos de datos pequeños que se utilizan para crear conexiones seguras y de confianza entre componentes de StorageGRID y entre componentes de StorageGRID y sistemas externos.

StorageGRID utiliza dos tipos de certificados de seguridad:

- **Se requieren certificados de servidor** cuando se utilizan conexiones HTTPS. Los certificados de servidor se utilizan para establecer conexiones seguras entre clientes y servidores, autenticar la identidad de un servidor a sus clientes y proporcionar una ruta de comunicación segura para los datos. Cada servidor y el cliente tienen una copia del certificado.
- **Los certificados de cliente** autentican una identidad de cliente o usuario al servidor, proporcionando una autenticación más segura que las contraseñas solamente. Los certificados de cliente no cifran datos.

Cuando un cliente se conecta al servidor mediante HTTPS, el servidor responde con el certificado de servidor, que contiene una clave pública. El cliente verifica este certificado comparando la firma del servidor con la firma de su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión con el servidor utilizando la misma clave pública.

StorageGRID funciona como servidor para algunas conexiones (como el extremo de equilibrio de carga) o como cliente para otras conexiones (como el servicio de replicación de CloudMirror).

Certificado de CA de cuadrícula predeterminado

StorageGRID incluye una entidad de certificación (CA) integrada que genera un certificado de CA de grid interno durante la instalación del sistema. El certificado de CA de cuadrícula se utiliza, de forma predeterminada, para proteger el tráfico interno de StorageGRID. Una entidad de certificación externa (CA) puede emitir certificados personalizados que cumplan plenamente con las políticas de seguridad de la información de su empresa. Aunque se puede utilizar el certificado de CA de cuadrícula para un entorno que no sea de producción, la práctica recomendada para un entorno de producción es utilizar certificados personalizados firmados por una entidad de certificación externa. También se admiten conexiones no seguras sin certificado, pero no se recomienda.

- Los certificados de CA personalizados no eliminan los certificados internos; sin embargo, los certificados personalizados deben ser los especificados para verificar las conexiones del servidor.
- Todos los certificados personalizados deben cumplir con el "directrices de fortalecimiento del sistema para los certificados de servidor".
- StorageGRID admite la agrupación de certificados de una CA en un único archivo (conocido como paquete de certificados de CA).

> ⓘ StorageGRID también incluye certificados de CA del sistema operativo que son los mismos en todos los entornos Grid. En los entornos de producción, asegúrese de especificar un certificado personalizado firmado por una entidad de certificación externa en lugar del certificado de CA del sistema operativo.

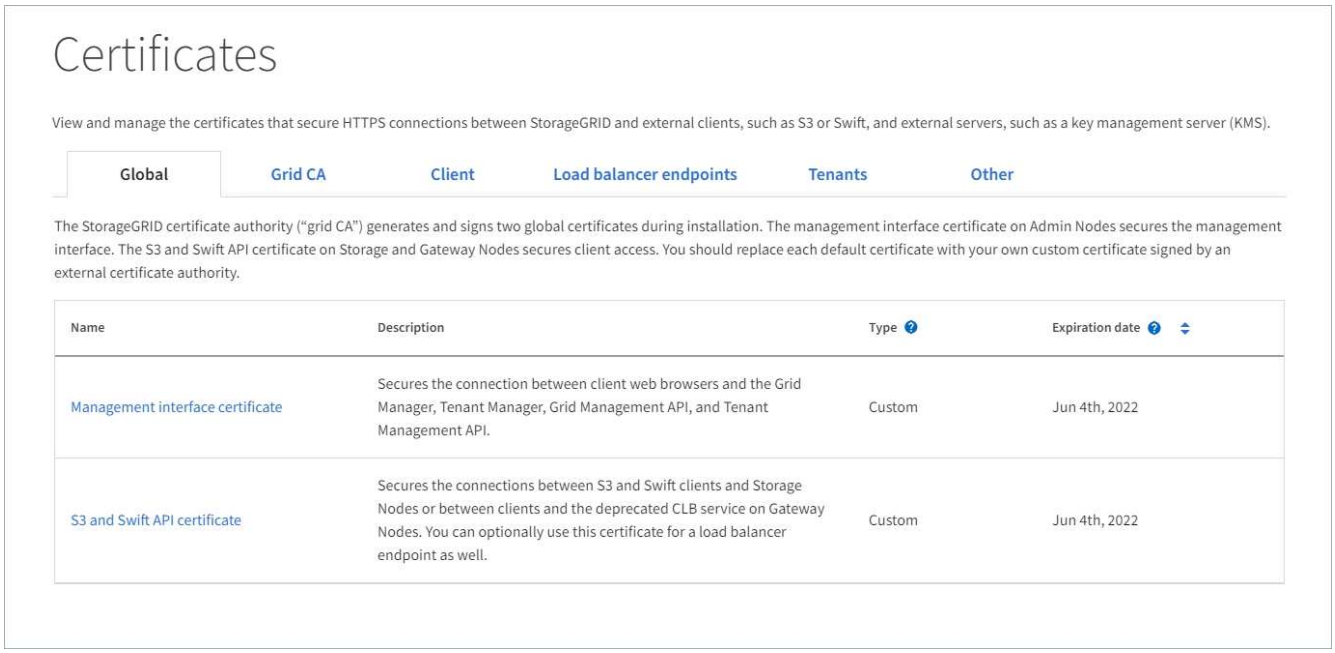
Las variantes de los tipos de certificado de servidor y cliente se implementan de varias maneras. Es necesario tener preparados todos los certificados necesarios para la configuración específica de StorageGRID antes de configurar el sistema.

Acceda a los certificados de seguridad

Puede acceder a información sobre todos los certificados de StorageGRID en una única ubicación, junto con enlaces al flujo de trabajo de configuración de cada certificado.

Pasos

1. En Grid Manager, selecciona **CONFIGURACIÓN** > **Seguridad** > **Certificados**.



2. Seleccione una ficha en la página certificados para obtener información sobre cada categoría de certificado y para acceder a la configuración de certificado. Puede acceder a una pestaña si tiene el "permiso apropiado".

   - **Global**: Protege el acceso a StorageGRID desde navegadores web y clientes API externos.
   - **Grid CA**: Protege el tráfico interno de StorageGRID.
   - **Cliente**: Protege las conexiones entre clientes externos y la base de datos Prometheus de StorageGRID.
   - **Puntos finales del equilibrador de carga**: Protege las conexiones entre los clientes S3 y Swift y el equilibrador de carga StorageGRID.
   - **Arrendatarios**: Protege las conexiones a servidores de federación de identidades o desde extremos de servicio de plataforma a recursos de almacenamiento S3.
   - **Otros**: Protege las conexiones StorageGRID que requieren certificados específicos.

   Cada una de las pestañas se describe a continuación con enlaces a detalles de certificados adicionales.

Global

Los certificados globales protegen el acceso a StorageGRID desde exploradores web y clientes de API de S3 y Swift externos. La autoridad de certificados StorageGRID genera inicialmente dos certificados globales durante la instalación. La práctica recomendada para un entorno de producción es usar certificados personalizados firmados por una entidad de certificación externa.

- Certificado de interfaz de gestión: Protege las conexiones del explorador Web cliente a las interfaces de administración de StorageGRID.
- Certificado API S3 y Swift: Protege las conexiones API de cliente a los nodos de almacenamiento, los nodos de administración y los nodos de puerta de enlace, que las aplicaciones de cliente S3 y Swift utilizan para cargar y descargar datos de objetos.

Entre la información sobre los certificados globales instalados se incluyen:

- **Nombre**: Nombre del certificado con enlace a la administración del certificado.
- **Descripción**
- **Tipo**: Personalizado o predeterminado.
  Siempre debe utilizar un certificado personalizado para mejorar la seguridad de grid.
- **Fecha de vencimiento**: Si se utiliza el certificado predeterminado, no se muestra ninguna fecha de vencimiento.

Podrá:

- Sustituya los certificados predeterminados por certificados personalizados firmados por una autoridad de certificado externa para mejorar la seguridad de la cuadrícula:
  - "Reemplace el certificado de interfaz de gestión generado por StorageGRID predeterminado" Se utiliza para las conexiones del administrador de grid y del administrador de inquilinos.
  - "Reemplace el certificado API de S3 y Swift" Se utiliza para las conexiones de extremo del balanceador de carga y del nodo de almacenamiento (opcional).
- "Restaure el certificado de interfaz de gestión predeterminado."
- "Restaure el certificado API S3 y Swift predeterminado."
- "Use un script para generar un nuevo certificado de interfaz de gestión autofirmado."
- Copie o descargue el "certificado de interfaz de gestión" o. "Certificado API S3 y Swift".

CA de grid

La Certificado de CA de grid, Generado por la autoridad de certificación StorageGRID durante la instalación de StorageGRID, protege todo el tráfico interno de StorageGRID.

La información del certificado incluye la fecha de caducidad del certificado y el contenido del mismo.

Puede hacerlo "Copie o descargue el certificado de Grid CA", pero no se puede cambiar.

Cliente

Certificados de cliente, Generada por una autoridad de certificados externa, asegura las conexiones entre herramientas de supervisión externas y la base de datos Prometheus de StorageGRID.

La tabla de certificados tiene una fila para cada certificado de cliente configurado e indica si el certificado se puede utilizar para el acceso a la base de datos Prometheus, junto con la fecha de caducidad del certificado.

Podrá:

- "Cargar o generar un nuevo certificado de cliente."
- Seleccione un nombre de certificado para mostrar los detalles del certificado, donde podrá:
  - "Cambie el nombre del certificado de cliente."
  - "Establezca el permiso de acceso Prometheus."
  - "Cargue y reemplace el certificado de cliente."
  - "Copie o descargue el certificado de cliente."
  - "Quite el certificado de cliente."
- Seleccione **acciones** para hacerlo rápidamente "editar", "asociar", o. "quitar" un certificado de cliente. Puede seleccionar hasta 10 certificados de cliente y eliminarlos a la vez utilizando **acciones** > **Quitar**.

Puntos finales del equilibrador de carga

Certificados de punto final de equilibrador de carga Proteja las conexiones entre los clientes S3 y Swift y el servicio de equilibrador de carga de StorageGRID en los nodos de pasarela y los nodos de administración.

La tabla de extremo de equilibrador de carga tiene una fila para cada extremo de equilibrador de carga configurado e indica si se está utilizando el certificado API global S3 y Swift o un certificado de extremo de equilibrador de carga personalizado para el extremo. También se muestra la fecha de caducidad de cada certificado.

> Los cambios en el certificado de extremo pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Podrá:

- "Ver un punto final de equilibrio de carga", incluyendo sus detalles de certificado.
- "Especifique un certificado de extremo de equilibrio de carga para FabricPool."
- "Use el certificado global de la API de S3 y Swift" en lugar de generar un nuevo certificado de extremo de equilibrio de carga.

Clientes

Los inquilinos pueden usar certificados de servidor de federación de identidades o. certificados de extremo de servicio de plataforma Para asegurar sus conexiones con StorageGRID.

La tabla de arrendatarios tiene una fila para cada arrendatario e indica si cada arrendatario tiene permiso para utilizar su propio origen de identidad o servicios de plataforma.

Podrá:

- "Seleccione un nombre de inquilino para iniciar sesión en el Administrador de inquilinos"
- "Seleccione un nombre de inquilino para ver los detalles de la federación de identidades del inquilino"
- "Seleccione el nombre de un inquilino para ver los detalles de los servicios de la plataforma de inquilino"
- "Especifique un certificado de extremo de servicio de plataforma durante la creación del extremo"

Otros

StorageGRID utiliza otros certificados de seguridad con fines específicos. Estos certificados se enumeran por su nombre funcional. Otros certificados de seguridad incluyen:

- Certificados de Cloud Storage Pool
- Certificados de notificación de alertas por correo electrónico
- Certificados de servidor de syslog externos
- Certificados de conexión de federación de grid
- Certificados de federación de identidades
- Certificados de servidor de gestión de claves (KMS)
- Certificados de inicio de sesión único

La información indica el tipo de certificado que una función utiliza y sus fechas de vencimiento del certificado de servidor y cliente, según corresponda. Al seleccionar un nombre de función, se abre una pestaña del navegador en la que puede ver y editar los detalles del certificado.

> Solo puede ver y acceder a la información de otros certificados si tiene el "permiso apropiado".

Podrá:

- "Especifique un certificado de Cloud Storage Pool para S3, C2S S3 o Azure"
- "Especifique un certificado para notificaciones de alertas por correo electrónico"
- "Use un certificado para un servidor de syslog externo"
- "Rotar certificados de conexión de federación de cuadrícula"
- "Ver y editar un certificado de federación de identidades"
- "Cargar certificados de servidor de gestión de claves (KMS) y de cliente"
- "Especifique manualmente un certificado SSO para una confianza de parte de confianza"

Detalles del certificado de seguridad

Cada tipo de certificado de seguridad se describe a continuación, con enlaces a las instrucciones de implementación.

Certificado de interfaz de gestión

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los exploradores web del cliente y la interfaz de gestión de StorageGRID, lo que permite a los usuarios acceder a Grid Manager y al Gestor de inquilinos sin advertencias de seguridad. Este certificado también autentica las conexiones API de gestión de grid y API de gestión de inquilinos. Puede usar el certificado predeterminado creado durante la instalación o cargar un certificado personalizado.	**CONFIGURACIÓN** > **Seguridad** > **certificados**, seleccione la ficha **Global** y, a continuación, seleccione **Certificado de interfaz de administración**	"Configure los certificados de interfaz de gestión"

Certificado API S3 y Swift

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica conexiones de cliente S3 o Swift seguras a un nodo de almacenamiento y a extremos de balanceador de carga (opcional).	**CONFIGURATION** > **Security** > **Certificates**, seleccione la ficha **Global** y, a continuación, seleccione **S3 y Swift API Certificate**	"Configure los certificados API S3 y Swift"

Certificado de CA de grid

Consulte Descripción de certificado de CA de cuadrícula predeterminada.

Certificado de cliente de administrador

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Cliente	Instalado en cada cliente, lo que permite que StorageGRID autentique el acceso de los clientes externos. • Permite a los clientes externos autorizados acceder a la base de datos Prometheus de StorageGRID. • Permite una supervisión segura de StorageGRID mediante herramientas externas.	**CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**	"Configurar certificados de cliente"

Certificado de punto final de equilibrador de carga

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre clientes S3 o Swift y el servicio StorageGRID Load Balancer en nodos de puerta de enlace y nodos de administrador. Puede cargar o generar un certificado de equilibrador de carga al configurar un extremo de equilibrador de carga. Las aplicaciones cliente utilizan el certificado de equilibrador de carga al conectarse a StorageGRID para guardar y recuperar datos de objeto. También puede utilizar una versión personalizada del global Certificado API S3 y Swift Certificado para autenticar conexiones al servicio Load Balancer. Si el certificado global se utiliza para autenticar las conexiones del equilibrador de carga, no es necesario cargar ni generar un certificado independiente para cada punto final del equilibrador de carga. **Nota:** el certificado utilizado para la autenticación del equilibrador de carga es el certificado más utilizado durante el funcionamiento normal de StorageGRID.	**CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**	• "Configurar puntos finales del equilibrador de carga" • "Cree un extremo de equilibrador de carga para FabricPool"

Certificado de extremo de Cloud Storage Pool

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión de un pool de almacenamiento en cloud de StorageGRID a una ubicación de almacenamiento externa, como S3 Glacier o el almacenamiento blob de Microsoft Azure. Se necesita un certificado diferente para cada tipo de proveedor de cloud.	**ILM** > **piscinas de almacenamiento**	"Cree un pool de almacenamiento en el cloud"

Certificado de notificación de alertas por correo electrónico

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica la conexión entre un servidor de correo electrónico SMTP y una StorageGRID que se usa para notificaciones de alerta. • Si las comunicaciones con el servidor SMTP requieren Transport Layer Security (TLS), debe especificar el certificado de CA del servidor de correo electrónico. • Especifique un certificado de cliente solo si el servidor de correo SMTP requiere certificados de cliente para la autenticación.	**ALERTAS** > **Configuración de correo electrónico**	"Configure notificaciones por correo electrónico para las alertas"

Certificado de servidor de syslog externo

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión TLS o RELP/TLS entre un servidor syslog externo que registra eventos en StorageGRID. **Nota:** no se requiere un certificado de servidor syslog externo para conexiones TCP, RELP/TCP y UDP a un servidor syslog externo.	**CONFIGURACIÓN** > **Monitoreo** > **Servidor de auditoría y syslog**	"Use un servidor de syslog externo"

Certificado de conexión de la federación de cuadrícula

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autenticar y cifrar la información enviada entre el sistema de StorageGRID actual y otro grid en una conexión de federación de grid.	**CONFIGURACIÓN** > **Sistema** > **Grid federation**	• "Crear conexiones de federación de grid" • "Rotar certificados de conexión"

Certificado de federación de identidades

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre StorageGRID y un proveedor de identidades externo, como Active Directory, OpenLDAP u Oracle Directory Server. Se utiliza para la federación de identidades, lo que permite que los grupos de administración y los usuarios sean gestionados por un sistema externo.	**CONFIGURACIÓN** > **Control de acceso** > **federación de identidades**	"Usar la federación de identidades"

Certificado de servidor de gestión de claves (KMS)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica la conexión entre StorageGRID y un servidor de gestión de claves (KMS) externo, que proporciona claves de cifrado a los nodos de los dispositivos StorageGRID.	**CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**	"Añadir servidor de gestión de claves (KMS)"

Certificado de extremo de servicios de plataforma

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión desde el servicio de plataforma StorageGRID a un recurso de almacenamiento S3.	**Administrador de inquilinos** > **ALMACENAMIENTO (S3)** > **terminales de servicios de plataforma**	"Cree un extremo de servicios de plataforma" "Editar extremo de servicios de plataforma"

Certificado de inicio de sesión único (SSO)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los servicios de federación de identidades, como Active Directory Federation Services (AD FS), y StorageGRID, que se utilizan para solicitudes de inicio de sesión único (SSO).	**CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**	"Configurar el inicio de sesión único"

Ejemplos de certificados

Ejemplo 1: Servicio de equilibrador de carga

En este ejemplo, StorageGRID actúa como servidor.

1. Se configura un extremo de equilibrador de carga y se carga o genera un certificado de servidor en StorageGRID.
2. Debe configurar una conexión de cliente S3 o Swift al extremo de equilibrio de carga y cargar el mismo certificado en el cliente.
3. Cuando el cliente desea guardar o recuperar datos, se conecta al extremo de equilibrio de carga mediante

HTTPS.

4. StorageGRID responde con el certificado de servidor, que contiene una clave pública y una firma basada en la clave privada.
5. El cliente verifica este certificado comparando la firma del servidor con la firma de su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión utilizando la misma clave pública.
6. El cliente envía datos de objeto a StorageGRID.

Ejemplo 2: Servidor de gestión de claves externo (KMS)

En este ejemplo, StorageGRID actúa como cliente.

1. Con el software de servidor de gestión de claves externo, configura StorageGRID como un cliente KMS y obtiene un certificado de servidor firmado por CA, un certificado de cliente público y la clave privada del certificado de cliente.
2. Con el Administrador de grid, configura un servidor KMS y carga los certificados de servidor y cliente y la clave privada de cliente.
3. Cuando un nodo StorageGRID necesita una clave de cifrado, realiza una solicitud al servidor KMS que incluye datos del certificado y una firma basada en la clave privada.
4. El servidor KMS valida la firma del certificado y decide que puede confiar en StorageGRID.
5. El servidor KMS responde mediante la conexión validada.

Configurar certificados de servidor

Tipos de certificado de servidor admitidos

El sistema StorageGRID admite certificados personalizados cifrados con RSA o ECDSA (algoritmo de firma digital de curva elíptica).

> El tipo de cifrado de la política de seguridad debe coincidir con el tipo de certificado del servidor. Por ejemplo, los cifrados RSA requieren certificados RSA y los cifrados ECDSA requieren certificados ECDSA. Consulte "Gestionar certificados de seguridad". Si configura una política de seguridad personalizada que no sea compatible con el certificado del servidor, puede hacerlo "vuelva temporalmente a la política de seguridad predeterminada".

Para obtener más información sobre cómo StorageGRID protege las conexiones de cliente, consulte "Seguridad para los clientes S3 y Swift".

Configure los certificados de interfaz de gestión

Puede reemplazar el certificado de interfaz de gestión predeterminado por un único certificado personalizado que permite a los usuarios acceder a Grid Manager y al Gestor de inquilinos sin tener que encontrar advertencias de seguridad. También puede revertir al certificado de interfaz de gestión predeterminado o generar una nueva.

Acerca de esta tarea

De manera predeterminada, cada nodo del administrador se envía un certificado firmado por la CA de grid. Estos certificados firmados por CA pueden sustituirse por una sola clave privada correspondiente y un certificado de interfaz de gestión personalizado común.

Dado que se utiliza un único certificado de interfaz de gestión personalizado para todos los nodos de administración, debe especificar el certificado como un comodín o certificado de varios dominios si los clientes necesitan verificar el nombre de host al conectarse a Grid Manager y al Gestor de inquilinos. Defina el certificado personalizado de modo que coincida con todos los nodos de administrador de la cuadrícula.

Debe completar la configuración en el servidor y, en función de la entidad emisora de certificados raíz (CA) que esté utilizando, los usuarios también pueden necesitar instalar el certificado de la CA de cuadrícula en el explorador Web que utilizarán para acceder a Grid Manager y al gestor de inquilinos.

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 este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo caduca el certificado actual seleccionando **CONFIGURACIÓN** > **Seguridad** > **certificados** y mirando la fecha de caducidad del certificado de interfaz de administración en la ficha Global.

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.
- Usted revertir de un certificado de interfaz de gestión personalizado al certificado de servidor predeterminado.

Añada un certificado de interfaz de gestión personalizado

Para agregar un certificado de interfaz de gestión personalizado, puede proporcionar su propio certificado o generar uno mediante el Gestor de cuadrícula.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**.
2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **utilizar certificado personalizado**.
4. Cargue o genere el certificado.

Cargue el certificado

Cargue los archivos de certificado de servidor requeridos.

a. Seleccione **cargar certificado**.

b. Cargue los archivos de certificado de servidor requeridos:

- **Certificado de servidor**: El archivo de certificado de servidor personalizado (codificado con PEM).
- **Clave privada de certificado**: Archivo de clave privada de certificado de servidor personalizado (`.key`).

> Las claves privadas EC deben ser de 224 bits o más. Las claves privadas RSA deben ser de 2048 bits o más.

- **Paquete CA**: Un único archivo opcional que contiene los certificados de cada entidad emisora de certificados intermedia (CA). 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.

c. Expanda **Detalles del certificado** para ver los metadatos de cada certificado que haya cargado. Si cargó un paquete de CA opcional, cada certificado aparece en su propia pestaña.

- Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

  Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

d. Seleccione **Guardar**.
El certificado de interfaz de gestión personalizado se utiliza para todas las conexiones nuevas subsiguientes a Grid Manager, Tenant Manager, Grid Manager API o la API de Tenant Manager.

Generar certificado

Genere los archivos de certificado de servidor.

> La práctica recomendada para un entorno de producción es usar un certificado de interfaz de gestión personalizado firmado por una entidad de certificación externa.

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o varios nombres de dominio completos que se deben incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.

Campo	Descripción
IP	Una o más direcciones IP que se incluirán en el certificado.
Asunto (opcional)	X,509 Asunto o nombre distinguido (DN) del propietario del certificado. Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la dirección IP como nombre común del asunto (CN).
Días válidos	Núm. De días después de la creación que caduca el certificado.
Agregue extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de claves y uso de claves ampliado se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. **Nota**: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyen estas extensiones.

c. Seleccione **generar**.

d. Seleccione **Detalles del certificado** para ver los metadatos del certificado generado.

   - Seleccione **Descargar certificado** para guardar el archivo de certificado.

     Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

e. Seleccione **Guardar**.
El certificado de interfaz de gestión personalizado se utiliza para todas las conexiones nuevas subsiguientes a Grid Manager, Tenant Manager, Grid Manager API o la API de Tenant Manager.

5. Actualice la página para garantizar que se actualice el explorador web.

> Tras cargar o generar un nuevo certificado, permita que se borren las alertas de caducidad de los certificados relacionados.

6. Después de añadir un certificado de interfaz de gestión personalizado, la página de certificado de interfaz de gestión muestra información detallada sobre certificados que están en uso.
Puede descargar o copiar el certificado PEM según sea necesario.

Restaure el certificado de interfaz de gestión predeterminado

Puede volver a utilizar el certificado de interfaz de gestión predeterminado para las conexiones de Grid Manager y de arrendatario Manager.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**.
2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **utilizar certificado predeterminado**.

   Cuando restaura el certificado de interfaz de gestión predeterminado, los archivos de certificado del servidor personalizados que configuró se eliminan y no pueden recuperarse del sistema. El certificado de la interfaz de gestión predeterminado se utiliza para todas las conexiones de clientes nuevas subsiguientes.

4. Actualice la página para garantizar que se actualice el explorador web.

Use un script para generar un nuevo certificado de interfaz de gestión autofirmado

Si se requiere una validación estricta del nombre de host, puede usar un script para generar el certificado de la interfaz de gestión.

Antes de empezar

- Ya tienes "permisos de acceso específicos".
- Usted tiene la `Passwords.txt` archivo.

Acerca de esta tarea

La práctica recomendada para un entorno de producción es usar un certificado firmado por una entidad de certificación externa.

Pasos

1. Obtenga el nombre de dominio completo (FQDN) de cada nodo de administrador.
2. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

3. Configure StorageGRID con un certificado autofirmado nuevo.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Para `--domains`, Utilice comodines para representar los nombres de dominio completos de todos los nodos Admin. Por ejemplo: `*.ui.storagegrid.example.com` utiliza el comodín * que se va a representar `admin1.ui.storagegrid.example.com` y.. `admin2.ui.storagegrid.example.com`.

- Configurado `--type` para `management` Para configurar el certificado de la interfaz de gestión, que utiliza el administrador de grid y el administrador de inquilinos.
- De forma predeterminada, los certificados generados son válidos durante un año (365 días) y deben volver a crearse antes de que expiren. Puede utilizar el `--days` argumento para anular el período de validez predeterminado.

> El período de validez de un certificado comienza cuando `make-certificate` se ejecuta. Debe asegurarse de que el cliente de gestión esté sincronizado con el mismo origen de hora que StorageGRID; de lo contrario, el cliente podría rechazar el certificado.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

El resultado contiene el certificado público que necesita el cliente API de gestión.

4. Seleccione y copie el certificado.

   Incluya las etiquetas INICIAL Y FINAL en su selección.

5. Cierre la sesión del shell de comandos. `$ exit`
6. Confirme que se configuró el certificado:
   a. Acceda a Grid Manager.
   b. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**
   c. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
7. Configure el cliente de administración para que utilice el certificado público que ha copiado. Incluya las etiquetas INICIAL Y FINAL.

Descargue o copie el certificado de la interfaz de gestión

Puede guardar o copiar el contenido del certificado de la interfaz de administración para utilizarlo en otro lugar.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**.
2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione la ficha **servidor** o **paquete CA** y, a continuación, descargue o copie el certificado.

Descargue el archivo de certificado o el paquete de CA

Descargue el certificado o el paquete de CA `.pem` archivo. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Descargar certificado** o **Descargar paquete de CA**.

   Si está descargando un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se descargan como un solo archivo.

b. Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Copie el certificado o el paquete de CA PEM

Copie el texto del certificado que se va a pegar en otro lugar. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM**.

   Si va a copiar un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se copian al mismo tiempo.

b. Pegue el certificado copiado en un editor de texto.

c. Guarde el archivo de texto con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Configure los certificados API S3 y Swift

Es posible reemplazar o restaurar el certificado de servidor que se utiliza para las conexiones de cliente S3 o Swift a los nodos de almacenamiento o a los extremos del balanceador de carga. El certificado de servidor personalizado de reemplazo es específico de su organización.

Acerca de esta tarea

De forma predeterminada, cada nodo de almacenamiento recibe un certificado de servidor X.509 firmado por la CA de grid. Estos certificados firmados por CA pueden sustituirse por un solo certificado de servidor personalizado común y una clave privada correspondiente.

Un único certificado de servidor personalizado se usa para todos los nodos de almacenamiento, por lo que debe especificar el certificado como comodín o certificado de varios dominios si los clientes necesitan verificar el nombre de host al conectarse al extremo de almacenamiento. Defina el certificado personalizado de forma que coincida con todos los nodos de almacenamiento de la cuadrícula.

Después de completar la configuración en el servidor, es posible que también necesite instalar el certificado de CA de grid en el cliente API S3 o Swift que usará para acceder al sistema, según la entidad de certificación (CA) raíz que use.

Para garantizar que las operaciones no se interrumpan por un certificado de servidor fallido, la alerta **Expiración del certificado de servidor global para S3 y Swift API** se activa cuando el certificado del servidor raíz está a punto de expirar. Según sea necesario, puede ver cuándo caduca el certificado actual seleccionando **CONFIGURACIÓN** > **Seguridad** > **certificados** y mirando la fecha de caducidad del certificado API S3 y Swift en la ficha Global.

Puede cargar o generar un certificado API personalizado de S3 y Swift.

Añada un certificado API de S3 y Swift personalizado

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**.
2. En la ficha **Global**, seleccione **S3 y Swift API Certificate**.
3. Seleccione **utilizar certificado personalizado**.
4. Cargue o genere el certificado.

Cargue el certificado

Cargue los archivos de certificado de servidor requeridos.

a. Seleccione **cargar certificado**.
b. Cargue los archivos de certificado de servidor requeridos:
   - **Certificado de servidor**: El archivo de certificado de servidor personalizado (codificado con PEM).
   - **Clave privada de certificado**: Archivo de clave privada de certificado de servidor personalizado (`.key`).

     > Las claves privadas EC deben ser de 224 bits o más. Las claves privadas RSA deben ser de 2048 bits o más.

   - **Paquete CA**: Un único archivo opcional que contiene los certificados de cada autoridad de certificación de emisión 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.
c. Seleccione los detalles del certificado para mostrar los metadatos y PEM de cada certificado API de S3 y Swift personalizado que se cargó. Si cargó un paquete de CA opcional, cada certificado aparece en su propia pestaña.
   - Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

     Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

     Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
d. Seleccione **Guardar**.

   El certificado de servidor personalizado se usa para conexiones posteriores de clientes S3 y Swift.

Generar certificado

Genere los archivos de certificado de servidor.

a. Seleccione **generar certificado**.
b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o varios nombres de dominio completos que se deben incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.

Campo	Descripción
IP	Una o más direcciones IP que se incluirán en el certificado.
Asunto (opcional)	X,509 Asunto o nombre distinguido (DN) del propietario del certificado. Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la dirección IP como nombre común del asunto (CN).
Días válidos	Núm. De días después de la creación que caduca el certificado.
Agregue extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de claves y uso de claves ampliado se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. **Nota**: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyen estas extensiones.

c. Seleccione **generar**.

d. Seleccione **Detalles de certificado** para mostrar los metadatos y PEM del certificado API de S3 y Swift personalizado que se generó.

   - Seleccione **Descargar certificado** para guardar el archivo de certificado.

     Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

e. Seleccione **Guardar**.

   El certificado de servidor personalizado se usa para conexiones posteriores de clientes S3 y Swift.

5. Seleccione una pestaña para mostrar los metadatos del certificado de servidor StorageGRID predeterminado, un certificado firmado de una CA que se cargó o un certificado personalizado generado.

   Tras cargar o generar un nuevo certificado, permita que se borren las alertas de caducidad de los certificados relacionados.

6. Actualice la página para garantizar que se actualice el explorador web.
7. Después de añadir un certificado de API personalizado de S3 y Swift, la página de certificados de la API

de S3 y Swift muestra información detallada de los certificados API personalizados de S3 y Swift que está en uso.
Puede descargar o copiar el certificado PEM según sea necesario.

Restaure el certificado API S3 y Swift predeterminado

Puede revertir a utilizar el certificado de API S3 y Swift predeterminado para las conexiones de clientes S3 y Swift a los nodos de almacenamiento. Sin embargo, no puede usar el certificado de API S3 y Swift predeterminado para un extremo de balanceador de carga.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**.
2. En la ficha **Global**, seleccione **S3 y Swift API Certificate**.
3. Seleccione **utilizar certificado predeterminado**.

   Cuando restaura la versión predeterminada del certificado de API global S3 y Swift, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar del sistema. El certificado de API de S3 y Swift predeterminado se utilizará para las conexiones de cliente nuevas S3 y Swift posteriores a los nodos de almacenamiento.

4. Seleccione **Aceptar** para confirmar la advertencia y restaurar el certificado API S3 y Swift predeterminado.

   Si tiene permiso de acceso raíz y se utilizó el certificado de API Swift y S3 personalizado para conexiones de extremos de equilibrio de carga, se muestra una lista de extremos de equilibrio de carga que ya no se podrán acceder mediante el certificado API predeterminado S3 y Swift. Vaya a. "Configurar puntos finales del equilibrador de carga" para editar o eliminar los puntos finales afectados.

5. Actualice la página para garantizar que se actualice el explorador web.

Descargue o copie el certificado de la API S3 y Swift

Es posible guardar o copiar el contenido de los certificados API S3 y Swift para usarlos en otra parte.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**.
2. En la ficha **Global**, seleccione **S3 y Swift API Certificate**.
3. Seleccione la ficha **servidor** o **paquete CA** y, a continuación, descargue o copie el certificado.

Descargue el archivo de certificado o el paquete de CA

Descargue el certificado o el paquete de CA `.pem` archivo. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Descargar certificado** o **Descargar paquete de CA**.

   Si está descargando un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se descargan como un solo archivo.

b. Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Copie el certificado o el paquete de CA PEM

Copie el texto del certificado que se va a pegar en otro lugar. Si utiliza un bundle de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM**.

   Si va a copiar un bundle de CA, todos los certificados de las pestañas secundarias del bundle de CA se copian al mismo tiempo.

b. Pegue el certificado copiado en un editor de texto.

c. Guarde el archivo de texto con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Información relacionada

- "USE LA API DE REST DE S3"
- "Use la API DE REST de Swift"
- "Configure los nombres de dominio de punto final S3"

Copie el certificado de la CA de cuadrícula

StorageGRID utiliza una entidad de certificación (CA) interna para proteger el tráfico interno. Este certificado no cambia si carga sus propios certificados.

Antes de empezar

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

Acerca de esta tarea

Si se ha configurado un certificado de servidor personalizado, las aplicaciones cliente deben verificar el servidor mediante el certificado de servidor personalizado. No deben copiar el certificado de CA desde el sistema StorageGRID.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **CA** de cuadrícula.
2. En la sección **Certificado PEM**, descargue o copie el certificado.

Descargue el archivo de certificado

Descargue el certificado `.pem` archivo.

a. Seleccione **Descargar certificado**.
b. Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

PEM de certificado de copia

Copie el texto del certificado que se va a pegar en otro lugar.

a. Seleccione **Copiar certificado PEM**.
b. Pegue el certificado copiado en un editor de texto.
c. Guarde el archivo de texto con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Configure los certificados StorageGRID para FabricPool

Para los clientes S3 que realizan una validación estricta del nombre de host y no admiten la desactivación de la validación estricta del nombre de host, como los clientes ONTAP que usan FabricPool, puede generar o cargar un certificado de servidor al configurar el punto final del equilibrador de carga.

Antes de empezar

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

Acerca de esta tarea

Al crear un extremo de equilibrador de carga, se puede generar un certificado de servidor autofirmado o cargar un certificado firmado por una entidad de certificación (CA) conocida. En los entornos de producción, se debe utilizar un certificado firmado por una CA conocida. Los certificados firmados por una CA se pueden rotar de forma no disruptiva. También son más seguros porque ofrecen una mejor protección contra los ataques de tipo "hombre en el medio".

En los siguientes pasos, se ofrecen directrices generales para clientes S3 que usan FabricPool. Para obtener información más detallada y procedimientos, consulte "Configure StorageGRID para FabricPool".

Pasos

1. Opcionalmente, configure un grupo de alta disponibilidad (ha) para que lo utilice FabricPool.
2. Cree un extremo de equilibrador de carga de S3 para que se utilice FabricPool.

Cuando crea un extremo de equilibrio de carga HTTPS, se le solicita que cargue el certificado de servidor, la clave privada de certificado y el paquete de CA opcional.

3. Adjuntar StorageGRID como nivel de cloud en ONTAP.

   Especifique el puerto de extremo de equilibrio de carga y el nombre de dominio completo utilizado en el certificado de CA que ha cargado. A continuación, proporcione el certificado de CA.

   > Si una CA intermedia emitió el certificado StorageGRID, debe proporcionar el certificado de CA intermedio. Si la CA raíz emitió directamente el certificado StorageGRID, debe proporcionar el certificado de CA raíz.

Configurar certificados de cliente

Los certificados de cliente permiten a los clientes externos autorizados acceder a la base de datos Prometheus de StorageGRID, lo que proporciona una forma segura de que las herramientas externas supervisen StorageGRID.

Si necesita acceder a StorageGRID mediante una herramienta de supervisión externa, debe cargar o generar un certificado de cliente mediante el Gestor de cuadrícula y copiar la información de certificado a la herramienta externa.

Consulte "Gestionar certificados de seguridad" y.. "Configurar certificados de servidor personalizados".

> Para garantizar que las operaciones no se interrumpan por un certificado de servidor fallido, la alerta **Caducidad de certificados de cliente configurados en la página Certificados** se activa cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo caduca el certificado actual seleccionando **CONFIGURACIÓN** > **Seguridad** > **certificados** y mirando la fecha de caducidad del certificado de cliente en la ficha Cliente.

> Si usa un servidor de gestión de claves (KMS) para proteger los datos en los nodos de dispositivos especialmente configurados, consulte la información específica acerca de "Cargando un certificado de cliente KMS".

Antes de empezar

- Tiene permiso de acceso raíz.
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Para configurar un certificado de cliente:
  - Tiene la dirección IP o el nombre de dominio del nodo de administrador.
  - Si configuró el certificado de interfaz de gestión StorageGRID, tiene la CA, el certificado de cliente y la clave privada utilizadas para configurar el certificado de interfaz de gestión.
  - Para cargar su propio certificado, la clave privada del certificado está disponible en su equipo local.
  - La clave privada debe haberse guardado o registrado en el momento de su creación. Si no tiene la clave privada original, debe crear una nueva.
- Para editar un certificado de cliente:
  - Tiene la dirección IP o el nombre de dominio del nodo de administrador.
  - Para cargar su propio certificado o un nuevo certificado, la clave privada, el certificado de cliente y la CA (si se utiliza) están disponibles en su equipo local.

Añada certificados de cliente

Para agregar el certificado de cliente, use uno de estos procedimientos:

- El certificado de interfaz de gestión ya está configurado
- CERTIFICADO de cliente emitido por CA
- Certificado generado desde Grid Manager

El certificado de interfaz de gestión ya está configurado

Utilice este procedimiento para agregar un certificado de cliente si ya se ha configurado un certificado de interfaz de gestión mediante una CA proporcionada por el cliente, un certificado de cliente y una clave privada.

Pasos

1. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado.
4. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione **Permitir prometheus**.
5. Seleccione **continuar**.
6. Para el paso **Adjuntar certificados**, cargue el certificado de la interfaz de administración.
   a. Seleccione **cargar certificado**.
   b. Seleccione **Browse** y seleccione el archivo de certificado de la interfaz de administración (`.pem`).
      - Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.
      - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
   c. Seleccione **Crear** para guardar el certificado en Grid Manager.

      El nuevo certificado aparece en la ficha Cliente.
7. Configurar una herramienta de supervisión externa, Como Grafana.

CERTIFICADO de cliente emitido por CA

Utilice este procedimiento para agregar un certificado de cliente de administrador si no se ha configurado un certificado de interfaz de gestión y tiene previsto agregar un certificado de cliente para Prometheus que utilice un certificado de cliente emitido por CA y una clave privada.

Pasos

1. Siga los pasos a. "configure un certificado de interfaz de gestión".
2. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.
3. Seleccione **Agregar**.
4. Introduzca un nombre de certificado.
5. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione

Permitir prometheus.

6. Seleccione **continuar**.
7. Para el paso **Adjuntar certificados**, cargue el certificado de cliente, la clave privada y los archivos del paquete de CA:
   a. Seleccione **cargar certificado**.
   b. Seleccione **Examinar** y seleccione el certificado de cliente, la clave privada y los archivos de paquete de CA (`.pem`).
      - Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.
      - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
   c. Seleccione **Crear** para guardar el certificado en Grid Manager.

      Los nuevos certificados aparecen en la ficha Cliente.
8. Configurar una herramienta de supervisión externa, Como Grafana.

Certificado generado desde Grid Manager

Utilice este procedimiento para agregar un certificado de cliente de administrador si no se ha configurado un certificado de interfaz de gestión y planea agregar un certificado de cliente para Prometheus que utilice la función generar certificado en Grid Manager.

Pasos

1. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado.
4. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione **Permitir prometheus**.
5. Seleccione **continuar**.
6. Para el paso **Adjuntar certificados**, selecciona **Generar certificado**.
7. Especifique la información del certificado:
   - **Tema** (opcional): X,509 Sujeto o nombre distinguido (DN) del titular del certificado.
   - **Días válidos**: El número de días que el certificado generado es válido, comenzando en el momento en que se genera.
   - **Agregar extensiones de uso de claves**: Si se selecciona (predeterminado y recomendado), el uso de claves y las extensiones de uso de claves extendidas se agregan al certificado generado.

     Estas extensiones definen el propósito de la clave contenida en el certificado.

     Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.
8. Seleccione **generar**.

9. Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.

   No podrá ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copie o descargue la clave en una ubicación segura.

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.
   - Seleccione **Descargar certificado** para guardar el archivo de certificado.

     Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

     Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar clave privada** para copiar la clave privada del certificado para pegarla en otro lugar.
   - Seleccione **Descargar clave privada** para guardar la clave privada como archivo.

     Especifique el nombre del archivo de clave privada y la ubicación de descarga.

10. Seleccione **Crear** para guardar el certificado en Grid Manager.

    El nuevo certificado aparece en la ficha Cliente.

11. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Global**.
12. Seleccione **Certificado de interfaz de administración**.
13. Seleccione **utilizar certificado personalizado**.
14. Cargue los archivos certificate.pem y private_key.pem desde el detalles del certificado de cliente paso. No es necesario cargar un paquete de CA.
    a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
    b. Cargue cada archivo de certificado (`.pem`).
    c. Seleccione **Guardar** para guardar el certificado en Grid Manager.

       El nuevo certificado se muestra en la página del certificado de interfaz de gestión.

15. Configurar una herramienta de supervisión externa, Como Grafana.

Configure una herramienta de monitorización externa

Pasos

1. Configure los siguientes ajustes en su herramienta de supervisión externa, como Grafana.
   a. **Nombre**: Escriba un nombre para la conexión.

      StorageGRID no requiere esta información, pero se debe proporcionar un nombre para probar la conexión.

   b. **URL**: Introduzca el nombre de dominio o la dirección IP del nodo de administración. Especifique HTTPS y el puerto 9091.

Por ejemplo: `https://admin-node.example.com:9091`

c. Activar **Licencia de cliente TLS** y **con CA Cert**.

d. En Detalles de autenticación TLS/SSL, copie y pegue: +

- El certificado de CA de la interfaz de administración para **CA Cert**
- El certificado de cliente para **Cliente Cert**
- La clave privada de **clave de cliente**

e. **ServerName**: Introduzca el nombre de dominio del nodo Admin.

Servername debe coincidir con el nombre de dominio tal y como aparece en el certificado de la interfaz de gestión.

2. Guarde y pruebe el certificado y la clave privada que copió desde StorageGRID o un archivo local.

Ahora puede acceder a la métrica Prometheus desde StorageGRID con su herramienta de supervisión externa.

Para obtener más información sobre las métricas, consulte "Instrucciones para supervisar StorageGRID".

Editar certificados de cliente

Puede editar un certificado de cliente de administrador para cambiar su nombre, habilitar o deshabilitar el acceso a Prometheus, o cargar un nuevo certificado cuando el actual haya caducado.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.

Las fechas de caducidad de los certificados y los permisos de acceso a Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya ha caducado, aparecerá un mensaje en la tabla y se activará una alerta.

2. Seleccione el certificado que desea editar.
3. Seleccione **Editar** y, a continuación, seleccione **Editar nombre y permiso**
4. Introduzca un nombre de certificado.
5. Para acceder a las métricas de Prometheus utilizando su herramienta de monitoreo externo, seleccione **Permitir prometheus**.
6. Seleccione **continuar** para guardar el certificado en Grid Manager.

El certificado actualizado se muestra en la ficha Cliente.

Adjunte un nuevo certificado de cliente

Puede cargar un nuevo certificado cuando el actual haya caducado.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.

Las fechas de caducidad de los certificados y los permisos de acceso a Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya ha caducado, aparecerá un mensaje en la tabla y se activará

una alerta.

2. Seleccione el certificado que desea editar.
3. Seleccione **Editar** y, a continuación, seleccione una opción de edición.

Cargue el certificado

Copie el texto del certificado que se va a pegar en otro lugar.

a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.

b. Cargue el nombre de certificado de cliente (`.pem`).

   Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.

   - Seleccione **Descargar certificado** para guardar el archivo de certificado.

     Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

c. Seleccione **Crear** para guardar el certificado en Grid Manager.

   El certificado actualizado se muestra en la ficha Cliente.

Generar certificado

Genere el texto del certificado para pegarlo en otro lugar.

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

   - **Tema** (opcional): X,509 Sujeto o nombre distinguido (DN) del titular del certificado.
   - **Días válidos**: El número de días que el certificado generado es válido, comenzando en el momento en que se genera.
   - **Agregar extensiones de uso de claves**: Si se selecciona (predeterminado y recomendado), el uso de claves y las extensiones de uso de claves extendidas se agregan al certificado generado.

     Estas extensiones definen el propósito de la clave contenida en el certificado.

     Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

c. Seleccione **generar**.

d. Seleccione **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el PEM del certificado.

   No podrá ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copie o descargue la clave en una ubicación segura.

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en

otro lugar.

- Seleccione **Descargar certificado** para guardar el archivo de certificado.

  Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar clave privada** para copiar la clave privada del certificado para pegarla en otro lugar.
- Seleccione **Descargar clave privada** para guardar la clave privada como archivo.

  Especifique el nombre del archivo de clave privada y la ubicación de descarga.

e. Seleccione **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la ficha Cliente.

Descargar o copiar certificados de cliente

Puede descargar o copiar un certificado de cliente para utilizarlo en otro lugar.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.
2. Seleccione el certificado que desea copiar o descargar.
3. Descargue o copie el certificado.

Descargue el archivo de certificado

Descargue el certificado `.pem` archivo.

a. Seleccione **Descargar certificado**.
b. Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado

Copie el texto del certificado que se va a pegar en otro lugar.

a. Seleccione **Copiar certificado PEM**.
b. Pegue el certificado copiado en un editor de texto.
c. Guarde el archivo de texto con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

Quite certificados de cliente

Si ya no necesita un certificado de cliente de administrador, puede eliminarlo.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**.
2. Seleccione el certificado que desea eliminar.
3. Seleccione **Eliminar** y, a continuación, confirme.

> Para eliminar hasta 10 certificados, seleccione cada certificado que desee eliminar en la ficha Cliente y, a continuación, seleccione **acciones** > **Eliminar**.

Una vez que se elimine un certificado, los clientes que lo hayan usado deben especificar un nuevo certificado de cliente para acceder a la base de datos Prometheus de StorageGRID.

Configurar los ajustes de seguridad

Gestione la política TLS y SSH

La política de TLS y SSH determina qué protocolos y cifrados se usan para establecer conexiones TLS seguras con aplicaciones de cliente y conexiones SSH seguras a servicios StorageGRID internos.

La directiva de seguridad controla cómo TLS y SSH cifran los datos en movimiento. En general, utilice la directiva de compatibilidad moderna (predeterminada), a menos que su sistema necesite cumplir con Common Criteria o que necesite utilizar otros cifrados.

> Algunos servicios de StorageGRID no se han actualizado para utilizar los cifrados en estas políticas.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

Seleccione una política de seguridad

Pasos

1. Selecciona **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD**.

   La pestaña **Políticas TLS y SSH** muestra las políticas disponibles. La política actualmente activa se indica mediante una marca de verificación verde en el mosaico de políticas.

2. Revise los mosaicos para obtener más información sobre las políticas disponibles.

Política	Descripción
Compatibilidad moderna (predeterminado)	Use la directiva predeterminada si necesita cifrado seguro y a menos que tenga requisitos especiales. Esta política es compatible con la mayoría de los clientes TLS y SSH.
Compatibilidad con versiones anteriores	Utilice esta directiva si necesita opciones de compatibilidad adicionales para clientes antiguos. Las opciones adicionales de esta política podrían hacerlo menos seguro que la política de compatibilidad moderna.
Criterios comunes	Utilice esta política si necesita la certificación Common Criteria.
Estricta con FIPS	Utilice esta directiva si necesita la certificación Common Criteria y necesita utilizar el módulo de seguridad criptográfica 3.0.8 de NetApp para conexiones de clientes externos a puntos finales del equilibrador de carga, el administrador de inquilinos y el administrador de grid. El uso de esta política puede reducir el rendimiento. **Nota**: Después de seleccionar esta política, todos los nodos deben serlo "reiniciado de forma rodante" Para activar el módulo de seguridad criptográfica de NetApp. Utilice **Mantenimiento** > **Reiniciar rodando** para iniciar y supervisar los reinicios.
Personalizado	Cree una política personalizada si necesita aplicar sus propios cifrados.

3. Para ver detalles sobre los cifrados, protocolos y algoritmos de cada política, selecciona **Ver detalles**.
4. Para cambiar la política actual, seleccione **Usar política**.

   Aparece una marca de verificación verde junto a **Política actual** en el mosaico de políticas.

Cree una política de seguridad personalizada

Puede crear una política personalizada si necesita aplicar sus propios cifrados.

Pasos

1. Desde el mosaico de la política que es más similar a la política personalizada que desea crear, seleccione **Ver detalles**.
2. Selecciona **Copiar al portapapeles** y luego selecciona **Cancelar**.

3. En el mosaico **Política personalizada**, selecciona **Configurar y usar**.
4. Pegue el JSON que copió y realice los cambios necesarios.
5. Seleccione **Usar política**.

   Aparece una marca de verificación verde junto a **Política actual** en el mosaico Política personalizada.

6. Opcionalmente, seleccione **Editar configuración** para realizar más cambios en la nueva política personalizada.

Vuelva temporalmente a la política de seguridad predeterminada

Si ha configurado una política de seguridad personalizada, es posible que no pueda iniciar sesión en Grid Manager si la política TLS configurada es incompatible con el "certificado de servidor configurado".

Puede revertir temporalmente a la política de seguridad predeterminada.

Pasos

1. Inicie sesión en un nodo de administrador:
   a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Ejecute el siguiente comando:

   ```
   restore-default-cipher-configurations
   ```

3. Desde un explorador web, acceda a Grid Manager en el mismo nodo de administración.
4. Siga los pasos de Seleccione una política de seguridad para volver a configurar la política.

Puede configurar la seguridad de red y de objetos para cifrar objetos almacenados, para evitar ciertas solicitudes S3 y Swift, o para permitir que las conexiones de cliente a los nodos de almacenamiento utilicen HTTP en lugar de HTTPS.

Cifrado de objetos almacenados

El cifrado de objetos almacenados permite el cifrado de todos los datos de objetos tal como se ingieren a través de S3. De forma predeterminada, los objetos almacenados no se cifran, pero puede optar por cifrar objetos mediante el algoritmo de cifrado AES-128 o AES-256. Cuando se activa la configuración, todos los objetos recién ingeridos se cifran pero no se realiza ningún cambio en los objetos almacenados existentes. Si deshabilita el cifrado, los objetos cifrados actualmente permanecen cifrados, pero los objetos recién procesados no se cifran.

La configuración de cifrado de objetos almacenados se aplica solo a objetos S3 que no han sido cifrados por el cifrado a nivel de cubo o de objeto.

Para obtener más información sobre los métodos de cifrado StorageGRID, consulte "Consulte los métodos de cifrado de StorageGRID".

Impida la modificación del cliente

Impedir la modificación del cliente es una configuración en todo el sistema. Cuando se selecciona la opción **Evitar modificación de cliente**, se rechazan las siguientes solicitudes.

API REST DE S3

- Eliminar solicitudes de bloque
- Cualquier solicitud para modificar los datos de un objeto existente, los metadatos definidos por el usuario o el etiquetado de objetos S3

API REST de Swift

- Eliminar solicitudes de contenedor
- Solicitudes para modificar cualquier objeto existente. Por ejemplo, se deniegan las siguientes operaciones: Put Overwrite, Delete, Metadata Update, etc.

Active HTTP para las conexiones del nodo de almacenamiento

De forma predeterminada, las aplicaciones cliente utilizan el protocolo de red HTTPS para cualquier conexión directa a los nodos de almacenamiento. Puede habilitar HTTP opcionalmente para estas conexiones, por ejemplo, al probar una cuadrícula que no sea de producción.

Utilice HTTP para las conexiones de nodos de almacenamiento solo si los clientes S3 y Swift necesitan establecer conexiones HTTP directamente a los nodos de almacenamiento. No es necesario que utilice esta opción para clientes que solo utilizan conexiones HTTPS o para clientes que se conectan al servicio de Equilibrador de Carga (porque puede hacerlo "configure cada punto final del equilibrador de carga" Para usar HTTP o HTTPS).

Consulte "Resumen: Direcciones IP y puertos para conexiones cliente" Para saber qué puertos S3 y los clientes Swift usan al conectarse a nodos de almacenamiento mediante HTTP o HTTPS.

Seleccione las opciones

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene permiso de acceso raíz.

Pasos

1. Selecciona **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD**.
2. Seleccione la pestaña **Red y objetos**.
3. Para el cifrado de objetos almacenados, utilice la configuración **Ninguno** (predeterminada) si no desea que los objetos almacenados se cifren, o seleccione **AES-128** o **AES-256** para cifrar los objetos almacenados.
4. Opcionalmente, seleccione **Evitar modificación de cliente** si desea evitar que los clientes S3 y Swift realicen solicitudes específicas.

   Si cambia este ajuste, el nuevo ajuste tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para el rendimiento y el escalado.

5. Opcionalmente, seleccione **Activar HTTP para conexiones de nodos de almacenamiento** si los clientes se conectan directamente a nodos de almacenamiento y desea utilizar conexiones HTTP.

   Tenga cuidado al habilitar HTTP para una cuadrícula de producción porque las solicitudes se enviarán sin cifrar.

6. Seleccione **Guardar**.

Cambie la configuración de seguridad de la interfaz

La configuración de seguridad de la interfaz le permite controlar si los usuarios están desconectados si están inactivos durante más de la cantidad de tiempo especificada y si se incluye un seguimiento de pila en las respuestas de error de la API.

Antes de empezar

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

Acerca de esta tarea

La página **Configuración de seguridad** incluye la configuración **Tiempo de espera de inactividad del navegador** y **Seguimiento de pila de API de administración**.

Tiempo de espera de inactividad del explorador

Indica cuánto tiempo puede permanecer inactivo el explorador de un usuario antes de que se cierre la sesión. El valor predeterminado es 15 minutos.

El tiempo de espera de inactividad del navegador también se controla mediante lo siguiente:

- Temporizador StorageGRID independiente no configurable, que se incluye para la seguridad del sistema. El token de autenticación de cada usuario caduca 16 horas después de que el usuario inicia sesión. Cuando caduca la autenticación de un usuario, ese usuario se desconecta automáticamente, incluso si el tiempo de espera de inactividad del explorador está desactivado o no se ha alcanzado el

valor del tiempo de espera del explorador. Para renovar el token, el usuario debe volver a iniciar sesión.

- Configuración de tiempo de espera para el proveedor de identidad, asumiendo que el inicio de sesión único (SSO) está activado para StorageGRID.

  Si se activa SSO y se agota el tiempo de espera del explorador de un usuario, el usuario debe volver a introducir sus credenciales SSO para volver a acceder a StorageGRID. Consulte "Configurar el inicio de sesión único".

Seguimiento de la pila de API de gestión

Controla si se devuelve un seguimiento de pila en las respuestas de error de la API de Grid Manager y de Tenant Manager.

Esta opción está desactivada de forma predeterminada, pero es posible que desee activar esta funcionalidad para un entorno de prueba. En general, debe dejar el rastreo de pila desactivado en entornos de producción para evitar revelar detalles internos del software cuando se producen errores de API.

Pasos

1. Selecciona **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD**.
2. Seleccione la pestaña **Interfaz**.
3. Para cambiar la configuración del tiempo de espera de inactividad del navegador:
   a. Expande el acordeón.
   b. Para cambiar el período de tiempo de espera, especifique un valor entre 60 segundos y 7 días. El tiempo de espera predeterminado es de 15 minutos.
   c. Para desactivar esta función, desactive la casilla de verificación.
   d. Seleccione **Guardar**.

      La nueva configuración no afecta a los usuarios que están conectados actualmente. Los usuarios deben iniciar sesión de nuevo o actualizar sus exploradores para que la nueva configuración de tiempo de espera tenga efecto.
4. Para cambiar la configuración del seguimiento de pila de API de administración:
   a. Expande el acordeón.
   b. Active la casilla de verificación para devolver un seguimiento de pila en las respuestas de error de la API de Grid Manager y de Tenant Manager.

      Deje desactivado el rastreo de pila en entornos de producción para evitar revelar los detalles internos del software cuando se produzcan errores de API.

   c. Seleccione **Guardar**.

Configuración de servidores de gestión de claves

Configurar servidores de gestión de claves: Descripción general

Puede configurar uno o más servidores de gestión de claves externos (KMS) para proteger los datos en nodos de dispositivo especialmente configurados.

StorageGRID solo admite ciertos servidores de gestión de claves. Para obtener una lista de productos y versiones compatibles, utilice "Herramienta de matriz de interoperabilidad de NetApp (IMT)".

¿Qué es un servidor de gestión de claves (KMS)?

Un servidor de gestión de claves (KMS) es un sistema externo de terceros que proporciona claves de cifrado a los nodos de los dispositivos StorageGRID en el sitio de StorageGRID asociado mediante el protocolo de interoperabilidad de gestión de claves (KMIP).

Puede utilizar uno o varios servidores de gestión de claves para administrar las claves de cifrado de nodos para los nodos de dispositivo StorageGRID que tengan activada la configuración * cifrado de nodos* durante la instalación. El uso de servidores de gestión de claves con estos nodos de dispositivos le permite proteger los datos aunque se haya eliminado un dispositivo del centro de datos. Una vez que se han cifrado los volúmenes del dispositivo, no podrá acceder a ningún dato del dispositivo a menos que el nodo se pueda comunicar con el KMS.

StorageGRID no crea ni gestiona las claves externas que se utilizan para cifrar y descifrar los nodos del dispositivo. Si planea usar un servidor de gestión de claves externo para proteger los datos StorageGRID, debe comprender cómo configurar ese servidor y debe comprender cómo gestionar las claves de cifrado. La realización de tareas de gestión de claves supera el alcance de estas instrucciones. Si necesita ayuda, consulte la documentación del servidor de gestión de claves o póngase en contacto con el soporte técnico.

Información general de la configuración de KMS y dispositivos

Antes de poder usar un servidor de gestión de claves (KMS) para proteger los datos de StorageGRID en los nodos de los dispositivos, debe completar dos tareas de configuración: Configurar uno o más servidores KMS y habilitar el cifrado de nodos de los nodos de los dispositivos. Cuando estas dos tareas de configuración se completan, el proceso de gestión de claves se realiza de forma automática.

El diagrama de flujo muestra los pasos de alto nivel para usar un KMS para proteger los datos de StorageGRID en los nodos de los dispositivos.

El diagrama de flujo muestra la configuración de KMS y la configuración de dispositivos que se producen en paralelo; sin embargo, puede configurar los servidores de gestión de claves antes o después de habilitar el cifrado de nodos para los nodos de la aplicación nuevos, en función de sus requisitos.

Configurar el servidor de gestión de claves (KMS)

La configuración de un servidor de gestión de claves incluye los siguientes pasos de alto nivel.

Paso	Consulte
Acceda al software KMS y añada un cliente para StorageGRID a cada clúster KMS o KMS.	"Configure StorageGRID como cliente en KMS"
Obtenga la información necesaria para el cliente StorageGRID en el KMS.	"Configure StorageGRID como cliente en KMS"

Paso	Consulte
Agregue el KMS al Gestor de cuadrícula, asígnelo a un único sitio o a un grupo predeterminado de sitios, cargue los certificados necesarios y guarde la configuración de KMS.	"Añadir un servidor de gestión de claves (KMS)"

Configure el aparato

La configuración de un nodo de dispositivo para el uso de KMS incluye los siguientes pasos de alto nivel.

1. Durante la fase de configuración de hardware de la instalación del dispositivo, utilice el instalador del dispositivo StorageGRID para activar el ajuste **cifrado de nodos** del dispositivo.

> No puede habilitar la configuración **Node Encryption** después de agregar un dispositivo a la cuadrícula, y no puede usar la administración de claves externa para dispositivos que no tienen el cifrado de nodos activado.

2. Ejecute el instalador del dispositivo StorageGRID. Durante la instalación, se asigna una clave de cifrado de datos aleatoria (DEK) a cada volumen de la cabina, como se indica a continuación:
   - Los depósitos se utilizan para cifrar los datos en cada volumen. Estas claves se generan mediante el cifrado de disco de Linux Unified Key Setup (LUKS) en el SO del dispositivo y no se pueden cambiar.
   - Cada DEK individual se cifra mediante una clave de cifrado de clave maestra (KEK). El KEK inicial es una clave temporal que cifra los depósitos hasta que el dispositivo pueda conectarse al KMS.
3. Añada el nodo del dispositivo a StorageGRID.

Consulte "Habilite el cifrado del nodo" para obtener más detalles.

Proceso de cifrado de gestión de claves (se produce automáticamente)

El cifrado de gestión de claves incluye los siguientes pasos de alto nivel que se realizan automáticamente.

1. Al instalar un dispositivo con el cifrado de nodos activado en la cuadrícula, StorageGRID determina si existe una configuración KMS para el sitio que contiene el nodo nuevo.
   - Si ya se ha configurado un KMS para el sitio, el dispositivo recibe la configuración de KMS.
   - Si aún no se ha configurado un KMS para el sitio, el KEK temporal continúa encriptado los datos del dispositivo hasta que configura un KMS para el sitio y el dispositivo recibe la configuración de KMS.
2. El dispositivo usa la configuración KMS para conectarse al KMS y solicitar una clave de cifrado.
3. El KMS envía una clave de cifrado al dispositivo. La nueva clave del KMS sustituye al KEK temporal y ahora se utiliza para cifrar y descifrar los depósitos de los volúmenes del dispositivo.

> Los datos que existan antes de que el nodo del dispositivo cifrado se conecte al KMS configurado se cifran con una clave temporal. Sin embargo, los volúmenes de los dispositivos no se deben considerar protegidos de la eliminación del centro de datos hasta que la clave temporal se sustituya por la clave de cifrado KMS.

4. Si el dispositivo está encendido o reiniciado, se vuelve a conectar con el KMS para solicitar la clave. La clave, que se guarda en la memoria volátil, no puede sobrevivir a una pérdida de energía o un reinicio.

Antes de configurar un servidor de gestión de claves (KMS) externo, debe comprender las consideraciones y los requisitos.

¿Qué versión de KMIP es compatible?

StorageGRID admite la versión KMIP 1.4.

"Especificación del protocolo de interoperabilidad de gestión de claves versión 1.4"

¿Cuáles son las consideraciones de red?

La configuración del firewall de red debe permitir que cada nodo del dispositivo se comunique a través del puerto que se utiliza para las comunicaciones del protocolo de interoperabilidad de gestión de claves (KMIP). El puerto KMIP predeterminado es 5696.

Debe asegurarse de que cada nodo de dispositivo que utilice cifrado de nodo tenga acceso de red al clúster KMS o KMS configurado para el sitio.

¿Qué versiones de TLS son compatibles?

Las comunicaciones entre los nodos del dispositivo y el KMS configurado utilizan conexiones TLS seguras. StorageGRID puede admitir el protocolo TLS 1,2 o TLS 1,3 cuando realiza conexiones KMIP a un clúster KMS o KMS, según lo que admite el KMS y cuál "Política de TLS y SSH" está utilizando.

StorageGRID negocia el protocolo y el cifrado (TLS 1,2) o el conjunto de cifrado (TLS 1,3) con el KMS cuando realiza la conexión. Para ver qué versiones de protocolo y qué conjuntos de cifrado/cifrado están disponibles, consulte `tlsOutbound` Sección de la política TLS y SSH activa de la cuadrícula (**CONFIGURACIÓN** > **Seguridad Configuración de seguridad**).

¿Qué dispositivos son compatibles?

Puede usar un servidor de administración de claves (KMS) para administrar las claves de cifrado de cualquier dispositivo StorageGRID de la cuadrícula que tenga activada la configuración **cifrado de nodos**. Este ajuste solo se puede habilitar durante la fase de configuración de hardware de la instalación del dispositivo mediante el instalador de StorageGRID Appliance.

> No se puede habilitar el cifrado de nodo después de añadir un dispositivo al grid, y no se puede usar la gestión de claves externa para dispositivos que no tienen el cifrado de nodo habilitado.

Puede usar el KMS configurado para dispositivos StorageGRID y nodos de dispositivos.

No puede usar el KMS configurado para nodos basados en software (no en dispositivos), incluidos los siguientes:

- Nodos puestos en marcha como máquinas virtuales (VM)
- Nodos implementados en motores de contenedor en hosts Linux

Los nodos puestos en marcha en estas otras plataformas pueden utilizar el cifrado fuera de StorageGRID a nivel de almacén de datos o disco.

¿Cuándo se deben configurar los servidores de gestión de claves?

Para una instalación nueva, normalmente debe configurar uno o más servidores de gestión de claves en Grid Manager antes de crear inquilinos. Este orden garantiza que los nodos estén protegidos antes de que se almacenen datos de objeto en ellos.

Puede configurar los servidores de gestión de claves en Grid Manager antes o después de instalar los nodos de dispositivo.

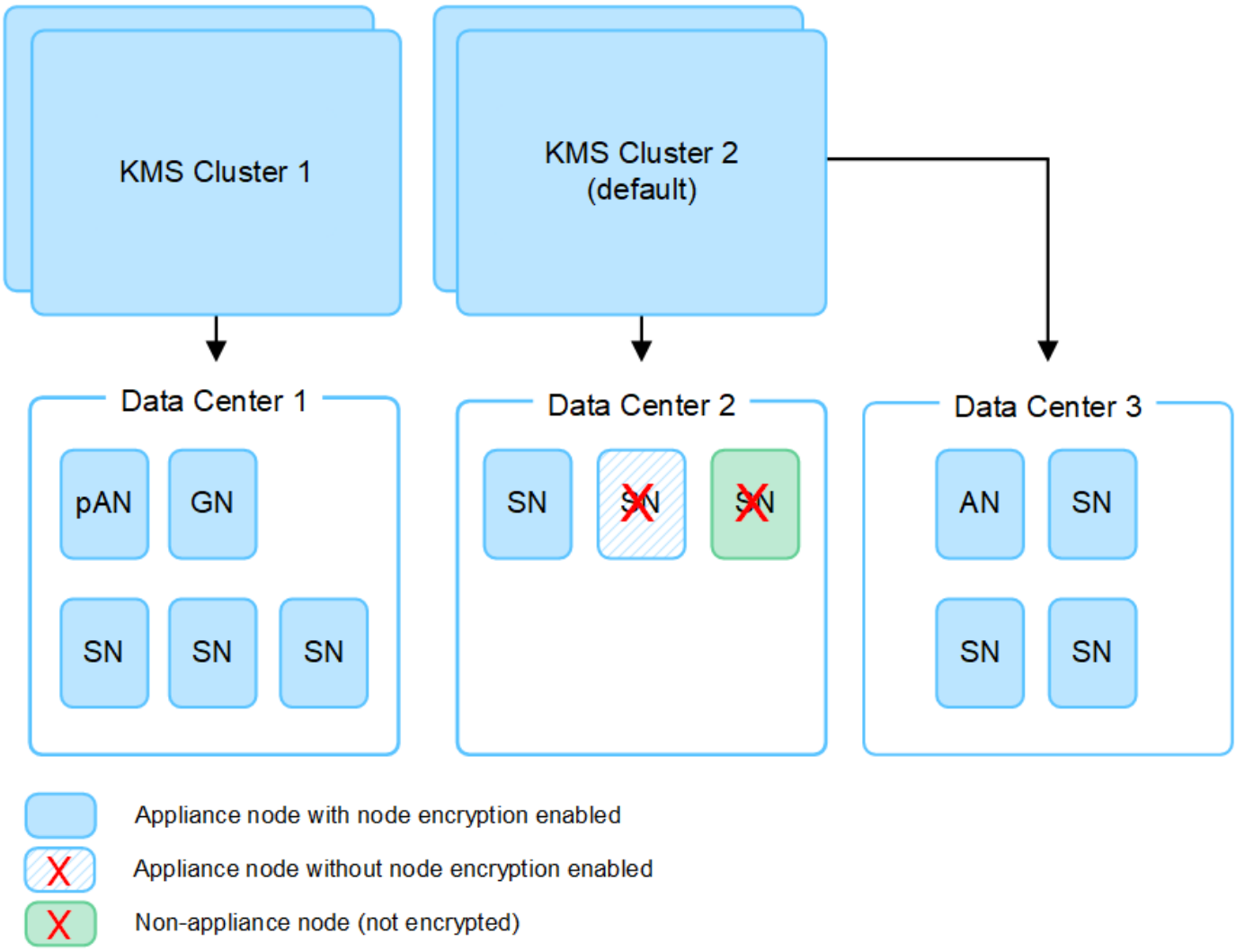
¿Cuántos servidores de gestión de claves necesito?

Puede configurar uno o varios servidores de gestión de claves externos para proporcionar claves de cifrado a los nodos de dispositivos en el sistema StorageGRID. Cada KMS proporciona una única clave de cifrado a los nodos de dispositivos StorageGRID en un único sitio o a un grupo de sitios.

StorageGRID admite el uso de clústeres KMS. Cada clúster de KMS contiene varios servidores de gestión de claves replicados que comparten configuraciones de configuración y claves de cifrado. Se recomienda usar clústeres KMS para la gestión de claves porque mejora las funcionalidades de conmutación por error de una configuración de alta disponibilidad.

Por ejemplo, supongamos que el sistema StorageGRID tiene tres sitios de centro de datos. Podría configurar un clúster KMS para proporcionar una clave a todos los nodos de dispositivos en el centro de datos 1 y un segundo clúster KMS para proporcionar una clave a todos los nodos de dispositivos de los demás sitios. Al agregar el segundo clúster KMS, puede configurar un KMS predeterminado para el Centro de datos 2 y el Centro de datos 3.

Tenga en cuenta que no puede usar un KMS para nodos que no sean del dispositivo ni para ningún nodo del dispositivo que no tenga habilitada la configuración **Node Encryption** durante la instalación.



¿Qué ocurre cuando se gira una clave?

Como una práctica recomendada de seguridad, debe hacerlo periódicamente "gire la clave de cifrado" Utilizado por cada KMS configurado.

Cuando la nueva versión de clave esté disponible:

- Se distribuye automáticamente a los nodos de dispositivos cifrados del sitio o de los sitios asociados con el KMS. La distribución debe producirse dentro de una hora a partir de la cual se gira la clave.
- Si el nodo de dispositivo cifrado está sin conexión cuando se distribuye la nueva versión de clave, el nodo recibirá la nueva clave en cuanto se reinicie.
- Si la nueva versión de clave no se puede utilizar para cifrar los volúmenes del dispositivo por cualquier motivo, se activa la alerta **KMS encryption key rotation failed** para el nodo del dispositivo. Es posible que deba ponerse en contacto con el soporte técnico para obtener ayuda para resolver esta alerta.

¿Puedo reutilizar un nodo de dispositivo después de cifrar?

Si necesita instalar un dispositivo cifrado en otro sistema StorageGRID, primero debe retirar el nodo grid para mover los datos del objeto a otro nodo. A continuación, puede utilizar el instalador de dispositivos de StorageGRID para "Borre la configuración de KMS". Al borrar la configuración KMS se deshabilita la configuración **cifrado de nodos** y se elimina la asociación entre el nodo del dispositivo y la configuración KMS

del sitio StorageGRID.

> Sin acceso a la clave de cifrado KMS, no se puede acceder a los datos que queden en el dispositivo y queden bloqueados de forma permanente.

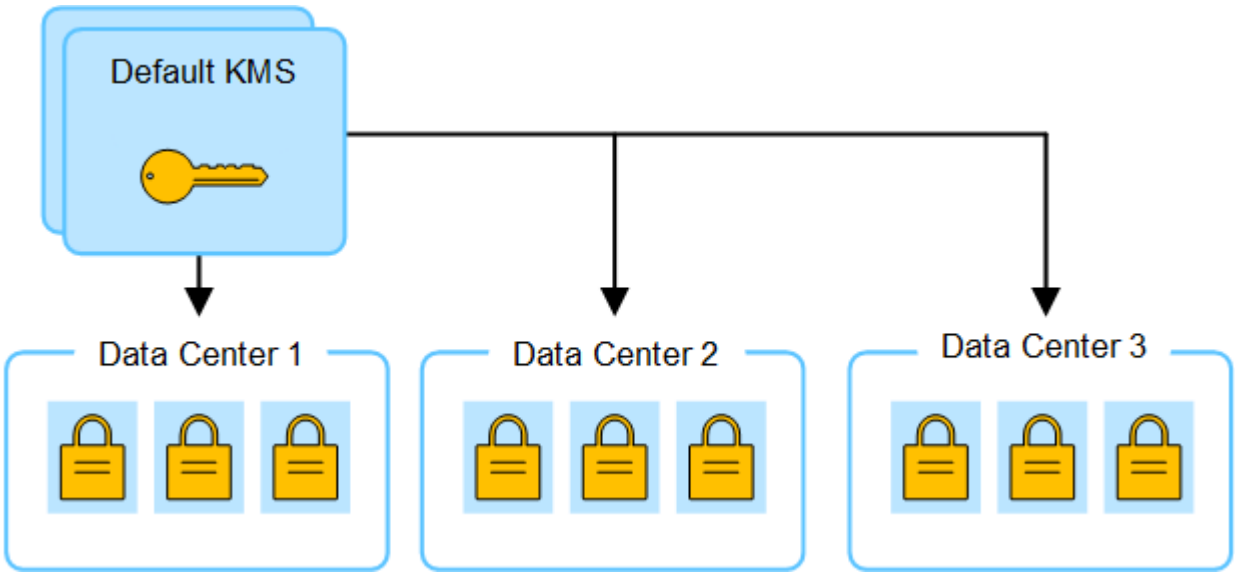
Consideraciones para cambiar el KMS de un sitio

Cada servidor de gestión de claves (KMS) o clúster KMS proporciona una clave de cifrado a todos los nodos de dispositivos en un único sitio o en un grupo de sitios. Si necesita cambiar qué KMS se utiliza para un sitio, es posible que necesite copiar la clave de cifrado de un KMS a otro.

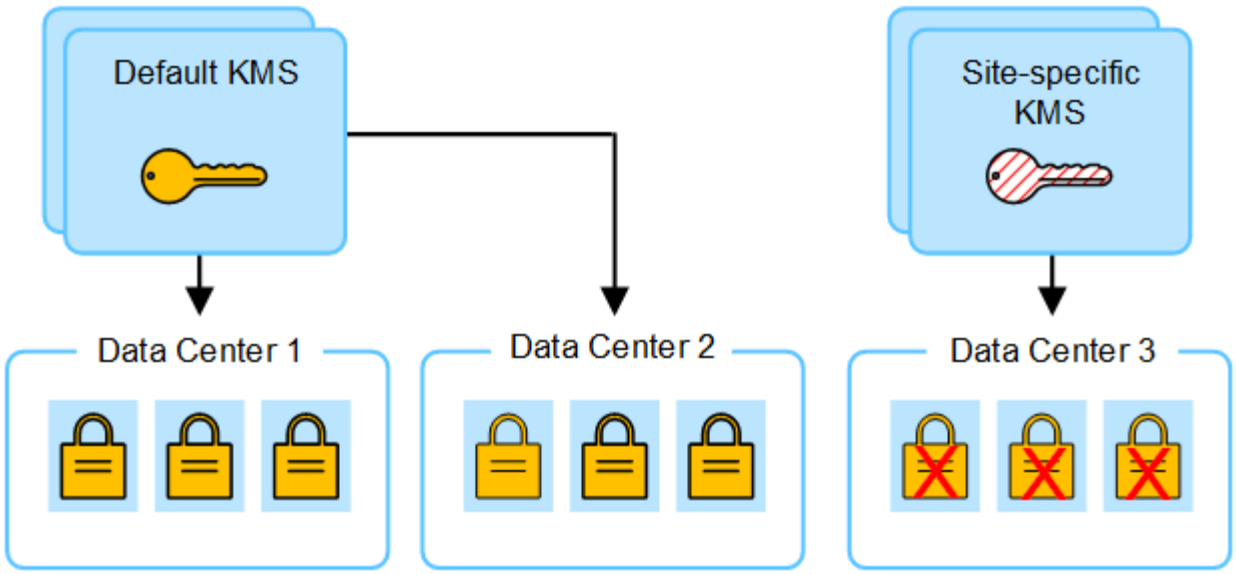
Si cambia el KMS utilizado para un sitio, debe asegurarse de que los nodos del dispositivo cifrados anteriormente en ese sitio se puedan descifrar utilizando la clave almacenada en el nuevo KMS. En algunos casos, es posible que necesite copiar la versión actual de la clave de cifrado del KMS original al KMS nuevo. Debe asegurarse de que el KMS tenga la clave correcta para descifrar los nodos del dispositivo cifrados en el sitio.

Por ejemplo:

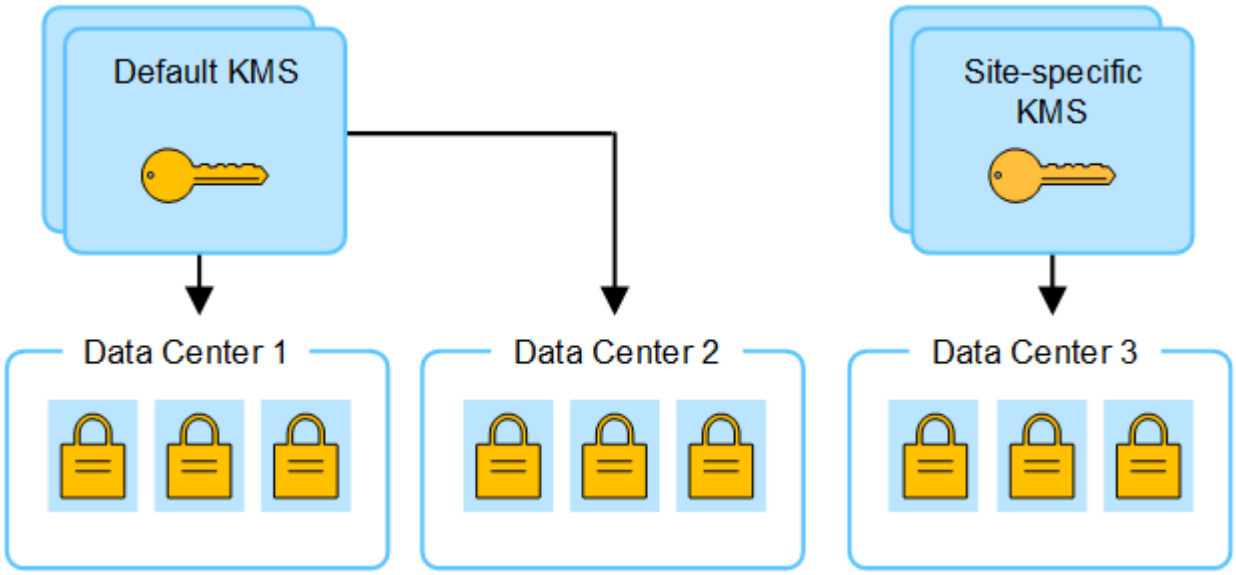
1. Inicialmente configuras un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos de dispositivo que tienen activada la configuración de **cifrado de nodos** se conectan al KMS y solicitan la clave de cifrado. Esta clave se usa para cifrar los nodos del dispositivo en todos los sitios. Esta misma clave también debe utilizarse para descifrar esos dispositivos.



3. Decide agregar un KMS específico de un sitio para un sitio (Data Center 3 en la figura). Sin embargo, como los nodos del dispositivo ya están cifrados, se produce un error de validación cuando se intenta guardar la configuración para el KMS específico del sitio. El error se produce porque el KMS específico del sitio no tiene la clave correcta para descifrar los nodos en ese sitio.



4. Para solucionar el problema, copia la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. (Técnicamente, copia la clave original en una nueva clave con el mismo alias. La clave original se convierte en una versión anterior de la clave nueva). El KMS específico del sitio tiene ahora la clave correcta para descifrar los nodos del dispositivo en el centro de datos 3, para que se puedan guardar en StorageGRID.



Utilice casos para cambiar qué KMS se utiliza para un sitio

La tabla resume los pasos necesarios para los casos más comunes para cambiar el KMS de un sitio.

Caso de uso para cambiar el KMS de un sitio	Pasos requeridos
Tiene una o más entradas KMS específicas del sitio y desea usar una de ellas como KMS predeterminado.	Edite el KMS específico del sitio. En el campo **administra claves para**, seleccione **Sitios no administrados por otro KMS (KMS predeterminado)**. El KMS específico del sitio se utilizará ahora como KMS predeterminado. Se aplicará a cualquier sitio que no tenga un KMS dedicado. "Editar un servidor de gestión de claves (KMS)"
Tiene un KMS predeterminado y agrega un sitio nuevo en una expansión. No desea utilizar el KMS predeterminado para el nuevo sitio.	1. Si los nodos del dispositivo en el sitio nuevo ya han sido cifrados por el KMS predeterminado, use el software KMS para copiar la versión actual de la clave de cifrado del KMS predeterminado a un KMS nuevo. 2. Con el Gestor de cuadrícula, agregue el nuevo KMS y seleccione el sitio. "Añadir un servidor de gestión de claves (KMS)"
Desea que el KMS para un sitio utilice un servidor diferente.	1. Si los nodos del dispositivo del sitio ya han sido cifrados por el KMS existente, use el software KMS para copiar la versión actual de la clave de cifrado del KMS existente al KMS nuevo. 2. Con el Administrador de cuadrícula, edite la configuración de KMS existente e introduzca el nuevo nombre de host o la dirección IP. "Añadir un servidor de gestión de claves (KMS)"

Configure StorageGRID como cliente en KMS

Debe configurar StorageGRID como cliente para cada servidor de gestión de claves externo o clúster de KMS antes de poder añadir el KMS a StorageGRID.

Estas instrucciones se aplican a Thales CipherTrust Manager y Hashicorp Vault. Para obtener una lista de productos y versiones compatibles, utilice "Herramienta de matriz de interoperabilidad de NetApp (IMT)".

Pasos

1. Desde el software KMS, cree un cliente StorageGRID para cada clúster KMS o KMS que vaya a utilizar.

   Cada KMS gestiona una única clave de cifrado para los nodos de dispositivos StorageGRID en un único sitio o en un grupo de sitios.

2. Cree una clave utilizando uno de los dos métodos siguientes:
   - Utilice la página de gestión de claves de su producto KMS. Cree una clave de cifrado AES para cada clúster KMS o KMS.

     La clave de cifrado debe ser de 2.048 bits o más, y debe ser exportable.

   - Haga que StorageGRID cree la clave. Se le pedirá que realice la prueba y guarde después "cargando certificados de cliente".

3. Registre la siguiente información de cada clúster KMS o KMS.

   Necesitará esta información cuando agregue el KMS a StorageGRID:

   - Nombre de host o dirección IP para cada servidor.
   - Puerto KMIP utilizado por el KMS.
   - Alias de clave para la clave de cifrado del KMS.

4. Para cada clúster de KMS o KMS, obtenga un certificado de servidor firmado por una entidad de certificación (CA) o un paquete de certificado que contiene cada uno de los archivos de certificado de CA codificados con PEM, concatenado en el orden de la cadena de certificados.

   El certificado de servidor permite que el KMS externo se autentique en StorageGRID.

   - El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.
   - El campo Nombre alternativo del asunto (SAN) de cada certificado de servidor debe incluir el nombre de dominio completo (FQDN) o la dirección IP a la que se conectará StorageGRID.

     > Al configurar el KMS en StorageGRID, debe introducir las mismas FQDN o direcciones IP en el campo **Nombre de host**.

   - El certificado de servidor debe coincidir con el certificado utilizado por la interfaz KMIP del KMS, que suele utilizar el puerto 5696.

5. Obtenga el certificado de cliente público emitido a StorageGRID por el KMS externo y la clave privada del certificado de cliente.

   El certificado de cliente permite que StorageGRID se autentique en el KMS.

Añadir un servidor de gestión de claves (KMS)

Utilice el asistente del servidor de gestión de claves de StorageGRID para agregar cada clúster KMS o KMS.

Antes de empezar

- Ha revisado el "consideraciones y requisitos para usar un servidor de gestión de claves".
- Ya tienes "Se ha configurado StorageGRID como cliente en el KMS"Y tiene la información necesaria para cada clúster KMS o KMS.
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

Acerca de esta tarea

Si es posible, configure cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplica a todos los sitios no administrados por otro KMS. Si crea el KMS predeterminado primero, todos los dispositivos cifrados por nodo de la cuadrícula se cifrarán con el KMS predeterminado. Si desea crear más tarde un KMS específico del sitio, primero debe copiar la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. Consulte "Consideraciones para cambiar el KMS de un sitio" para obtener más detalles.

Paso 1: Detalles de KM

En el Paso 1 (detalles de KMS) del Asistente para agregar un servidor de gestión de claves, proporciona detalles sobre el clúster de KMS o KMS.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Aparece la página del servidor de gestión de claves con la pestaña Detalles de configuración seleccionada.

2. Seleccione **Crear**.

   Paso 1 (detalles de KMS) del asistente Add a Key Management Server.

3. Introduzca la siguiente información para el KMS y el cliente StorageGRID que configuró en ese KMS.

Campo	Descripción
Nombre de KM	Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de clave	El alias de clave exacto del cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. **Nota**: Si no has creado una clave usando tu producto KMS, se te pedirá que StorageGRID cree la clave.
Administra claves para	El sitio StorageGRID que se asociará a este KMS. Si es posible, debe configurar cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplica a todos los sitios no administrados por otro KMS. • Seleccione un sitio si este KMS gestionará las claves de cifrado de los nodos de los dispositivos en un sitio específico. • Seleccione **Sitios no gestionados por otro KMS (por defecto KMS)** para configurar un KMS predeterminado que se aplicará a cualquier sitio que no tenga un KMS dedicado y a cualquier sitio que agregue en expansiones posteriores. **Nota:** se producirá Un error de validación al guardar la configuración de KMS si selecciona un sitio que anteriormente estaba cifrado por el KMS predeterminado pero no proporciona la versión actual de la clave de cifrado original al nuevo KMS.
Puerto	El puerto que el servidor KMS utiliza para las comunicaciones mediante el protocolo de interoperabilidad de gestión de claves (KMIP). De forma predeterminada es 5696, que es el puerto estándar KMIP.

Campo	Descripción
Nombre del hostl	El nombre de dominio completo o la dirección IP del KMS. **Nota:** El campo Nombre Alternativo del Asunto (SAN) del certificado del servidor debe incluir el FQDN o la dirección IP que introduzca aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor del clúster.
5. Seleccione **continuar**.

Paso 2: Cargar certificado de servidor

En el paso 2 (Cargar certificado de servidor) del asistente Agregar un servidor de gestión de claves, cargue el certificado de servidor (o paquete de certificados) para el KMS. El certificado de servidor permite que el KMS externo se autentique en StorageGRID.

Pasos

1. Desde **Paso 2 (Cargar certificado de servidor)**, busque la ubicación del certificado de servidor guardado o el paquete de certificados.
2. Cargue el archivo de certificado.

   Se muestran los metadatos del certificado del servidor.

   > Si cargó un paquete de certificados, los metadatos de cada certificado aparecen en la pestaña correspondiente.

3. Seleccione **continuar**.

Paso 3: Cargar certificados de cliente

En el paso 3 (Cargar certificados de cliente) del asistente para agregar un servidor de gestión de claves, cargue el certificado de cliente y la clave privada de certificado de cliente. El certificado de cliente permite que StorageGRID se autentique en el KMS.

Pasos

1. Desde **Paso 3 (Cargar certificados de cliente)**, busque la ubicación del certificado de cliente.
2. Cargue el archivo de certificado de cliente.

   Aparecen los metadatos del certificado de cliente.

3. Busque la ubicación de la clave privada del certificado de cliente.
4. Cargue el archivo de clave privada.
5. Selecciona **Probar y guardar**.

   Si no existe una clave, se le pedirá que StorageGRID cree una.

   Se prueban las conexiones entre el servidor de gestión de claves y los nodos del dispositivo. Si todas las conexiones son válidas y se encuentra la clave correcta en el KMS, el servidor de gestión de claves nuevo

se añade a la tabla de la página del servidor de gestión de claves.

> Inmediatamente después de añadir un KMS, el estado del certificado en la página servidor de gestión de claves aparece como Desconocido. StorageGRID puede tardar hasta 30 minutos en obtener el estado real de cada certificado. Debe actualizar el navegador web para ver el estado actual.

6. Si aparece un mensaje de error al seleccionar **Probar y guardar**, revise los detalles del mensaje y luego seleccione **Aceptar**.

   Por ejemplo, puede recibir un error 422: Entidad no procesable si se produjo un error en una prueba de conexión.

7. Si necesita guardar la configuración actual sin probar la conexión externa, seleccione **Forzar guardar**.

   > Al seleccionar **Force save** se guarda la configuración de KMS, pero no se prueba la conexión externa de cada dispositivo a ese KMS. Si hay un problema con la configuración, es posible que no pueda reiniciar los nodos de los dispositivos que tienen habilitado el cifrado de nodos en el sitio afectado. Es posible que pierda acceso a los datos hasta que se resuelvan los problemas.

8. Revise la advertencia de confirmación y seleccione **Aceptar** si está seguro de que desea forzar el guardado de la configuración.

   La configuración de KMS se guarda pero la conexión con el KMS no se prueba.

Administrar un KMS

La gestión de un servidor de gestión de claves (KMS) implica ver y editar detalles, gestionar certificados, ver nodos cifrados y eliminar un KMS cuando ya no es necesario.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permiso de acceso necesario".

Ver detalles de KMS

Es posible ver información sobre cada servidor de gestión de claves (KMS) en el sistema StorageGRID, incluidos los detalles de claves y el estado actual de los certificados de servidor y de cliente.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Aparecerá la página Servidor de gestión de claves con la siguiente información:

   - En la pestaña Detalles de configuración, se enumeran los servidores de gestión de claves configurados.
   - El separador Nodos Cifrados muestra todos los nodos que tienen el cifrado de nodos activado.

2. Para ver los detalles de un KMS específico y realizar operaciones en ese KMS, seleccione el nombre del KMS. La página de detalles del KMS muestra la siguiente información:

Campo	Descripción
Administra claves para	El sitio StorageGRID asociado con el KMS. Este campo muestra el nombre de un sitio StorageGRID específico o **Sitios no administrados por otro KMS (KMS predeterminado).**
Nombre del hostl	El nombre de dominio completo o la dirección IP del KMS. Si existe un clúster de dos servidores de gestión de claves, se muestran el nombre de dominio completo o la dirección IP de ambos servidores. Si hay más de dos servidores de gestión de claves en un clúster, el nombre de dominio completo o la dirección IP del primer KMS se enumeran junto con la cantidad de servidores de gestión de claves adicionales en el clúster. Por ejemplo: `10.10.10.10 and 10.10.10.11` o. `10.10.10.10 and 2 others`. Para ver todos los nombres de host de un clúster, seleccione un KMS y seleccione **Editar** o **Acciones** > **Editar**.

3. Seleccione una pestaña en la página de detalles de KMS para ver la siguiente información:

Pestaña	Campo	Descripción
Detalles clave	Nombre de clave	El alias clave del cliente StorageGRID en el KMS.
UID de clave	Identificador único de la última versión de la clave.	Última modificación
La fecha y la hora de la última versión de la clave.	Certificado de servidor	Metadatos
Los metadatos del certificado, como el número de serie, la fecha y la hora de caducidad y el certificado PEM.	Certificado PEM	El contenido del archivo PEM (correo de privacidad mejorada) para el certificado.
Certificado de cliente	Metadatos	Los metadatos del certificado, como el número de serie, la fecha y la hora de caducidad y el certificado PEM.

4. Con la frecuencia requerida por las prácticas de seguridad de su organización, seleccione **Rotar clave** o utilice el software KMS para crear una nueva versión de la clave.

   Cuando la rotación de claves es correcta, se actualizan los campos UID Clave y Última Modificación.

Si gira la clave de cifrado con el software KMS, gírela de la última versión utilizada de la clave a una nueva versión de la misma clave. No gire a una clave completamente diferente.

Nunca intente girar una clave cambiando el nombre de clave (alias) del KMS. StorageGRID requiere que se pueda acceder a todas las versiones de claves usadas anteriormente (así como a las futuras) desde el KMS con el mismo alias de clave. Si cambia el alias de clave para un KMS configurado, es posible que StorageGRID no pueda descifrar los datos.

Gestionar certificados

Resuelva con prontitud cualquier problema de servidor o certificado de cliente. Si es posible, sustituya los certificados antes de que caduquen.

Debe solucionar cualquier problema con los certificados Lo antes posible. para mantener el acceso a los datos.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.
2. En la tabla, observe el valor de Caducidad de certificado para cada KMS.
3. Si se desconoce la caducidad del certificado para cualquier KMS, espere hasta 30 minutos y, a continuación, actualice el explorador web.
4. Si la columna Caducidad del certificado indica que un certificado ha caducado o está a punto de caducar, seleccione el KMS para ir a la página de detalles del KMS.
   a. Seleccione **Certificado de servidor** y verifique el valor del campo “Expires on”.
   b. Para reemplazar el certificado, seleccione **Editar certificado** para cargar un nuevo certificado.
   c. Repita estos subpasos y seleccione **Certificado de cliente** en lugar de Certificado de servidor.
5. Cuando se activan las alertas **KMS CA CERTIFICATION**, **KMS client certificate expiration** y **KMS server certificate expiration**, anote la descripción de cada alerta y realice las acciones recomendadas.

StorageGRID puede tardar hasta 30 minutos en obtener actualizaciones para la expiración del certificado. Actualice el explorador web para ver los valores actuales.

Vea los nodos cifrados

Puede ver información acerca de los nodos del dispositivo en el sistema StorageGRID que tienen activada la configuración * cifrado de nodos*.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Se muestra la página servidor de gestión de claves. En la pestaña Configuration Details, se muestra todos los servidores de gestión de claves que se configuraron.

2. En la parte superior de la página, seleccione la pestaña **Nodos encriptados**.

   La pestaña Nodos cifrados muestra los nodos del dispositivo en su sistema StorageGRID que tienen habilitada la configuración **Encriptación de nodos**.

3. Revise la información de la tabla de cada nodo del dispositivo.

Columna	Descripción
Nombre del nodo	El nombre del nodo del dispositivo.
Tipo de nodo	El tipo de nodo: Almacenamiento, administrador o puerta de enlace.
Sitio	El nombre del sitio StorageGRID donde se instala el nodo.
Nombre de KM	Nombre descriptivo del KMS utilizado para el nodo. Si no aparece ningún KMS, seleccione la pestaña Detalles de configuración para agregar un KMS. "Añadir un servidor de gestión de claves (KMS)"
UID de clave	El ID único de la clave de cifrado utilizada para cifrar y descifrar datos en el nodo del dispositivo. Para ver un UID de clave completo, seleccione el texto. Un guión (--) indica que el UID de la clave es desconocido, posiblemente debido a un problema de conexión entre el nodo del dispositivo y el KMS.
Estado	El estado de la conexión entre el KMS y el nodo del dispositivo. Si el nodo está conectado, la Marca de tiempo se actualiza cada 30 minutos. El estado de la conexión puede tardar varios minutos en actualizarse después de que cambie la configuración de KMS. **Nota:** Actualiza tu navegador web para ver los nuevos valores.

4. Si la columna Estado indica un problema de KMS, resuelva el problema inmediatamente.

   Durante las operaciones normales de KMS, el estado será **conectado a KMS**. Si un nodo está desconectado de la cuadrícula, se muestra el estado de conexión del nodo (administrativamente abajo o Desconocido).

   Otros mensajes de estado corresponden a las alertas StorageGRID con los mismos nombres:

   - No se ha podido cargar la configuración DE KMS
   - Error de conectividad DE KMS
   - No se ha encontrado el nombre de la clave de cifrado DE KMS
   - Error en la rotación de la clave de cifrado DE KMS
   - LA clave KMS no pudo descifrar el volumen de un dispositivo
   - KMS no está configurado

   Realice las acciones recomendadas para estas alertas.

   Debe solucionar cualquier problema inmediatamente para garantizar que los datos están totalmente protegidos.

Editar un KMS

Es posible que deba editar la configuración de un servidor de gestión de claves, por ejemplo, si un certificado está a punto de expirar.

Antes de empezar

- Si planea actualizar el sitio seleccionado para un KMS, ha revisado el "Consideraciones para cambiar el KMS de un sitio".
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Se muestra la página Servidor de gestión de claves donde se muestran todos los servidores de gestión de claves que se configuraron.

2. Selecciona el KMS que deseas editar y selecciona **Acciones** > **Editar**.

   También puede editar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Editar** en la página de detalles del KMS.

3. Opcionalmente, actualice los detalles en **Paso 1 (detalles de KMS)** del asistente Editar un servidor de administración de claves.

Campo	Descripción
Nombre de KM	Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de clave	El alias de clave exacto del cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. Solo es necesario editar el nombre de la clave en casos excepcionales. Por ejemplo, debe editar el nombre de clave si se cambia el nombre del alias en el KMS o si se han copiado todas las versiones de la clave anterior al historial de versiones del nuevo alias.
Administra claves para	Si está editando un KMS específico del sitio y aún no tiene un KMS predeterminado, seleccione opcionalmente **Sitios no gestionados por otro KMS (KMS predeterminado)**. Esta selección convierte un KMS específico del sitio al KMS predeterminado, que se aplicará a todos los sitios que no tienen un KMS dedicado y a cualquier sitio agregado en una expansión. **Nota:** Si está editando un KMS específico del sitio, no puede seleccionar otro sitio. Si está editando el KMS predeterminado, no puede seleccionar un sitio específico.
Puerto	El puerto que el servidor KMS utiliza para las comunicaciones mediante el protocolo de interoperabilidad de gestión de claves (KMIP). De forma predeterminada es 5696, que es el puerto estándar KMIP.

Campo	Descripción
Nombre del hostl	El nombre de dominio completo o la dirección IP del KMS. **Nota:** El campo Nombre Alternativo del Asunto (SAN) del certificado del servidor debe incluir el FQDN o la dirección IP que introduzca aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor del clúster.
5. Seleccione **continuar**.

   Paso 2 (Cargar certificado de servidor) del asistente Editar un servidor de gestión de claves.

6. Si necesita sustituir el certificado del servidor, seleccione **examinar** y cargue el nuevo archivo.
7. Seleccione **continuar**.

   El paso 3 (Cargar certificados de cliente) del asistente Editar un servidor de gestión de claves aparece.

8. Si necesita sustituir el certificado de cliente y la clave privada del certificado de cliente, seleccione **examinar** y cargue los nuevos archivos.
9. Selecciona **Probar y guardar**.

   Se prueban las conexiones entre el servidor de gestión de claves y todos los nodos de dispositivos cifrados por nodo en los sitios afectados. Si todas las conexiones de nodos son válidas y se encuentra la clave correcta en el KMS, el servidor de gestión de claves se agrega a la tabla de la página servidor de gestión de claves.

10. Si aparece un mensaje de error, revise los detalles del mensaje y seleccione **Aceptar**.

    Por ejemplo, puede recibir un error 422: Entidad no procesable si el sitio seleccionado para este KMS ya está administrado por otro KMS o si se produjo un error en una prueba de conexión.

11. Si necesita guardar la configuración actual antes de resolver los errores de conexión, seleccione **Forzar guardar**.

    > Al seleccionar **Force save** se guarda la configuración de KMS, pero no se prueba la conexión externa de cada dispositivo a ese KMS. Si hay un problema con la configuración, es posible que no pueda reiniciar los nodos de los dispositivos que tienen habilitado el cifrado de nodos en el sitio afectado. Es posible que pierda acceso a los datos hasta que se resuelvan los problemas.

    Se guarda la configuración de KMS.

12. Revise la advertencia de confirmación y seleccione **Aceptar** si está seguro de que desea forzar el guardado de la configuración.

    La configuración del KMS se guarda, pero la conexión al KMS no se prueba.

Quitar un servidor de gestión de claves (KMS)

En algunos casos, es posible quitar un servidor de gestión de claves. Por ejemplo, puede que desee quitar un KMS específico de un sitio si ha retirado del servicio el sitio.

Antes de empezar

- Ha revisado el "consideraciones y requisitos para usar un servidor de gestión de claves".
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

Acerca de esta tarea

Puede eliminar un KMS en los siguientes casos:

- Puede eliminar un KMS específico de un sitio si se ha dado de baja o si el sitio incluye ningún nodo de dispositivo con cifrado de nodo activado.
- Puede eliminar el KMS predeterminado si ya existe un KMS específico del sitio para cada sitio que tiene nodos de dispositivo con cifrado de nodo activado.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Se muestra la página Servidor de gestión de claves donde se muestran todos los servidores de gestión de claves que se configuraron.

2. Selecciona el KMS que deseas eliminar y selecciona **Acciones** > **Eliminar**.

   También puede eliminar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Eliminar** en la página de detalles del KMS.

3. Confirme que lo siguiente es verdadero:
   - Está eliminando un KMS específico del sitio para un sitio que no tiene ningún nodo de dispositivo con cifrado de nodo activado.
   - Está eliminando el KMS predeterminado, pero ya existe un KMS específico para cada sitio con cifrado de nodo.
4. Seleccione **Sí**.

   La configuración de KMS se elimina.

Administrar la configuración de proxy

Configurar proxy de almacenamiento

Si utiliza servicios de plataforma o pools de almacenamiento en cloud, puede configurar un proxy no transparente entre los nodos de almacenamiento y los extremos de S3 externos. Por ejemplo, es posible que necesite un proxy no transparente para permitir que los mensajes de servicios de plataforma se envíen a extremos externos, como un punto final en Internet.

La configuración de proxy de almacenamiento configurada no se aplica a los extremos de servicios de plataforma Kafka.

Antes de empezar

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

Acerca de esta tarea

Puede configurar los ajustes para un solo proxy de almacenamiento.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Ajustes de proxy**.
2. En la pestaña **Almacenamiento**, selecciona la casilla de verificación **Habilitar proxy de almacenamiento**.
3. Seleccione el protocolo para el proxy de almacenamiento.
4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. De manera opcional, introduzca el puerto utilizado para conectarse al servidor proxy.

   Deje este campo en blanco para utilizar el puerto predeterminado para el protocolo: 80 para HTTP o 1080 para SOCKS5.

6. Seleccione **Guardar**.

   Después de guardar el proxy de almacenamiento, se pueden configurar y probar nuevos puntos finales para los servicios de plataforma o los pools de Cloud Storage.

   Los cambios de proxy pueden tardar hasta 10 minutos en surtir efecto.

7. Compruebe la configuración del servidor proxy para asegurarse de que los mensajes de StorageGRID relacionados con el servicio de la plataforma no se bloqueen.
8. Si necesita deshabilitar un proxy de almacenamiento, desactive la casilla de verificación y seleccione **Guardar**.

Configurar valores de proxy de administración

Si envía paquetes AutoSupport mediante HTTP o HTTPS, puede configurar un servidor proxy no transparente entre los nodos de administración y el soporte técnico (AutoSupport).

Para obtener más información acerca de AutoSupport, consulte "Configure AutoSupport".

Antes de empezar

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

Acerca de esta tarea

Puede configurar los ajustes para un solo proxy de administración.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Ajustes de proxy**.

   Aparecerá la página Configuración de Proxy. De forma predeterminada, se selecciona Almacenamiento en el menú de pestañas.

2. Seleccione la pestaña **Admin**.
3. Seleccione la casilla de verificación **Enable Admin Proxy**.
4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. Introduzca el puerto utilizado para conectarse al servidor proxy.
6. Opcionalmente, introduzca un nombre de usuario y una contraseña para el servidor proxy.

   Deje estos campos en blanco si el servidor proxy no requiere un nombre de usuario ni una contraseña.

7. Seleccione una de las siguientes opciones:

   - Si desea proteger la conexión con el proxy de administración, seleccione **Verificar certificado**. Cargue un paquete de CA para verificar la autenticidad de los certificados SSL que presenta el servidor proxy de administrador.

     > AutoSupport On Demand, E-Series AutoSupport a través de StorageGRID y Update Path Determination en la página de actualización de StorageGRID no funcionarán si se verifica un certificado proxy.

   Después de cargar el paquete de CA, aparecen sus metadatos.

   - Si no desea validar los certificados al comunicarse con el servidor proxy de administración, seleccione **No verificar el certificado**.

8. Seleccione **Guardar**.

   Una vez que se guarda el proxy de administrador, se configura el servidor proxy entre los nodos de administrador y el soporte técnico.

   > Los cambios de proxy pueden tardar hasta 10 minutos en surtir efecto.

9. Si necesita deshabilitar el proxy de administración, desactive la casilla de verificación **Habilitar proxy de administración** y, a continuación, seleccione **Guardar**.

Controle los firewalls

Controle el acceso a un firewall externo

Puede abrir o cerrar puertos específicos en el firewall externo.

Puede controlar el acceso a las interfaces de usuario y las API de los nodos de administrador de StorageGRID. Para ello, abra y cierre puertos específicos en el firewall externo. Por ejemplo, es posible que desee evitar que los inquilinos puedan conectarse a Grid Manager en el firewall, además de utilizar otros métodos para controlar el acceso al sistema.

Si desea configurar el firewall interno de StorageGRID, consulte "Configure el firewall interno".

Puerto	Descripción	Si el puerto está abierto…
443	Puerto HTTPS predeterminado para nodos de administración	Los exploradores web y los clientes de la API de gestión pueden acceder a Grid Manager, a la API de gestión de grid, al administrador de inquilinos y a la API de gestión de inquilinos. **Nota:** el puerto 443 también se utiliza para tráfico interno.
8443	Puerto de Grid Manager restringido en nodos de administración	• Los exploradores web y los clientes de la API de gestión pueden acceder a Grid Manager y a la API de gestión de grid mediante HTTPS. • Los exploradores web y los clientes de API de gestión no pueden acceder al administrador de inquilinos ni a la API de gestión de inquilinos. • Se rechazarán las solicitudes de contenido interno.
9443	Puerto de administrador de inquilinos restringido en los nodos de administrador	• Los exploradores web y los clientes de API de gestión pueden acceder al administrador de inquilinos y a la API de gestión de inquilinos mediante HTTPS. • Los exploradores web y los clientes de API de gestión no pueden acceder a Grid Manager ni a la API de administración de grid. • Se rechazarán las solicitudes de contenido interno.

El inicio de sesión único (SSO) no está disponible en los puertos de administrador de grid restringido o de administrador de inquilinos. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autentiquen con inicio de sesión único.

Información relacionada

- "Inicie sesión en Grid Manager"
- "Cree una cuenta de inquilino"
- "Comunicaciones externas"

Gestionar los controles internos del firewall

StorageGRID incluye un firewall interno en cada nodo que mejora la seguridad del grid al permitirle controlar el acceso de red al nodo. Utilice el firewall para evitar el acceso a la red en todos los puertos, excepto los necesarios para su implementación de grid específica. Los cambios de configuración que realice en la página de control del firewall se despliegan en cada nodo.

Utilice las tres pestañas de la página de control de Firewall para personalizar el acceso que necesita para su grid.

- **Lista de direcciones privilegiadas**: Utilice esta pestaña para permitir el acceso seleccionado a los puertos cerrados. Puede agregar direcciones IP o subredes en la notación CIDR que pueden acceder a los puertos cerrados mediante la pestaña Administrar acceso externo.
- **Administrar acceso externo**: Utilice esta pestaña para cerrar los puertos que están abiertos por defecto, o reabrir los puertos previamente cerrados.
- **Red de cliente no confiable**: Utilice esta pestaña para especificar si un nodo confía en el tráfico entrante de la red cliente.

  La configuración de esta ficha sustituye a la configuración de la ficha Administrar acceso externo.

  - Un nodo con una red de cliente que no sea de confianza aceptará solo conexiones en los puertos de punto final del equilibrador de carga configurados en ese nodo (puntos finales enlazados de tipo de nodo, interfaz de nodo y global).
  - Los puertos de punto final del equilibrador de carga *son los únicos puertos abiertos* en redes de cliente que no son de confianza, independientemente de la configuración de la pestaña Administrar redes externas.
  - Cuando se confía, se puede acceder a todos los puertos abiertos en la pestaña Administrar acceso externo, así como a cualquier punto final del equilibrador de carga abierto en la red cliente.

> La configuración que realice en una pestaña puede afectar a los cambios de acceso que realice en otra pestaña. Asegúrese de comprobar la configuración en todas las pestañas para asegurarse de que su red se comporta de la forma que espera.

Para configurar los controles internos del firewall, consulte "Configurar los controles del firewall".

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulte "Controle el acceso a un firewall externo".

Lista de direcciones con privilegios y pestañas Gestionar acceso externo

El separador Lista de Direcciones con Privilegios permite registrar una o más direcciones IP a las que se les concede acceso a los puertos de grid que están cerrados. La pestaña Administrar acceso externo permite cerrar el acceso externo a los puertos externos seleccionados o a todos los puertos externos abiertos (los puertos externos son puertos a los que pueden acceder los nodos que no son de cuadrícula de forma predeterminada). Estas dos pestañas a menudo se pueden utilizar juntas para personalizar el acceso exacto a la red que necesita para su grid.

> Las direcciones IP con privilegios no tienen acceso de puerto de grid interno por defecto.

Ejemplo 1: Utilice un host de salto para tareas de mantenimiento

Supongamos que desea utilizar un host de salto (un host reforzado con seguridad) para la administración de la red. Puede utilizar estos pasos generales:

1. Utilice el separador Lista de Direcciones con Privilegios para agregar la dirección IP del host de salto.
2. Utilice la pestaña Gestionar acceso externo para bloquear todos los puertos.

> Agregue la dirección IP con privilegios antes de bloquear los puertos 443 y 8443. Cualquier usuario conectado actualmente a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones con privilegios.

Después de guardar la configuración, todos los puertos externos en el nodo de administración de la cuadrícula se bloquearán para todos los hosts excepto el host de salto. A continuación, puede utilizar el host de salto para realizar tareas de mantenimiento en la red de forma más segura.

Ejemplo 2: Limitar el acceso a Grid Manager y al administrador de inquilinos

Supongamos que desea limitar el acceso a Grid Manager y al gestor de inquilinos (puertos predefinidos) por motivos de seguridad. Puede utilizar estos pasos generales:

1. Utilice el conmutador en la pestaña Administrar acceso externo para bloquear el puerto 443.
2. Utilice el conmutador en la pestaña Administrar acceso externo para permitir el acceso al puerto 8443.
3. Utilice el conmutador en la pestaña Administrar acceso externo para permitir el acceso al puerto 9443.

Después de guardar la configuración, los hosts no podrán acceder al puerto 443, pero podrán acceder a Grid Manager a través del puerto 8443 y al gestor de inquilinos a través del puerto 9443.

> Los puertos 443, 8443 y 9443 son los puertos predefinidos para Grid Manager y Tenant Manager. Puede alternar cualquier puerto para limitar el acceso a un gestor de inquilinos o Grid Manager específico.

Ejemplo 3: Bloquear puertos sensibles

Suponga que desea bloquear los puertos confidenciales y el servicio en ese puerto (por ejemplo, SSH en el puerto 22). Puede utilizar los siguientes pasos generales:

1. Utilice el separador Lista de Direcciones con Privilegios para otorgar acceso sólo a los hosts que necesitan acceso al servicio.
2. Utilice la pestaña Gestionar acceso externo para bloquear todos los puertos.

> Agregue la dirección IP con privilegios antes de bloquear el acceso a los puertos asignados para acceder a Grid Manager y al gestor de inquilinos (los puertos predefinidos son 443 y 8443). Cualquier usuario conectado actualmente a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones con privilegios.

Después de guardar la configuración, el puerto 22 y el servicio SSH estarán disponibles para los hosts de la lista de direcciones con privilegios. Se denegará el acceso al servicio a todos los demás hosts sin importar de qué interfaz proviene la solicitud.

Ejemplo 4: Desactivar el acceso a los servicios no utilizados

A nivel de red, puede desactivar algunos servicios que no desea utilizar. Por ejemplo, si no proporcionará acceso Swift, debe realizar los siguientes pasos generales:

1. Utilice el conmutador en la pestaña Administrar acceso externo para bloquear el puerto 18083.
2. Utilice el conmutador en la pestaña Administrar acceso externo para bloquear el puerto 18085.

Después de guardar la configuración, el nodo de almacenamiento ya no permite la conectividad Swift, pero sigue permitiendo el acceso a otros servicios en puertos no bloqueados.

Pestaña Redes de cliente que no son de confianza

Si está utilizando una red de cliente, puede ayudar a proteger StorageGRID de ataques hostiles aceptando tráfico de cliente entrante sólo en puntos finales configurados explícitamente.

De forma predeterminada, la red de cliente de cada nodo de cuadrícula es *Trusted*. Es decir, de forma predeterminada, StorageGRID confía en las conexiones entrantes a cada nodo de grid en All "puertos externos disponibles".

Puede reducir la amenaza de ataques hostiles en su sistema StorageGRID especificando que la red cliente de cada nodo sea *no confiable*. Si la red de cliente de un nodo no es de confianza, el nodo sólo acepta conexiones entrantes en los puertos configurados explícitamente como puntos finales de equilibrador de carga. Consulte "Configurar puntos finales del equilibrador de carga" y.. "Configurar los controles del firewall".

Ejemplo 1: Gateway Node solo acepta solicitudes HTTPS S3

Supongamos que desea que un nodo de puerta de enlace rechace todo el tráfico entrante en la red cliente excepto las solicitudes HTTPS S3. Debe realizar estos pasos generales:

1. Desde la "Puntos finales del equilibrador de carga" Configure un punto final del equilibrador de carga para S3 sobre HTTPS en el puerto 443.
2. En la página de control de firewall, seleccione Sin confianza para especificar que la red cliente del nodo de puerta de enlace no sea de confianza.

Después de guardar la configuración, se descarta todo el tráfico entrante en la red cliente del nodo de puerta de enlace, excepto las solicitudes HTTPS S3 en el puerto 443 y las solicitudes ICMP echo (ping).

Ejemplo 2: El nodo de almacenamiento envía solicitudes de servicios de plataforma S3

Suponga que desea habilitar el tráfico de servicios de la plataforma S3 saliente desde un nodo de almacenamiento, pero desea evitar las conexiones entrantes a ese nodo de almacenamiento en la red de clientes. Debe realizar este paso general:

- En la pestaña Redes de cliente sin confianza de la página de control de firewall, indique que la red de cliente en el nodo de almacenamiento no es de confianza.

Después de guardar la configuración, el nodo de almacenamiento ya no acepta ningún tráfico entrante en la red cliente, pero continúa permitiendo las solicitudes salientes a los destinos de servicios de plataforma configurados.

Ejemplo 3: Limitar el acceso a Grid Manager a una subred

Supongamos que desea permitir el acceso de Grid Manager solo en una subred específica. Debe realizar los siguientes pasos:

1. Conecte la red cliente de sus nodos de administración a la subred.
2. Utilice la pestaña Red de cliente sin confianza para configurar la red cliente como no confiable.
3. Cuando cree un extremo del balanceador de carga de la interfaz de gestión, introduzca el puerto y seleccione la interfaz de gestión a la que accederá el puerto.
4. Seleccione **Sí** para Red cliente no confiable.
5. Utilice el separador Gestionar acceso externo para bloquear todos los puertos externos (con o sin direcciones IP con privilegios definidas para hosts fuera de esa subred).

Después de guardar la configuración, solo los hosts de la subred especificada pueden acceder a Grid Manager. Todos los demás hosts están bloqueados.

Configure el firewall interno

Puede configurar el firewall de StorageGRID para controlar el acceso a la red a puertos específicos de los nodos de StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Ha revisado la información de "Gestionar los controles del firewall" y.. "Directrices sobre redes".
- Si desea que un nodo de administración o un nodo de puerta de enlace acepte tráfico entrante sólo en puntos finales configurados explícitamente, ha definido los puntos finales del equilibrador de carga.

> ⓘ Al cambiar la configuración de la red cliente, las conexiones de cliente existentes pueden fallar si no se han configurado los puntos finales del equilibrador de carga.

Acerca de esta tarea

StorageGRID incluye un firewall interno en cada nodo que le permite abrir o cerrar algunos de los puertos en los nodos del grid. Puede utilizar las pestañas de control del firewall para abrir o cerrar los puertos que están abiertos de forma predeterminada en la red de grid, la red de administración y la red de cliente. También puede crear una lista de direcciones IP con privilegios que pueden acceder a los puertos de cuadrícula que están cerrados. Si utiliza una red cliente, puede especificar si un nodo confía en el tráfico entrante de la red cliente y puede configurar el acceso de puertos específicos en la red cliente.

Limitar el número de puertos abiertos a direcciones IP fuera de su red a solo aquellos que son absolutamente necesarios mejora la seguridad de su red. Utilice la configuración en cada una de las tres pestañas de control de Firewall para asegurarse de que solo los puertos necesarios estén abiertos.

Para obtener más información sobre el uso de controles de firewall, incluidos ejemplos, consulte "Gestionar los controles del firewall".

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulte "Controle el acceso a un firewall externo".

Acceda a los controles del cortafuegos

Pasos

1. Selecciona **CONFIGURACIÓN** > **Seguridad** > **Control de firewall**.

   Las tres pestañas de esta página se describen en "Gestionar los controles del firewall".

2. Seleccione cualquier pestaña para configurar los controles del firewall.

   Puede utilizar estas pestañas en cualquier orden. Las configuraciones establecidas en una pestaña no limitan lo que puede hacer en las otras pestañas; sin embargo, los cambios de configuración que realice en una pestaña pueden cambiar el comportamiento de los puertos configurados en otras pestañas.

Lista de direcciones con privilegios

Utilice el separador Lista de Direcciones con Privilegios para otorgar a los hosts acceso a los puertos que están cerrados por defecto o cerrados por valores en el separador Gestionar Acceso Externo.

Las direcciones IP y subredes con privilegios no tienen acceso interno a la cuadrícula por defecto. Además, los puntos finales del equilibrador de carga y los puertos adicionales abiertos en la pestaña de lista de direcciones con privilegios son accesibles incluso si están bloqueados en la pestaña Gestionar acceso externo.

> La configuración de la pestaña Lista de direcciones con privilegios no puede sustituir la configuración de la pestaña Red de clientes sin confianza.

Pasos

1. En la pestaña Lista de direcciones con privilegios, introduzca la dirección o subred IP que desea otorgar acceso a los puertos cerrados.
2. Opcionalmente, seleccione **Agregar otra dirección IP o subred en notación CIDR** para agregar clientes con privilegios adicionales.

   > Agregue el menor número posible de direcciones a la lista de privilegios.

3. Opcionalmente, seleccione **Permitir direcciones IP privilegiadas para acceder a los puertos internos de StorageGRID**. Consulte "Puertos internos StorageGRID".

   > Esta opción elimina algunas protecciones para los servicios internos. Déjelo desactivado si es posible.

4. Seleccione **Guardar**.

Gestione el acceso externo

Cuando se cierra un puerto en la pestaña Administrar acceso externo, ninguna dirección IP que no sea de grid puede acceder al puerto a menos que agregue la dirección IP a la lista de direcciones con privilegios. Solo puede cerrar los puertos que están abiertos de forma predeterminada y sólo puede abrir los puertos que haya cerrado.

> La configuración de la pestaña Administrar acceso externo no puede sustituir la configuración de la pestaña Red de cliente no confiable. Por ejemplo, si un nodo no es de confianza, el puerto SSH/22 se bloquea en la red cliente incluso si está abierto en la pestaña Gestionar acceso externo. La configuración de la pestaña Red de cliente no confiable anula los puertos cerrados (como 443, 8443, 9443) en la red cliente.

Pasos

1. Selecciona **Administrar acceso externo**.
   El separador muestra una tabla con todos los puertos externos (puertos a los que pueden acceder los nodos que no son de cuadrícula por defecto) para los nodos de la cuadrícula.
2. Configure los puertos que desea abrir y cerrar mediante las siguientes opciones:
   - Utilice la palanca situada junto a cada puerto para abrir o cerrar el puerto seleccionado.
   - Seleccione **Abrir todos los puertos mostrados** para abrir todos los puertos enumerados en la tabla.

- Seleccione **Cerrar todos los puertos mostrados** para cerrar todos los puertos enumerados en la tabla.

> Si cierra los puertos 443 o 8443 de Grid Manager, cualquier usuario conectado actualmente a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones con privilegios.

> Utilice la barra de desplazamiento situada a la derecha de la tabla para asegurarse de que ha visto todos los puertos disponibles. Utilice el campo de búsqueda para buscar la configuración de cualquier puerto externo introduciendo un número de puerto. Puede introducir un número de puerto parcial. Por ejemplo, si introduce un **2**, se mostrarán todos los puertos que tengan la cadena "2" como parte de su nombre.

3. Seleccione **Guardar**

Red cliente no confiable

Si la red cliente de un nodo no es de confianza, el nodo solo acepta el tráfico entrante en los puertos configurados como puntos finales de equilibrio de carga y, opcionalmente, los puertos adicionales que seleccione en esta pestaña. También puede usar esta pestaña para especificar la configuración predeterminada para los nuevos nodos agregados en una expansión.

> Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Los cambios de configuración que realice en la pestaña **Red de clientes sin confianza** anulan la configuración de la pestaña **Administrar acceso externo**.

Pasos

1. Seleccione **Red cliente no confiable**.
2. En la sección Definir Nuevo Nodo por Defecto, especifique cuál debe ser el valor por defecto cuando se agregan nuevos nodos a la cuadrícula en un procedimiento de expansión.

   - **De confianza** (por defecto): Cuando se agrega un nodo en una expansión, su red cliente es de confianza.
   - **No fiable**: Cuando se agrega un nodo en una expansión, su red cliente no es de confianza.

     Según sea necesario, puede volver a esta pestaña para cambiar la configuración de un nuevo nodo específico.

   > Esta configuración no afecta a los nodos existentes del sistema StorageGRID.

3. Utilice las siguientes opciones para seleccionar los nodos que deben permitir conexiones de cliente solo en puntos finales del equilibrador de carga configurados explícitamente o puertos seleccionados adicionales:

   - Seleccione **Untrust on Visualized Nodes** para agregar todos los nodos mostrados en la tabla a la lista Untrusted Client Network.
   - Seleccione **Confiar en los nodos mostrados** para eliminar todos los nodos mostrados en la tabla de la lista Red de clientes sin confianza.

◦ Utilice el conmutador situado junto a cada nodo para establecer la red cliente como de confianza o no de confianza para el nodo seleccionado.

Por ejemplo, puede seleccionar **Untrust on displayed nodes** para agregar todos los nodos a la lista Untrusted Client Network y, a continuación, usar el conmutador junto a un nodo individual para agregar ese nodo a la lista Trusted Client Network.

> Use la barra de desplazamiento en la parte derecha de la tabla para asegurarse de que ha visto todos los nodos disponibles. Utilice el campo de búsqueda para encontrar la configuración de cualquier nodo introduciendo el nombre del nodo. Puede introducir un nombre parcial. Por ejemplo, si introduce un **GW**, se mostrarán todos los nodos que tengan la cadena “GW” como parte de su nombre.

4. Seleccione **Guardar**.

La nueva configuración del firewall se aplica y aplica inmediatamente. Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Gestione inquilinos

Gestionar inquilinos: Información general

Como administrador de grid, debe crear y gestionar las cuentas de inquilino que utilizan los clientes S3 y Swift para almacenar y recuperar objetos.

> Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.

¿Qué son las cuentas de inquilinos?

Una cuenta de inquilino permite usar la API DE REST de simple Storage Service (S3) o la API DE REST de Swift para almacenar y recuperar objetos en un sistema StorageGRID.

Cada cuenta de inquilino tiene grupos locales o federados, usuarios, bloques de S3 o contenedores Swift y objetos.

Las cuentas de arrendatario se pueden utilizar para segregar objetos almacenados por diferentes entidades. Por ejemplo, pueden utilizarse varias cuentas de inquilino en cualquiera de estos casos de uso:

- **Caso de uso empresarial:** Si administra un sistema StorageGRID en una aplicación empresarial, es posible que desee segregar el almacenamiento de objetos de la red por los diferentes departamentos de la organización. En este caso, podría crear cuentas de inquilino para el departamento de marketing, el departamento de soporte al cliente, el departamento de recursos humanos, etc.

  > Si utiliza el protocolo de cliente S3, puede utilizar bloques S3 y políticas de bloques para segregar objetos entre los departamentos de una empresa. No es necesario utilizar cuentas de inquilino. Consulte las instrucciones de implementación "Bloques de S3 y políticas de bloques" si quiere más información.

- **Caso de uso del proveedor de servicios:** Si administra un sistema StorageGRID como proveedor de servicios, puede segregar el almacenamiento de objetos de la red por las diferentes entidades que alquile el almacenamiento en la red. En este caso, creará cuentas de inquilino para la empresa A, la empresa B,

la empresa C, etc.

Para obtener más información, consulte "Usar una cuenta de inquilino".

¿Cómo se crea una cuenta de inquilino?

Al crear una cuenta de inquilino, especifique la siguiente información:

- Información básica, incluido el nombre del inquilino, el tipo de cliente (S3 o Swift) y la cuota de almacenamiento opcional.
- Permisos para la cuenta de inquilino, como si la cuenta de inquilino puede usar los servicios de la plataforma S3, configurar su propio origen de identidad, usar S3 Select o usar una conexión de federación de grid.
- Acceso raíz inicial para el inquilino, basado en si el sistema StorageGRID utiliza usuarios y grupos locales, federación de identidades o inicio de sesión único (SSO).

Además, puede habilitar la configuración Bloqueo de objetos S3 para el sistema StorageGRID si las cuentas de arrendatario S3 necesitan cumplir con los requisitos normativos. Cuando se habilita el bloqueo de objetos S3, todas las cuentas de inquilinos S3 pueden crear y gestionar bloques conforme a la normativa.

¿Para qué se utiliza el gestor de inquilinos?

Después de crear la cuenta de inquilino, los usuarios de inquilino pueden iniciar sesión en el Administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidad se comparta con la cuadrícula)
- Gestionar grupos y usuarios
- Utilice la federación de grid para la clonación de cuentas y la replicación entre grid
- Gestión de claves de acceso de S3
- Cree y gestione bloques de S3
- Utilice los servicios de la plataforma S3
- Utilice S3 Select
- Supervise el uso del almacenamiento

Mientras que los usuarios inquilinos de S3 pueden crear y gestionar la clave de acceso y los depósitos S3 con el administrador de inquilinos, deben usar una aplicación cliente S3 para ingerir y gestionar objetos. Consulte "USE LA API DE REST DE S3" para obtener más detalles.

Los usuarios de Swift deben tener el permiso de acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso de acceso raíz no permite que los usuarios se autentiquen en la API DE REST de Swift para crear contenedores y procesar objetos. Los usuarios deben tener el permiso de administrador de Swift para autenticarse en la API DE REST de Swift.

Cree una cuenta de inquilino

Debe crear al menos una cuenta de inquilino para controlar el acceso al almacenamiento en su sistema de StorageGRID.

Los pasos para crear una cuenta de inquilino varían en función de si "federación de identidades" y.. "inicio de sesión único" Están configurados y si la cuenta de Grid Manager que utiliza para crear la cuenta de arrendatario pertenece a un grupo de administración con el permiso acceso raíz.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Acceso raíz o cuentas de inquilino".
- Si la cuenta de arrendatario utilizará el origen de identidad configurado para el Administrador de grid y desea otorgar permiso de acceso raíz para la cuenta de arrendatario a un grupo federado, ha importado ese grupo federado en el Gestor de grid. No es necesario asignar ningún permiso de Grid Manager a este grupo de administración. Consulte "Gestione los grupos de administradores".
- Si desea permitir que un inquilino de S3 clone los datos de su cuenta y replique objetos de bucket en otro grid mediante una conexión de federación de grid:
  - Ya tienes "se ha configurado la conexión de federación de grid".
  - El estado de la conexión es **Conectado**.
  - Tiene permiso de acceso raíz.
  - Ha revisado las consideraciones de "gestionar los inquilinos permitidos para la federación de grid".
  - Si la cuenta de arrendatario utilizará el origen de identidad configurado para Grid Manager, ha importado el mismo grupo federado en Grid Manager en ambas cuadrículas.

    Al crear el inquilino, seleccionará este grupo para que tenga el permiso inicial de acceso raíz para las cuentas de inquilino de origen y de destino.

> Si este grupo de administración no existe en ambas cuadrículas antes de crear el arrendatario, el arrendatario no se replica en el destino.

Acceda al asistente

Pasos

1. Seleccione **ARRENDATARIOS**.
2. Seleccione **Crear**.

Introduzca los detalles

Pasos

1. Introduzca los detalles del arrendatario.

Campo	Descripción
Nombre	Un nombre para la cuenta de inquilino. Los nombres de inquilinos no necesitan ser únicos. Cuando se crea la cuenta de inquilino, recibe un ID de cuenta único de 20 dígitos.

Campo	Descripción
Descripción (opcional)	Descripción para ayudar a identificar al inquilino. Si va a crear un inquilino que utilizará una conexión de federación de grid, opcionalmente, utilice este campo para ayudar a identificar cuál es el inquilino de origen y cuál es el inquilino de destino. Por ejemplo, esta descripción para un inquilino creado en Grid 1 también aparecerá para el inquilino replicado en Grid 2: «Este inquilino se creó en Grid 1».
Tipo de cliente	El tipo de protocolo de cliente que usará este inquilino, ya sea **S3** o **Swift**. **Nota**: El soporte para aplicaciones cliente Swift ha sido obsoleto y será eliminado en una versión futura.
Cuota de almacenamiento (opcional)	Si desea que este inquilino tenga una cuota de almacenamiento, un valor numérico para la cuota y las unidades.

2. Seleccione **continuar**.

Seleccione permisos

Pasos

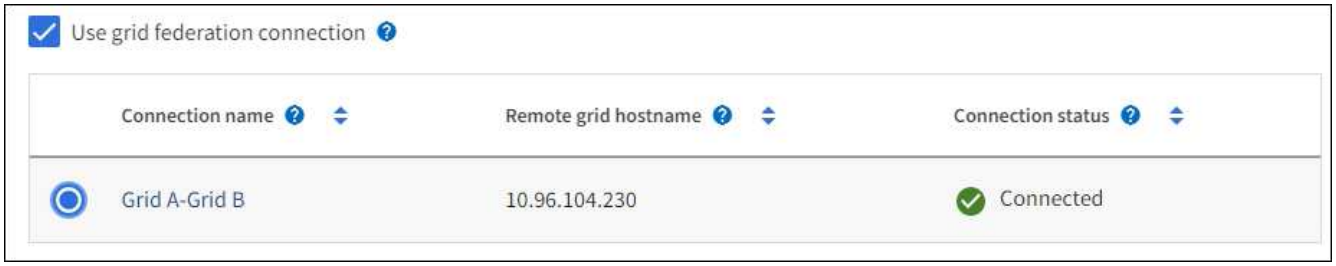
1. Opcionalmente, seleccione cualquier permiso que desee que tenga este inquilino.

> Algunos de estos permisos tienen requisitos adicionales. Para obtener más información, seleccione el icono de ayuda de cada permiso.

Permiso	Si se ha seleccionado…
Permitir los servicios de plataforma	El inquilino puede usar servicios de plataforma S3 como CloudMirror. Consulte "Gestione servicios de plataformas para cuentas de inquilinos de S3".
Usar origen de identidad propio	El inquilino puede configurar y gestionar su propio origen de identidad para usuarios y grupos federados. Esta opción está desactivada si tiene "SSO configurado" Para su sistema StorageGRID.
Permitir selección S3	El inquilino puede emitir solicitudes de API S3 SelectObjectContent para filtrar y recuperar datos de objetos. Consulte "Gestione S3 Select para cuentas de inquilinos". **Importante**: Las solicitudes de SelectObjectContent pueden disminuir el rendimiento del equilibrador de carga para todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.

Permiso	Si se ha seleccionado…
Utilizar conexión de federación de grid	El inquilino puede utilizar una conexión de federación de grid. Seleccionando esta opción: • Hace que este arrendatario y todos los grupos de arrendatarios y usuarios agregados a la cuenta se clonen desde esta cuadrícula (la cuadrícula *source*) a la otra cuadrícula de la conexión seleccionada (la cuadrícula *destination*). • Permite a este inquilino configurar la replicación entre grid entre bloques correspondientes en cada grid. Consulte "Gestione los inquilinos permitidos para la federación de grid".

2. Si seleccionó **Usar conexión de federación de grid**, seleccione una de las conexiones de federación de grid disponibles.



3. Seleccione **continuar**.

Defina el acceso raíz y cree un inquilino

Pasos

1. Defina el acceso raíz para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza la federación de identidades, el inicio de sesión único (SSO) o ambos.

Opción	Haga esto
Si la federación de identidades no está activada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidades está activada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si se activan tanto la federación de identidades como el inicio de sesión único (SSO)	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

2. Seleccione **Crear arrendatario**.

Aparece un mensaje Correcto y el nuevo arrendatario aparece en la página Inquilinos. Para saber cómo

se ven los detalles de los inquilinos y se supervisa la actividad de los inquilinos, consulte "Supervise la actividad de los inquilinos".

3. Si seleccionó el permiso **Usar conexión de federación de grid** para el inquilino:
   a. Confirme que se ha replicado un inquilino idéntico en la otra cuadrícula de la conexión. Los inquilinos de ambas cuadrículas tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos.

      Si ve el mensaje de error «El inquilino se creó sin un clon», consulte las instrucciones de "Solucionar errores de federación de grid".

   b. Si proporcionó una contraseña de usuario raíz local al definir el acceso raíz, "cambie la contraseña del usuario raíz local" para el inquilino replicado.

      Un usuario raíz local no puede iniciar sesión en el gestor de inquilinos en la cuadrícula de destino hasta que se cambie la contraseña.

Iniciar sesión en el inquilino (opcional)

Según sea necesario, puede iniciar sesión en el nuevo inquilino ahora para completar la configuración, o puede iniciar sesión en el inquilino más adelante. Los pasos de inicio de sesión dependen de si ha iniciado sesión en Grid Manager mediante el puerto predeterminado (443) o un puerto restringido. Consulte "Controle el acceso a un firewall externo".

Inicie sesión ahora

Si está usando…	Realice lo siguiente…
Puerto 443 y se establece una contraseña para el usuario raíz local	1. Seleccione **Iniciar sesión como root**. Al iniciar sesión, aparecen enlaces para configurar buckets, federación de identidades, grupos y usuarios. 2. Seleccione los vínculos para configurar la cuenta de arrendatario. Cada enlace abre la página correspondiente en el Administrador de arrendatarios. Para completar la página, consulte "instrucciones para el uso de cuentas de inquilino".
Puerto 443 y no ha establecido una contraseña para el usuario raíz local	Seleccione **Iniciar sesión** e introduzca las credenciales de un usuario en el grupo federado de acceso raíz.

Si está usando…	Realice lo siguiente…
Un puerto restringido	1. Selecciona **Finalizar** 2. Seleccione **Restringido** en la tabla de arrendatarios para obtener más información sobre el acceso a esta cuenta de arrendatario. La dirección URL del administrador de inquilinos tiene el siguiente formato: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* Es un nombre de dominio completo o la dirección IP de un nodo de administrador ◦ *port* es el puerto de solo inquilino ◦ *20-digit-account-id* Es el ID de cuenta único del inquilino

Inicie sesión más tarde

Si está usando…	Realice una de estas…
Puerto 443	• En Grid Manager, seleccione **ARRENDATARIOS** y seleccione **Iniciar sesión** a la derecha del nombre del arrendatario. • Introduzca la URL del inquilino en un navegador web: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* Es un nombre de dominio completo o la dirección IP de un nodo de administrador ◦ *20-digit-account-id* Es el ID de cuenta único del inquilino
Un puerto restringido	• En Grid Manager, seleccione **ARRENDATARIOS** y seleccione **restringido**. • Introduzca la URL del inquilino en un navegador web: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* Es un nombre de dominio completo o la dirección IP de un nodo de administrador ◦ *port* es el puerto restringido solo para inquilinos ◦ *20-digit-account-id* Es el ID de cuenta único del inquilino

Configure el inquilino

Siga las instrucciones de "Usar una cuenta de inquilino" Para gestionar usuarios y grupos de inquilinos, claves de acceso S3, bloques, servicios de plataforma, y clonación de cuentas y replicación entre grid.

Edite la cuenta de inquilino

Una cuenta de inquilino se puede editar para cambiar el nombre para mostrar, la cuota de almacenamiento o los permisos de inquilino.

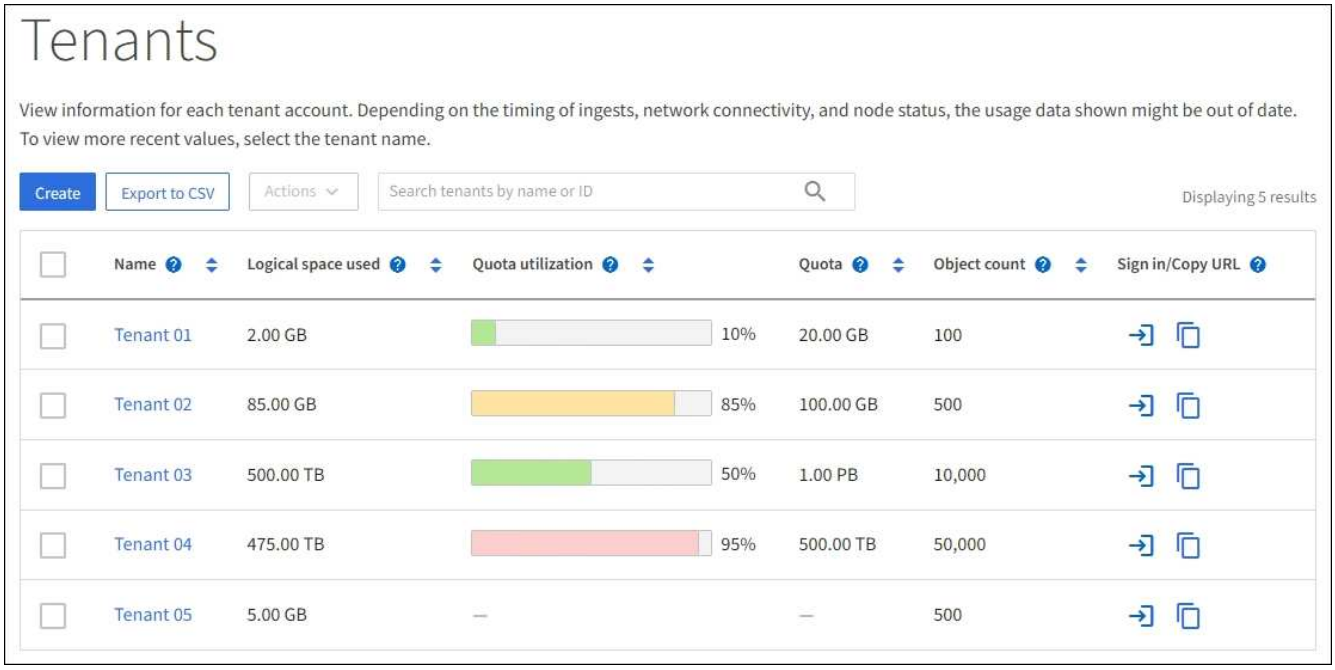
> Si un inquilino tiene el permiso **Usar conexión de federación de grid**, puede editar los detalles del inquilino desde cualquier cuadrícula en la conexión. Sin embargo, los cambios que realice en una cuadrícula de la conexión no se copiarán en la otra cuadrícula. Si desea mantener los detalles del arrendatario exactamente sincronizados entre las cuadrículas, realice las mismas modificaciones en ambas cuadrículas. Consulte "Gestione los inquilinos permitidos para la conexión de federación de grid".

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Acceso raíz o cuentas de inquilino".

Pasos

1. Seleccione **ARRENDATARIOS**.



2. Localice la cuenta de inquilino que desea editar.

   Utilice el cuadro de búsqueda para buscar un inquilino por nombre o ID de inquilino.

3. Seleccione el inquilino. Puede realizar una de las siguientes acciones:
   - Selecciona la casilla de verificación para el inquilino y selecciona **Acciones** > **Editar**.
   - Seleccione el nombre del inquilino para mostrar la página de detalles y seleccione **Editar**.
4. Si lo desea, cambie los valores de estos campos:
   - **Nombre**
   - **Descripción**
   - **Cuota de almacenamiento**

5. Seleccione **continuar**.
6. Seleccione o borre los permisos para la cuenta de inquilino.
   - Si deshabilita **Servicios de plataforma** para un arrendatario que ya los está utilizando, los servicios que han configurado para sus cubos S3 dejarán de funcionar. No se envía ningún mensaje de error al inquilino. Por ejemplo, si el inquilino ha configurado la replicación de CloudMirror para un bloque de S3, podrán seguir almacenando objetos en el bloque, pero las copias de esos objetos ya no se realizarán en el bloque S3 externo que se hayan configurado como extremo. Consulte "Gestione servicios de plataformas para cuentas de inquilinos de S3".
   - Cambie la configuración de **Uses own identity source** para determinar si la cuenta de inquilino utilizará su propia fuente de identidad o la fuente de identidad que se configuró para Grid Manager.

     Si **usa su propia fuente de identidad** es:

     - Desactivado y seleccionado, el arrendatario ya ha activado su propio origen de identidad. Un arrendatario debe desactivar su origen de identidad antes de poder utilizar el origen de identidad configurado para el Gestor de cuadrícula.
     - Desactivado y no seleccionado, SSO está activado para el sistema StorageGRID. El inquilino debe utilizar el origen de identidad configurado para el administrador de grid.
   - Seleccione o desactive el permiso **Permitir S3 Select** según sea necesario. Consulte "Gestione S3 Select para cuentas de inquilinos".
   - Para eliminar el permiso **Use grid federation connection**:
     i. Vaya a la página de detalles del inquilino.
     ii. Seleccione la pestaña **Grid federation**.
     iii. Selecciona **Eliminar permiso**.
   - Para agregar el permiso **Use grid federation connection**:
     i. Seleccione la casilla de verificación **Usar conexión de federación de cuadrícula**.
     ii. Opcionalmente, seleccione **Clonar usuarios y grupos locales existentes** para clonarlos a la cuadrícula remota. Si desea, puede detener la clonado en curso o volver a intentar la clonado si no se pudieron clonar algunos usuarios o grupos locales después de completar la última operación de clonado.

Cambiar la contraseña del usuario raíz local del inquilino

Puede que necesite cambiar la contraseña del usuario raíz local de un inquilino si el usuario raíz está bloqueado en la cuenta.

Antes de empezar

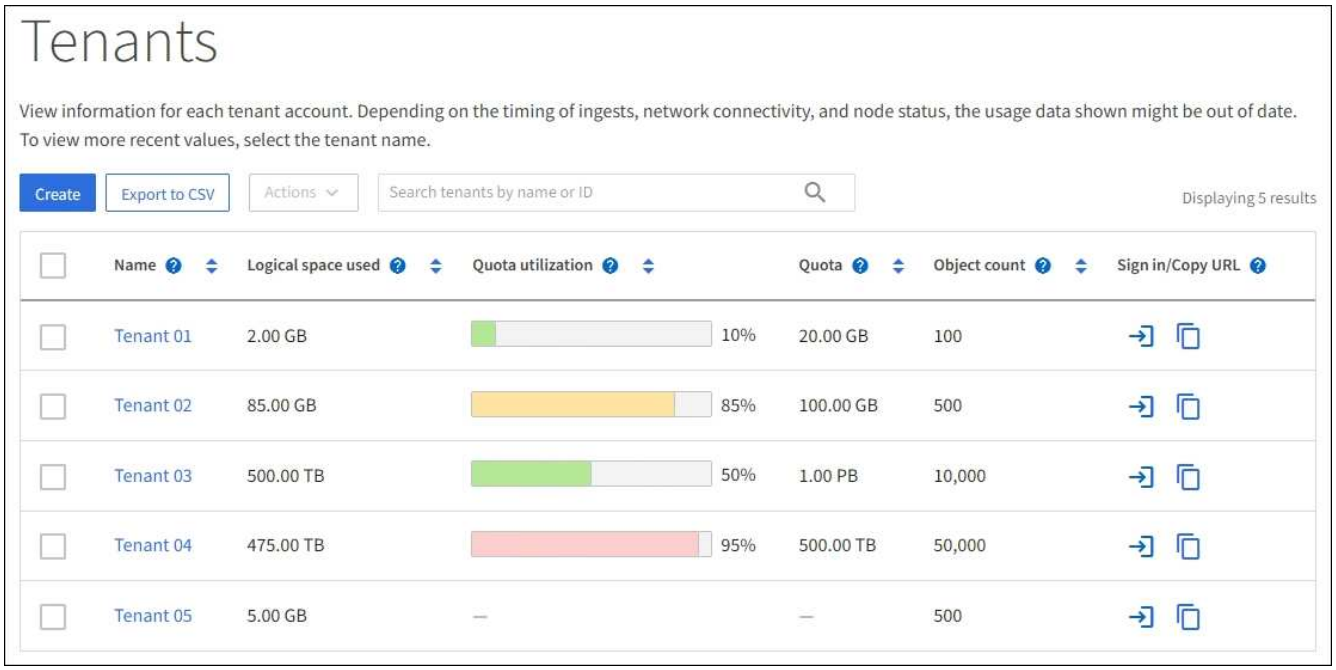
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".

Acerca de esta tarea

Si está habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, el usuario raíz local no puede iniciar sesión en la cuenta de inquilino. Para realizar tareas de usuario raíz, los usuarios deben pertenecer a un grupo federado que tenga el permiso acceso raíz para el arrendatario.

Pasos

1. Seleccione **ARRENDATARIOS**.



2. Seleccione la cuenta de inquilino. Puede realizar una de las siguientes acciones:
   - Selecciona la casilla de verificación para el inquilino y selecciona **Acciones** > **Cambiar contraseña raíz**.
   - Seleccione el nombre del inquilino para mostrar la página de detalles y seleccione **Acciones** > **Cambiar contraseña raíz**.
3. Introduzca la nueva contraseña de la cuenta de inquilino.
4. Seleccione **Guardar**.

Eliminar cuenta de inquilino

Puede eliminar una cuenta de inquilino si desea eliminar de forma permanente el acceso del inquilino al sistema.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Quitó todos los bloques (S3), los contenedores (Swift) y los objetos asociados con la cuenta de inquilino.
- Si el inquilino puede usar una conexión de federación de grid, ha revisado las consideraciones para "Eliminación de un inquilino con el permiso de conexión Usar federación de grid".

Pasos

1. Seleccione **ARRENDATARIOS**.
2. Localice la cuenta de inquilino o las cuentas que desea eliminar.

   Utilice el cuadro de búsqueda para buscar un inquilino por nombre o ID de inquilino.
3. Para eliminar varios inquilinos, selecciona las casillas de verificación y selecciona **Acciones** > **Eliminar**.
4. Para suprimir un solo inquilino, realice una de las siguientes acciones:
   - Selecciona la casilla de verificación y selecciona **Acciones** > **Eliminar**.

- Seleccione el nombre del inquilino para mostrar la página de detalles y, a continuación, seleccione * Acciones * > * Eliminar *.

5. Seleccione **Sí**.

Gestione los servicios de la plataforma

Gestionar servicios de plataforma para inquilinos: Información general

Si habilita los servicios de plataforma para cuentas de inquilino de S3, debe configurar su grid para que los inquilinos puedan acceder a los recursos externos necesarios para usar estos servicios.

¿Qué son los servicios de plataforma?

Los servicios de plataforma incluyen la replicación de CloudMirror, las notificaciones de eventos y el servicio de integración de búsqueda.

Replicación de CloudMirror

El servicio de replicación de CloudMirror de StorageGRID se usa para reflejar objetos concretos desde un bloque de StorageGRID en un destino externo especificado.

Por ejemplo, podría usar la replicación de CloudMirror para reflejar registros de clientes específicos en Amazon S3 y, a continuación, aprovechar los servicios de AWS para realizar análisis de los datos.

> La replicación de CloudMirror tiene algunas similitudes y diferencias importantes con la función de replicación entre redes. Para obtener más información, consulte "Compare la replicación entre grid y la replicación de CloudMirror".

> La replicación de CloudMirror no es compatible si el bloque de origen tiene la función S3 Object Lock habilitada.

Notificaciones

Las notificaciones de eventos por bloque se utilizan para enviar notificaciones sobre acciones específicas realizadas en objetos a un clúster Kafka externo especificado o a Amazon Simple Notification Service.

Por ejemplo, podría configurar que se envíen alertas a administradores acerca de cada objeto agregado a un bloque, donde los objetos representan los archivos de registro asociados a un evento crítico del sistema.

> Aunque la notificación de eventos se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos S3 (incluido el estado retener hasta fecha y retención legal) de los objetos no se incluirán en los mensajes de notificación.

Servicio de integración de búsqueda

El servicio de integración de búsqueda se utiliza para enviar metadatos de objetos S3 a un índice de Elasticsearch especificado en el que se pueden buscar o analizar los metadatos mediante el servicio externo.

Por ejemplo, podría configurar sus bloques para que envíen metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, podría usar Elasticsearch para realizar búsquedas en los bloques y ejecutar análisis sofisticados de los patrones presentes en los metadatos de objetos.

Aunque la integración de Elasticsearch se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos de S3 (incluidos los Estados Retain Until Date and Legal Hold) de los objetos no se incluirán en los mensajes de notificación.

Los servicios de plataforma ofrecen a los inquilinos la capacidad de usar recursos de almacenamiento externo, servicios de notificación y servicios de búsqueda o análisis con sus datos. Puesto que la ubicación objetivo para los servicios de plataforma suele ser externa a la implementación de StorageGRID, debe decidir si desea permitir a los inquilinos utilizar estos servicios. Si lo hace, debe habilitar el uso de servicios de plataforma al crear o editar cuentas de inquilino. También debe configurar la red de modo que los mensajes de servicios de plataforma que generan los inquilinos puedan llegar a sus destinos.

Recomendaciones para el uso de servicios de plataformas

Antes de utilizar los servicios de plataforma, tenga en cuenta las siguientes recomendaciones:

- Si un bloque de S3 del sistema StorageGRID tiene habilitadas las versiones y la replicación de CloudMirror, también debe habilitar el control de versiones de bloques de S3 para el extremo de destino. Esto permite que la replicación de CloudMirror genere versiones de objetos similares en el extremo.
- No debe usar más de 100 inquilinos activos con solicitudes S3 que requieran la replicación, las notificaciones y la integración de búsqueda de CloudMirror. Tener más de 100 inquilinos activos puede dar como resultado un rendimiento del cliente S3 más lento.
- Las solicitudes a un punto final que no se puedan completar se pondrán en cola a un máximo de 500.000 solicitudes. Este límite se comparte por igual entre los inquilinos activos. Los nuevos inquilinos pueden exceder temporalmente este límite de 500.000 para que los nuevos inquilinos no sean penalizados injustamente.

Información relacionada

- "Gestione los servicios de la plataforma"
- "Configure las opciones de proxy de almacenamiento"
- "Supervisar StorageGRID"

Red y puertos para servicios de plataforma

Si permite que un inquilino de S3 utilice los servicios de plataforma, debe configurar las redes para el grid para garantizar que los mensajes de servicios de plataforma se puedan entregar a sus destinos.

Puede habilitar los servicios de plataforma para una cuenta de inquilino de S3 al crear o actualizar la cuenta de inquilino. Si se habilitan los servicios de plataforma, el inquilino puede crear extremos que sirvan como destino para la replicación de CloudMirror, notificaciones de eventos o mensajes de integración de búsqueda desde sus bloques de S3. Estos mensajes de servicios de plataforma se envían desde los nodos de almacenamiento que ejecutan el servicio ADC a los extremos de destino.

Por ejemplo, los inquilinos pueden configurar los siguientes tipos de extremos de destino:

- Un clúster de Elasticsearch alojado localmente
- Una aplicación local que admite la recepción de mensajes de Amazon Simple Notification Service
- Un clúster Kafka alojado localmente
- Un bloque de S3 alojado localmente en la misma instancia de StorageGRID u otra

- Un extremo externo, como un extremo en Amazon Web Services.

Para garantizar que los mensajes de servicios de plataforma se puedan entregar, debe configurar la red o las redes que contienen los nodos de almacenamiento ADC. Debe asegurarse de que se pueden utilizar los siguientes puertos para enviar mensajes de servicios de plataforma a los extremos de destino.

De forma predeterminada, los mensajes de servicios de plataforma se envían a los siguientes puertos:

- **80**: Para URI de punto final que comienzan con http (la mayoría de los puntos finales)
- **443**: Para URI de punto final que comienzan con https (la mayoría de los puntos finales)
- **9092**: Para URI de punto final que comienzan con http o https (solo puntos finales Kafka)

Los inquilinos pueden especificar un puerto diferente cuando crean o editan un extremo.

> Si se usa una puesta en marcha de StorageGRID como destino de la replicación de CloudMirror, podrían recibirse mensajes de replicación en un puerto distinto de 80 o 443. Compruebe que el puerto que se utiliza para S3 en la implementación de StorageGRID de destino se especifique en el extremo.

Si utiliza un servidor proxy no transparente, también debe hacerlo "configure las opciones del proxy de almacenamiento" para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

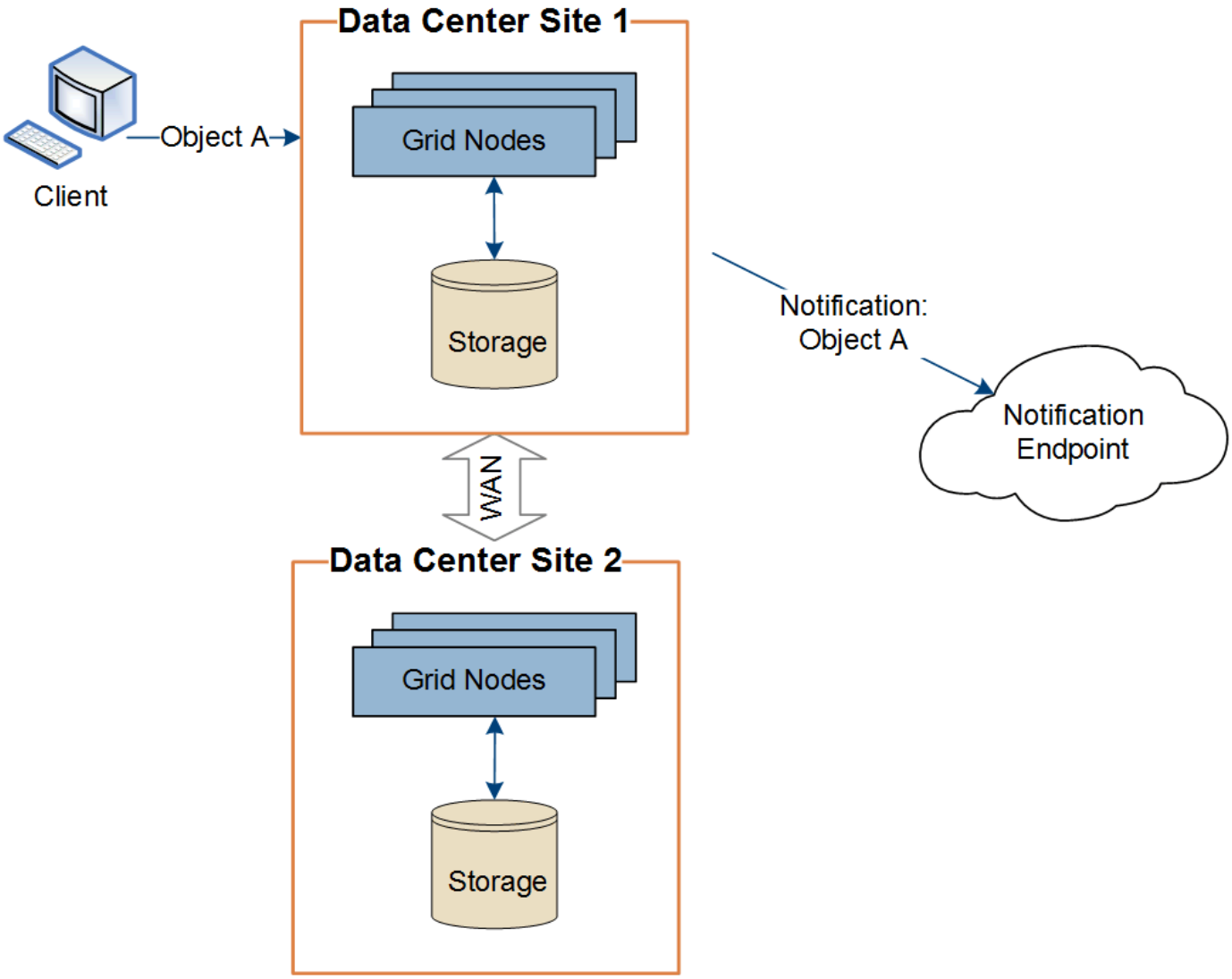
Información relacionada

- "Usar una cuenta de inquilino"

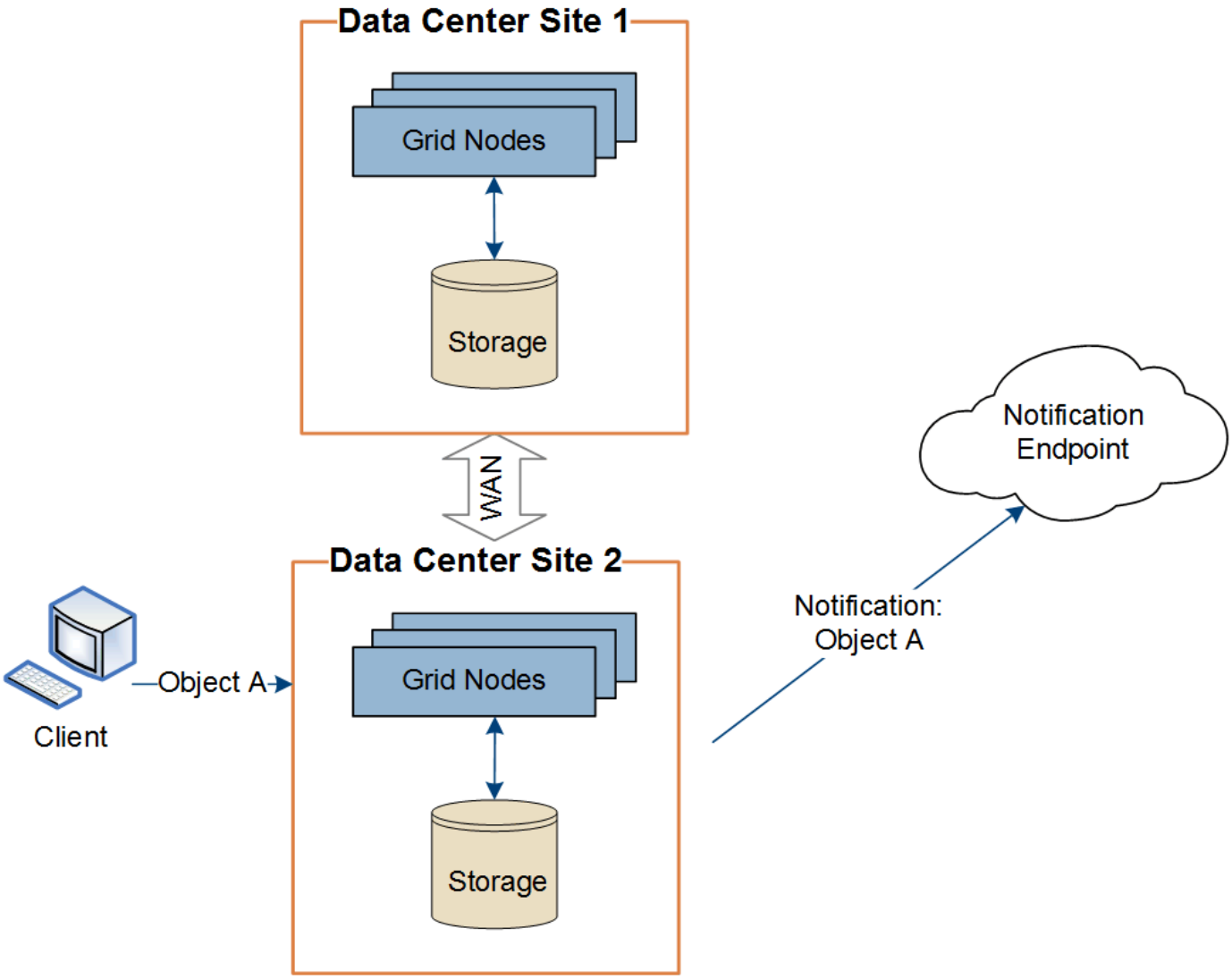
Entrega de mensajes de servicios de plataforma por sitio

Todas las operaciones de servicios de plataforma se realizan in situ.

Es decir, si un inquilino utiliza un cliente para realizar una operación S3 API Create en un objeto conectando a un nodo de puerta de enlace en el sitio 1 del centro de datos, se activa y envía la notificación acerca de esa acción desde el sitio 1 del centro de datos.



Si el cliente realiza posteriormente una operación de eliminación de API de S3 en ese mismo objeto desde el centro de datos Sitio 2, se activa y envía la notificación sobre la acción de eliminación desde el centro de datos Sitio 2.



Asegúrese de que la red de cada sitio esté configurada de modo que los mensajes de servicios de la plataforma se puedan entregar a sus destinos.

Solucione problemas de servicios de plataforma

Los extremos utilizados en los servicios de plataforma los crean y mantienen los usuarios de arrendatarios en el Administrador de arrendatarios; sin embargo, si un arrendatario tiene problemas al configurar o utilizar servicios de plataforma, puede utilizar el Administrador de grid para ayudar a resolver el problema.

Problemas con nuevos extremos

Para que un inquilino pueda utilizar los servicios de plataforma, deben crear uno o varios extremos mediante el administrador de inquilinos. Cada extremo representa un destino externo para un servicio de plataforma, como un bucket de StorageGRID S3, un bucket de Amazon Web Services, un tema del servicio de notificación simple de Amazon, un tema de Kafka o un clúster de Elasticsearch alojado localmente o en AWS. Cada extremo incluye la ubicación del recurso externo y las credenciales que se necesitan para acceder a ese recurso.

Cuando un inquilino crea un extremo, el sistema StorageGRID valida que existe el extremo y que se puede acceder a él utilizando las credenciales que se han especificado. La conexión con el extremo se valida desde

un nodo en cada sitio.

Si falla la validación del punto final, un mensaje de error explica por qué falló la validación del punto final. El usuario inquilino debe resolver el problema y, a continuación, intentar crear el extremo de nuevo.

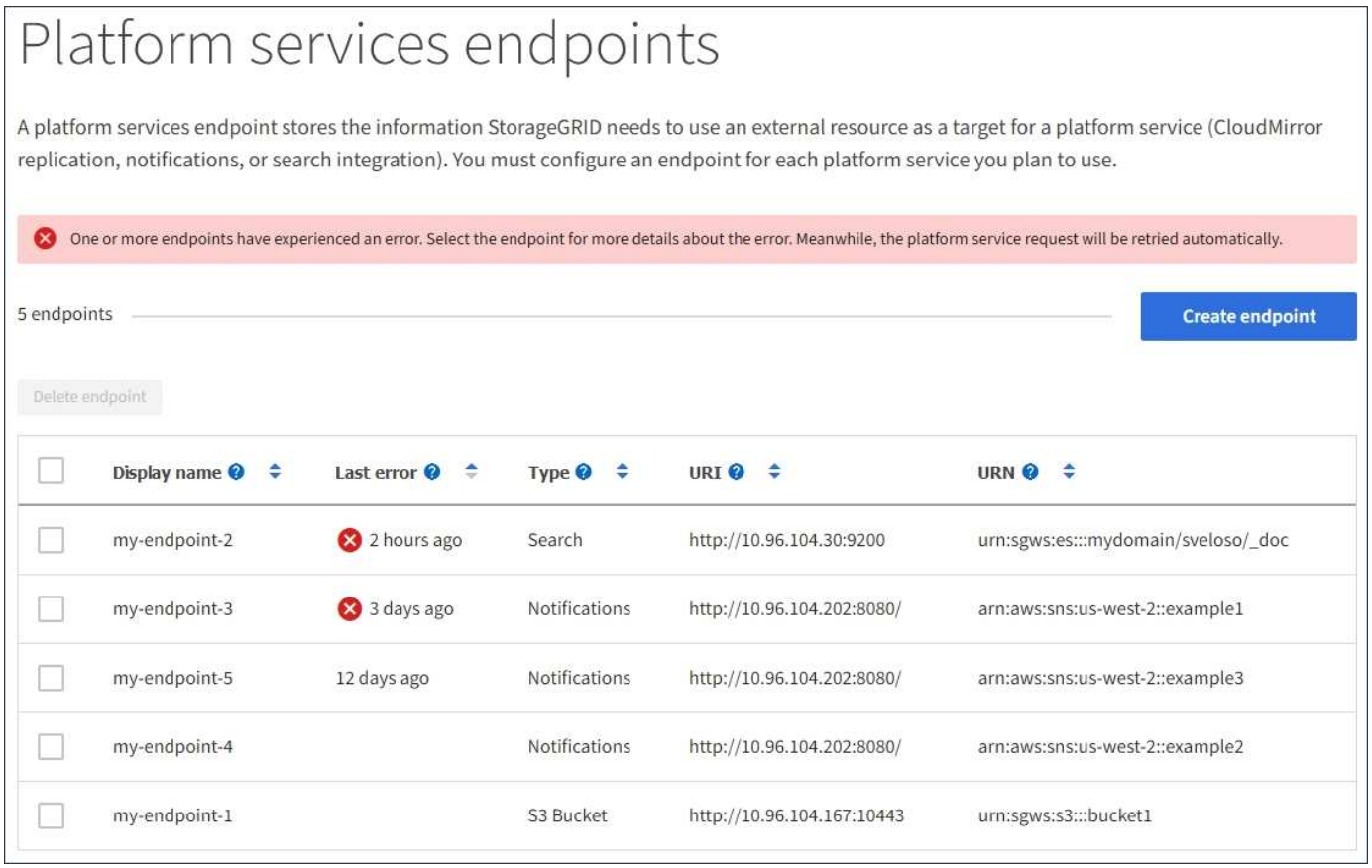
> La creación de punto final fallará si los servicios de plataforma no están activados para la cuenta de inquilino.

Problemas con los extremos existentes

Si se produce un error cuando StorageGRID intenta llegar a un punto final existente, se muestra un mensaje en el panel de control del gestor de inquilinos.

> One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

Los usuarios de arrendatarios pueden ir a la página endpoints para revisar el mensaje de error más reciente de cada extremo y determinar cuánto tiempo ha ocurrido el error. La columna **último error** muestra el mensaje de error más reciente para cada extremo e indica cuánto tiempo se produjo el error. Errores que incluyen el icono se ha producido en los últimos 7 días.



> Algunos mensajes de error en la columna **último error** pueden incluir un identificador de registro entre paréntesis. Un administrador de grid o soporte técnico puede usar este ID para encontrar información más detallada sobre el error en bycast.log.

Problemas relacionados con los servidores proxy

Si ha configurado un "proxy de almacenamiento" Entre los nodos de almacenamiento y los extremos del servicio de plataforma, se podrían producir errores si el servicio de proxy no permite mensajes de StorageGRID. Para resolver estos problemas, compruebe la configuración de su servidor proxy para asegurarse de que los mensajes relacionados con el servicio de la plataforma no estén bloqueados.

Determine si se ha producido un error

Si se ha producido algún error de punto final en los últimos 7 días, el panel de control del gestor de inquilinos muestra un mensaje de alerta. Puede ir a la página endpoints para ver más detalles sobre el error.

Error en las operaciones del cliente

Algunos problemas de los servicios de plataforma pueden provocar errores en las operaciones del cliente en el bloque de S3. Por ejemplo, las operaciones del cliente S3 fallarán si se detiene el servicio interno Replicated State Machine (RSM) o si hay demasiados mensajes de servicios de plataforma en cola para su entrega.

Para comprobar el estado de los servicios:

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > ***Storage Node*** > **SSM** > **Servicios**.

Errores de punto final recuperables e irrecuperables

Una vez creados los extremos, los errores de solicitud de servicio de la plataforma pueden producirse por varios motivos. Algunos errores se pueden recuperar con la intervención del usuario. Por ejemplo, pueden producirse errores recuperables por los siguientes motivos:

- Las credenciales del usuario se han eliminado o han caducado.
- El bloque de destino no existe.
- No se puede entregar la notificación.

Si StorageGRID encuentra un error recuperable, la solicitud de servicio de la plataforma se reintentará hasta que se complete correctamente.

Otros errores son irrecuperables. Por ejemplo, se produce un error irrecuperable si se elimina el extremo.

Si StorageGRID encuentra un error de punto final irrecuperable, la alarma heredada total de eventos (SMTT) se activa en el Administrador de grid. Para ver la alarma de legado total de eventos:

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > ***node*** > **SSM** > **Eventos**.
3. Ver último evento en la parte superior de la tabla.

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

4. Siga las instrucciones proporcionadas en el contenido de la alarma SMTT para corregir el problema.
5. Seleccione la ficha **Configuración** para restablecer los recuentos de eventos.
6. Notifique al inquilino los objetos cuyos mensajes de servicios de plataforma no se han entregado.

7. Indique al inquilino que vuelva a activar la replicación o notificación fallida actualizando los metadatos o las etiquetas del objeto.

   El arrendatario puede volver a enviar los valores existentes para evitar realizar cambios no deseados.

Los mensajes de servicios de plataforma no se pueden entregar

Si el destino encuentra un problema que le impide aceptar mensajes de servicios de plataforma, la operación de cliente en el bloque se realiza correctamente, pero el mensaje de servicios de plataforma no se entrega. Por ejemplo, este error puede ocurrir si se actualizan las credenciales en el destino de modo que StorageGRID ya no pueda autenticarse en el servicio de destino.

Si los mensajes de servicios de plataforma no se pueden entregar debido a un error irrecuperable, la alarma de legado de Total Events (SMTT) se activa en Grid Manager.

Rendimiento más lento para las solicitudes de servicio de la plataforma

El software StorageGRID puede reducir las solicitudes entrantes de S3 para un bloque si la velocidad a la que se envían las solicitudes supera la velocidad a la que el extremo de destino puede recibir las solicitudes. La limitación sólo se produce cuando hay una acumulación de solicitudes que están a la espera de ser enviadas al extremo de destino.

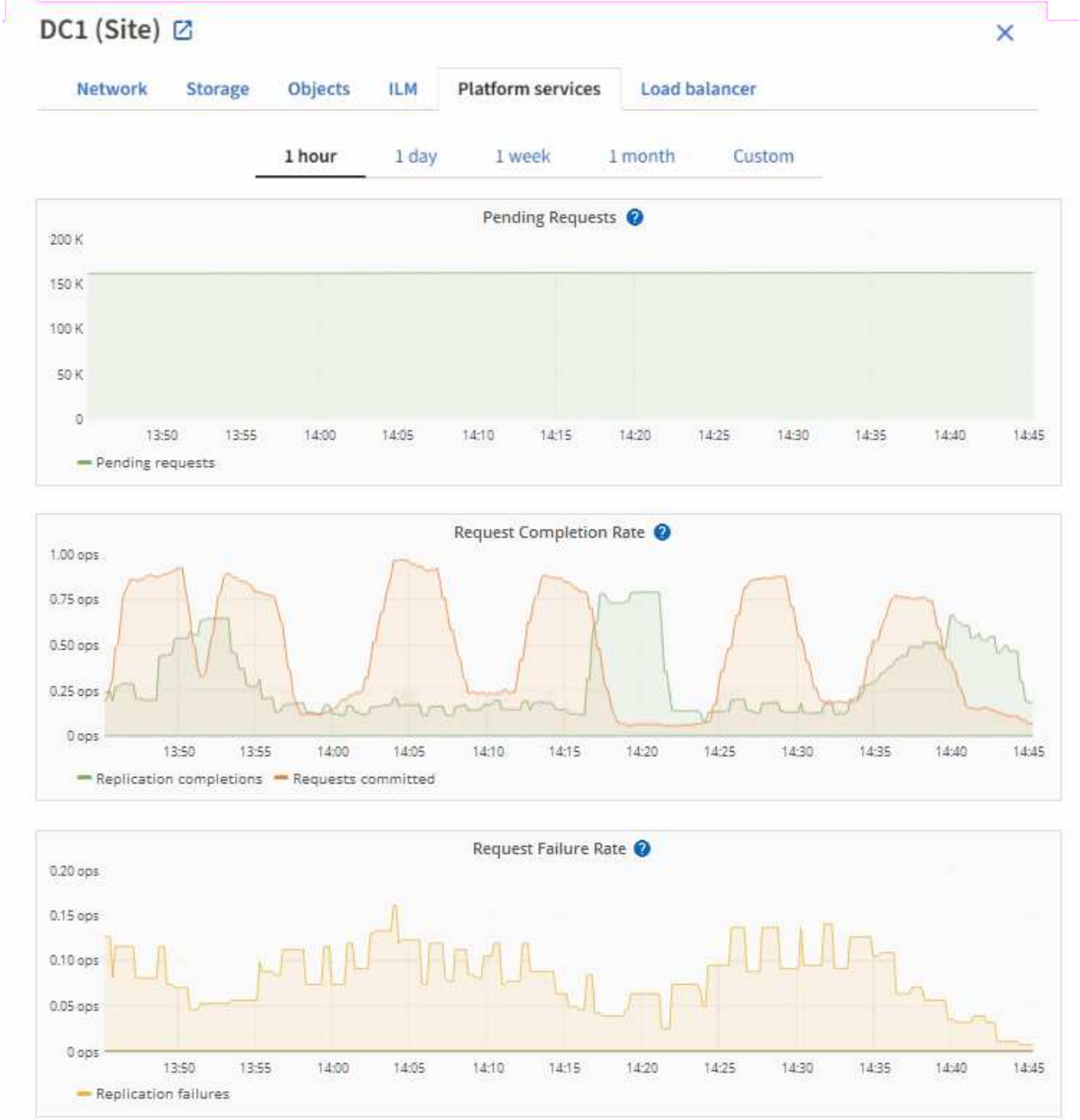
El único efecto visible es que las solicitudes entrantes de S3 tardarán más en ejecutarse. Si empieza a detectar un rendimiento significativamente más lento, debe reducir la tasa de procesamiento o utilizar un extremo con mayor capacidad. Si la acumulación de solicitudes sigue creciendo, las operaciones de S3 del cliente (como SOLICITUDES PUT) fallarán en el futuro.

Las solicitudes de CloudMirror tienen más probabilidades de que se vean afectadas por el rendimiento del extremo de destino, ya que estas solicitudes suelen requerir más transferencia de datos que las solicitudes de integración de búsqueda o notificación de eventos.

Las solicitudes de servicio de la plataforma fallan

Para ver la tasa de fallos de solicitud para servicios de plataforma:

1. Selecciona **NODOS**.
2. Seleccione ***site*** > **Servicios de plataforma**.
3. Vea el gráfico de tasa de errores de solicitud.



Alerta de servicios de plataforma no disponibles

La alerta **Servicios de plataforma no disponibles** indica que no se pueden realizar operaciones de servicio de plataforma en un sitio porque hay demasiados nodos de almacenamiento con el servicio RSM en ejecución o disponibles.

El servicio RSM garantiza que las solicitudes de servicio de la plataforma se envíen a sus respectivos extremos.

Para resolver esta alerta, determine qué nodos de almacenamiento del sitio incluyen el servicio RSM. (El servicio RSM está presente en los nodos de almacenamiento que también incluyen el servicio ADC). A continuación, asegúrese de que la mayoría simple de estos nodos de almacenamiento esté en funcionamiento y disponible.

Si se produce un error en más de un nodo de almacenamiento que contiene el servicio RSM de un sitio, perderá las solicitudes de servicio de plataforma pendientes para ese sitio.

Orientación adicional para la solución de problemas para extremos de servicios de la plataforma

Para obtener información adicional, consulte **Use una cuenta de inquilino › Solucionar problemas de los extremos de servicios de la plataforma**.

Información relacionada

- "Solucionar los problemas del sistema StorageGRID"

Gestione S3 Select para cuentas de inquilinos

Puede permitir que determinados inquilinos S3 usen S3 Select para emitir solicitudes SelectObjectContent en objetos individuales.

S3 Select proporciona una forma eficiente de buscar en grandes cantidades de datos sin tener que implementar una base de datos y recursos asociados para permitir las búsquedas. También reduce el coste y la latencia de la recuperación de datos.

¿Qué es S3 Select?

S3 Select permite que los clientes S3 utilicen solicitudes SelectObjectContent para filtrar y recuperar solo los datos necesarios de un objeto. La implementación de StorageGRID de S3 Select incluye un subconjunto de comandos y funciones de S3 Select.

Consideraciones y requisitos para usar S3 Select

Requisitos de administración de grid

El administrador de grid debe conceder a los inquilinos la Capacidad Select S3. Seleccione **permitir selección de S3** cuando "crear un inquilino" o. "edición de un arrendatario".

Requisitos de formato de objeto

El objeto que desea consultar debe tener uno de los siguientes formatos:

- **CSV**. Se puede utilizar tal cual o comprimir en archivos GZIP o bzip2.
- **Parquet**. Requisitos adicionales para objetos de parquet:
  - S3 Select solo admite la compresión en columnas usando GZIP o Snappy. S3 Select no admite la compresión de objetos completos para objetos de parquet.
  - S3 La selección no es compatible con la salida de parquet. Debe especificar el formato de salida como CSV o JSON.
  - El tamaño máximo del grupo de filas sin comprimir es de 512 MB.
  - Debe utilizar los tipos de dato especificados en el esquema del objeto.
  - No puede utilizar los tipos lógicos INTERVAL, JSON, LIST, TIME o UUID.

Requisitos de los extremos

La solicitud SelectObjectContent debe enviarse a un "Extremo del equilibrador de carga de StorageGRID".

Los nodos de administración y puerta de enlace utilizados por el punto final deben ser uno de los siguientes:

- Nodo de dispositivo SG100 o SG1000
- Nodo de software basado en VMware
- Nodo bare metal que ejecuta un kernel con cgroup v2 habilitado

Consideraciones generales

Las consultas no pueden enviarse directamente a los nodos de almacenamiento.

> Las solicitudes SelectObjectContent pueden reducir el rendimiento de equilibrio de carga de todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.

Consulte "Instrucciones para usar S3 Select".

Para ver "Gráficos Grafana" Para las operaciones de S3 Select a lo largo del tiempo, seleccione **SUPPORT** > **Tools** > **Metrics** en Grid Manager.

Configurar conexiones de cliente

Configurar las conexiones del cliente S3 y Swift: Información general

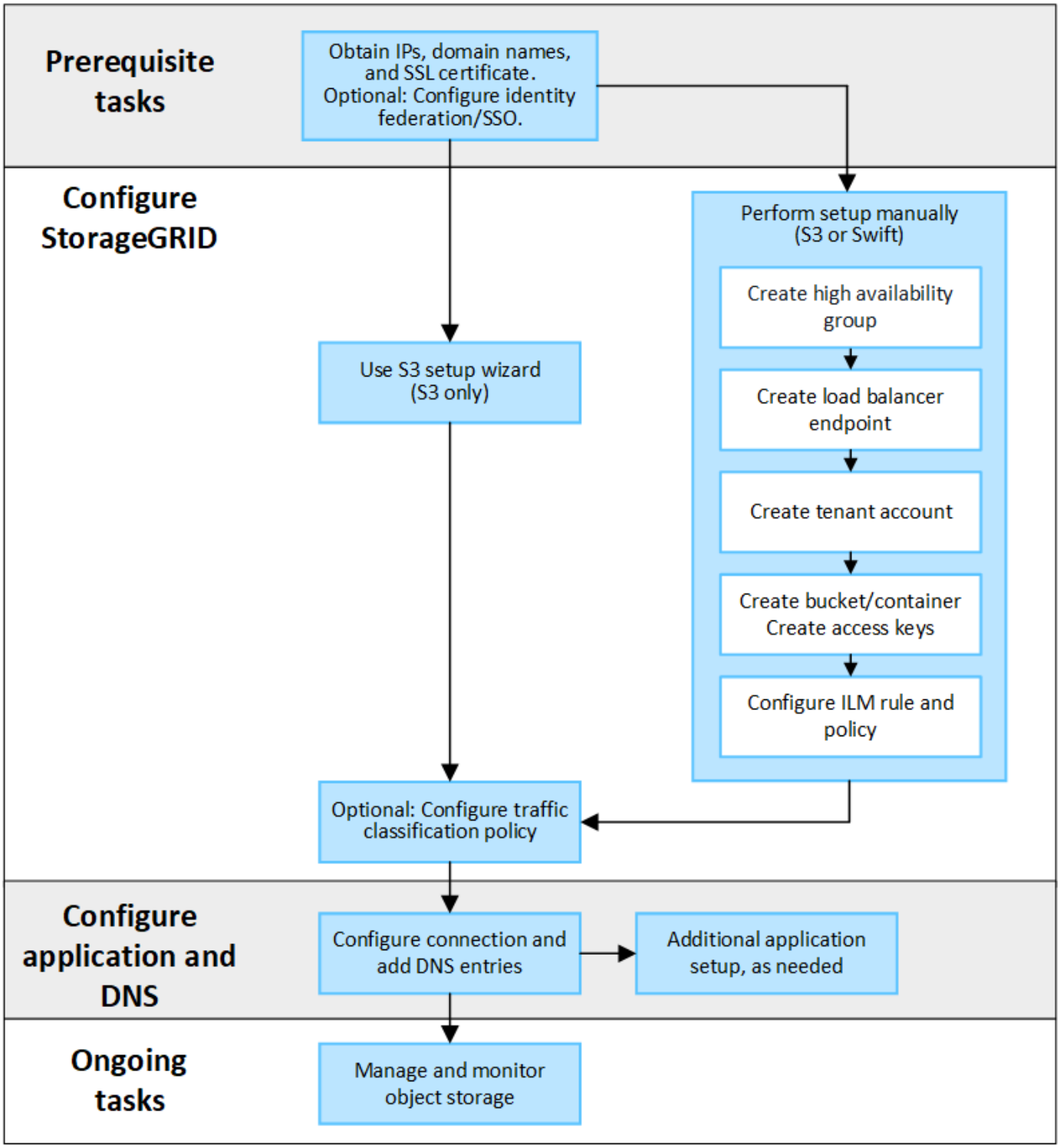
Como administrador de grid, puede gestionar las opciones de configuración que controlan cómo las aplicaciones cliente S3 y Swift se conectan al sistema StorageGRID para almacenar y recuperar los datos.

> Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.

Flujo de trabajo de configuración

Como se muestra en el diagrama de flujo de trabajo, hay cuatro pasos principales para conectar StorageGRID a cualquier aplicación S3 o Swift:

1. Realice tareas de requisitos previos en StorageGRID, según cómo se conectará la aplicación cliente a StorageGRID.
2. Utilice StorageGRID para obtener los valores que la aplicación necesita para conectarse a la cuadrícula. Puede utilizar el asistente de configuración de S3 o configurar cada entidad de StorageGRID manualmente.
3. Use la aplicación S3 o Swift para completar la conexión a StorageGRID. Cree entradas DNS para asociar direcciones IP a cualquier nombre de dominio que desee utilizar.
4. Realice tareas continuas en la aplicación y en StorageGRID para gestionar y supervisar el almacenamiento de objetos a lo largo del tiempo.



Información necesaria para asociar StorageGRID a una aplicación cliente

Para poder asociar StorageGRID a una aplicación cliente S3 o Swift, debe realizar pasos de configuración en StorageGRID y obtener cierto valor.

¿Qué valores necesito?

La tabla siguiente muestra los valores que debe configurar en StorageGRID y donde los utiliza la aplicación S3 o Swift y el servidor DNS.

Valor	Donde se configura el valor	Donde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	Entrada DNS
Puerto	StorageGRID > Punto final del equilibrador de carga	Aplicación cliente
Certificado SSL	StorageGRID > Punto final del equilibrador de carga	Aplicación cliente
Nombre del servidor (FQDN)	StorageGRID > Punto final del equilibrador de carga	• Aplicación cliente • Entrada DNS
S3 ID de clave de acceso y clave de acceso secreta	StorageGRID > inquilino y bloque	Aplicación cliente
Nombre de cubo/contenedor	StorageGRID > inquilino y bloque	Aplicación cliente

¿Cómo obtengo estos valores?

Dependiendo de sus requisitos, puede hacer cualquiera de los siguientes pasos para obtener la información que necesita:

- * Utilice el "S3 Asistente de configuración"*. El asistente de configuración de S3 le ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera uno o dos archivos que puede utilizar al configurar la aplicación S3. El asistente le guiará por los pasos necesarios y le ayudará a garantizar que la configuración cumple las prácticas recomendadas de StorageGRID.

  Si está configurando una aplicación S3, se recomienda utilizar el asistente de configuración de S3 a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

- * Utilice el "Asistente de configuración de FabricPool"*. De forma similar al asistente de configuración de S3, el asistente de configuración de FabricPool ayuda a configurar rápidamente los valores necesarios y genera un archivo que se puede usar al configurar un nivel de cloud de FabricPool en ONTAP.

  Si va a utilizar StorageGRID como sistema de almacenamiento de objetos para un nivel cloud de FabricPool, se recomienda utilizar el asistente de configuración de FabricPool, a menos que sepa que tiene requisitos especiales o que su implementación requerirá una gran personalización.

- **Configurar artículos manualmente**. Si se conecta a una aplicación Swift (o se conecta a una aplicación S3 y prefiere no utilizar el asistente de configuración S3), puede obtener los valores requeridos realizando la configuración manualmente. Siga estos pasos:

  a. Configure el grupo de alta disponibilidad (HA) que desee utilizar para la aplicación S3 o Swift. Consulte "Configuración de grupos de alta disponibilidad".

  b. Cree el extremo del equilibrador de carga que utilizará la aplicación S3 o Swift. Consulte "Configurar puntos finales del equilibrador de carga".

c. Cree la cuenta de inquilino que utilizará la aplicación S3 o Swift. Consulte "Cree una cuenta de inquilino".

d. Para un inquilino de S3, inicie sesión en la cuenta de inquilino y genere un ID de clave de acceso y una clave de acceso secreta para cada usuario que acceda a la aplicación. Consulte "Cree sus propias claves de acceso".

e. Cree uno o varios bloques de S3 o contenedores Swift dentro de la cuenta de inquilino. Para S3, consulte "Crear bloque de S3". En el caso de Swift, utilice el "Solicitud de contenedor PUT".

f. Para agregar instrucciones de ubicación específicas para los objetos que pertenecen al inquilino o bloque/contenedor nuevo, cree una regla de ILM nueva y active una nueva política de ILM para utilizar esa regla. Consulte "Cree la regla de ILM" y.. "Cree una política de ILM".

Seguridad para los clientes S3 o Swift

Las cuentas de inquilino de StorageGRID usan aplicaciones cliente S3 o Swift para guardar datos de objetos en StorageGRID. Debe revisar las medidas de seguridad implementadas para las aplicaciones cliente.

Resumen

En la tabla siguiente se resume cómo se implementa la seguridad para las API DE REST DE S3 y Swift:

Problema de seguridad	Implementación de la API DE REST
Seguridad de la conexión	TLS
Autenticación del servidor	Certificado de servidor X.509 firmado por CA del sistema o certificado de servidor personalizado suministrado por el administrador
Autentificación de clientes	**S3** Cuenta S3 (ID de clave de acceso y clave de acceso secreta) **Swift** Cuenta Swift (nombre de usuario y contraseña)
Autorización de cliente	**S3** Propiedad de buckets y todas las políticas de control de acceso aplicables **Swift** Acceso al rol de administrador

Cómo ofrece StorageGRID seguridad a las aplicaciones cliente

Las aplicaciones cliente S3 y Swift pueden conectarse al servicio de Load Balancer en los nodos de pasarela o nodos de administración, o bien directamente a nodos de almacenamiento.

- Los clientes que se conectan al servicio Load Balancer pueden usar HTTPS o HTTP, según su forma de hacerlo "configure el punto final del equilibrador de carga".

  HTTPS proporciona una comunicación segura cifrada con TLS y se recomienda. Debe adjuntar un

certificado de seguridad al punto final.

HTTP proporciona una comunicación menos segura y sin cifrar y solo debe utilizarse para redes que no sean de producción o de prueba.

- Los clientes que se conectan a los nodos de almacenamiento también pueden usar HTTPS o HTTP.

  HTTPS es el valor predeterminado y se recomienda.

  HTTP proporciona una comunicación menos segura y sin cifrar, pero puede ser opcionalmente "activado" para grids de prueba o de no producción.

- Las comunicaciones entre StorageGRID y el cliente se cifran mediante TLS.
- Las comunicaciones entre el servicio Load Balancer y los nodos de almacenamiento de la cuadrícula están cifradas si el extremo de equilibrio de carga está configurado para aceptar conexiones HTTP o HTTPS.
- Los clientes deben proporcionar encabezados de autenticación HTTP a StorageGRID para realizar operaciones de API DE REST. Consulte "Autenticar solicitudes" y.. "Extremos de API de Swift compatibles".

Certificados de seguridad y aplicaciones cliente

En todos los casos, las aplicaciones cliente pueden realizar conexiones TLS mediante un certificado de servidor personalizado cargado por el administrador de grid o un certificado generado por el sistema StorageGRID:

- Cuando las aplicaciones cliente se conectan al servicio Load Balancer, utilizan el certificado configurado para el punto final del equilibrio de carga. Cada punto final del equilibrador de carga tiene su propio certificado— un certificado de servidor personalizado cargado por el administrador de grid o un certificado que el administrador de grid generó en StorageGRID al configurar el punto final.

  Consulte "Consideraciones que tener en cuenta al equilibrio de carga".

- Cuando las aplicaciones cliente se conectan directamente a un nodo de almacenamiento, utilizan los certificados de servidor generados por el sistema que se generaron para los nodos de almacenamiento cuando se instaló el sistema StorageGRID (que están firmados por la entidad de certificación del sistema), o bien, un único certificado de servidor personalizado proporcionado para la cuadrícula por un administrador de grid. Consulte "Añada un certificado de API S3 o Swift personalizado".

Los clientes deben configurarse para que confíen en la entidad emisora de certificados que firmó el certificado que utilicen para establecer conexiones TLS.

Algoritmos de cifrado y hash compatibles para bibliotecas TLS

El sistema StorageGRID admite un conjunto de conjuntos de cifrado que las aplicaciones cliente pueden utilizar al establecer una sesión TLS. Para configurar los cifrados, vaya a **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD** y seleccione **Políticas TLS y SSH**.

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3.

SSLv3 y TLS 1.1 (o versiones anteriores) ya no son compatibles.

Utilice el asistente de configuración de S3

Utilice el asistente de configuración de S3: Consideraciones y requisitos

Puede usar el asistente de configuración de S3 para configurar StorageGRID como el sistema de almacenamiento de objetos de una aplicación S3.

Cuándo utilizar el asistente de configuración de S3

El asistente de configuración de S3 le guiará en cada paso de la configuración de StorageGRID para su uso con una aplicación S3. Como parte de completar el asistente, descargará archivos que puede utilizar para introducir valores en la aplicación S3. Utilice el asistente para configurar su sistema con mayor rapidez y asegurarse de que su configuración cumple las prácticas recomendadas de StorageGRID.

Si tiene "Permiso de acceso raíz", Puede completar el asistente de configuración de S3 cuando comience a utilizar el Administrador de cuadrícula de StorageGRID, o puede acceder y completar el asistente en cualquier momento posterior. En función de los requisitos, también puede configurar algunos o todos los elementos necesarios manualmente y, a continuación, utilizar el asistente para ensamblar los valores que necesita una aplicación S3.

Antes de utilizar el asistente

Antes de utilizar el asistente, confirme que ha completado estos requisitos previos.

Obtenga direcciones IP y configure interfaces VLAN

Si va a configurar un grupo de alta disponibilidad (HA), sabrá a qué nodos se conectará la aplicación S3 y a qué red StorageGRID se utilizará. También sabe qué valores introducir para la subred CIDR, la dirección IP de la puerta de enlace y las direcciones IP virtuales (VIP).

Si planea utilizar una LAN virtual para segregar el tráfico de la aplicación S3, ya ha configurado la interfaz VLAN. Consulte "Configure las interfaces VLAN".

Configurar la federación de identidades y SSO

Si tiene pensado utilizar la federación de identidades o el inicio de sesión único (SSO) para el sistema StorageGRID, tiene activadas estas funciones. También sabe qué grupo federado debe tener acceso raíz para la cuenta de inquilino que utilizará la aplicación S3. Consulte "Usar la federación de identidades" y.. "Configurar el inicio de sesión único".

Obtener y configurar nombres de dominio

Sabe qué nombre de dominio completo (FQDN) debe utilizar para StorageGRID. Las entradas del servidor de nombres de dominio (DNS) asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo de alta disponibilidad que cree con el asistente.

Si tiene pensado utilizar S3 solicitudes virtuales de estilo hospedado, debería tener "Nombres de dominio de punto final S3 configurados". Se recomienda utilizar solicitudes virtuales de estilo alojado.

Revisión de los requisitos del equilibrio de carga y del certificado de seguridad

Si tiene pensado utilizar el equilibrador de carga de StorageGRID, ha revisado las consideraciones generales sobre el equilibrio de carga. Tiene los certificados que cargará o los valores necesarios para generar un certificado.

Si planea utilizar un punto final de equilibrio de carga externo (de terceros), tiene el nombre de dominio completo (FQDN), el puerto y el certificado para ese equilibrador de carga.

Configure cualquier conexión de federación de grid

Si desea permitir que el inquilino S3 clone los datos de la cuenta y replique objetos del bloque en otra cuadrícula mediante una conexión de federación de grid, antes de iniciar el asistente confirme lo siguiente:

- Ya tienes "se ha configurado la conexión de federación de grid".
- El estado de la conexión es **Conectado**.
- Tiene permiso de acceso raíz.

Acceda al asistente de configuración de S3 y complete este

Puede utilizar el asistente de configuración de S3 para configurar StorageGRID para su uso con una aplicación S3. El asistente de configuración proporciona los valores que la aplicación necesita para acceder a un bucket de StorageGRID y guardar objetos.

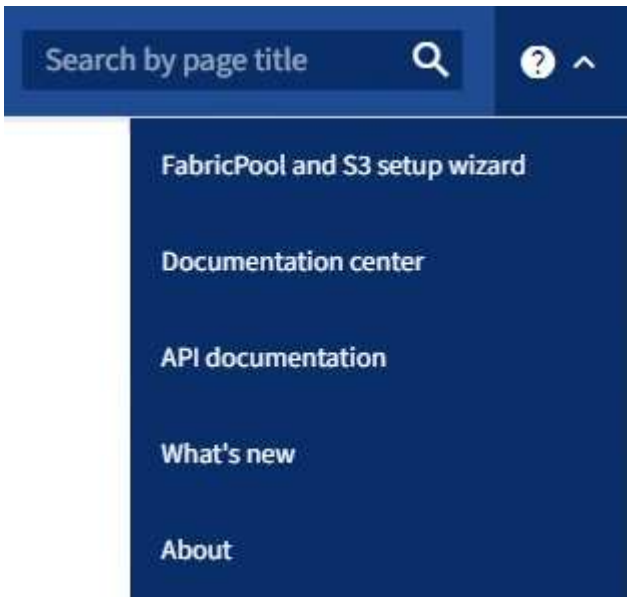
Antes de empezar

- Usted tiene la "Permiso de acceso raíz".
- Ha revisado el "consideraciones y requisitos" para utilizar el asistente.

Acceda al asistente

Pasos

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Si el banner del asistente de configuración **FabricPool y S3** aparece en el panel de control, seleccione el enlace en el banner. Si el banner ya no aparece, seleccione el icono de ayuda en la barra de encabezado del Administrador de cuadrículas y seleccione **FabricPool y el asistente de configuración S3**.



3. En la sección de aplicación S3 de la página del asistente de configuración de FabricPool y S3, seleccione **Configurar ahora**.

Paso 1 de 6: Configurar el grupo de alta disponibilidad

Un grupo de alta disponibilidad es una colección de nodos que contiene cada uno de ellos el servicio de equilibrador de carga de StorageGRID. Un grupo de alta disponibilidad puede contener nodos de pasarela,

nodos de administración o ambos.

Puede usar un grupo de alta disponibilidad para ayudar a mantener las conexiones de datos de S3 GbE disponibles. Si falla la interfaz activa del grupo HA, una interfaz de backup puede gestionar la carga de trabajo con poco impacto en las operaciones de S3.

Para obtener más detalles sobre esta tarea, consulte "Gestión de grupos de alta disponibilidad".

Pasos

1. Si va a utilizar un equilibrador de carga externo, no es necesario crear un grupo de alta disponibilidad. Seleccione **Omitir este paso** y vaya a. Paso 2 de 6: Configurar punto final de equilibrio de carga.
2. Para usar el equilibrador de carga de StorageGRID, es posible crear un grupo de alta disponibilidad nuevo o usar un grupo de alta disponibilidad existente.

Crear grupo de alta disponibilidad

a. Para crear un nuevo grupo HA, selecciona **Crear grupo HA**.

b. Para el paso **Enter details**, complete los siguientes campos.

Campo	Descripción
Nombre del GRUPO HA	Un nombre mostrado exclusivo para este grupo HA.
Descripción (opcional)	La descripción de este grupo de alta disponibilidad.

c. Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo HA.

Utilice los encabezados de columna para ordenar las filas o introduzca un término de búsqueda para localizar las interfaces más rápidamente.

Puede seleccionar uno o varios nodos, pero solo puede seleccionar una interfaz para cada nodo.

d. Para el paso **Priorize interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo HA.

Arrastre las filas para cambiar los valores en la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.

Si el grupo de alta disponibilidad incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si falla esa interfaz, las direcciones VIP pasan a la siguiente interfaz de respaldo, etc. Cuando se resuelven los fallos, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

e. Para el paso **Introducir direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de subred	La dirección de la subred VIP en la notación CIDR — una dirección IPv4 seguida de una barra diagonal y la longitud de subred (0-32). La dirección de red no debe tener ningún bit de host configurado. Por ejemplo: `192.16.0.0/22`.
Dirección IP de la puerta de enlace (opcional)	Si las direcciones IP de S3 utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID, introduzca la dirección IP de la puerta de enlace local VIP de StorageGRID. La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.

Campo	Descripción
Dirección IP virtual	Introduzca al menos una y como máximo diez direcciones VIP para la interfaz activa en el grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP. Al menos una dirección debe ser IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

f. Seleccione **Crear grupo HA** y luego seleccione **Finalizar** para volver al asistente de configuración S3.

g. Seleccione **Continuar** para ir al paso del equilibrador de carga.

Use el grupo de alta disponibilidad existente

a. Para usar un grupo HA existente, seleccione el nombre del grupo HA en el **Seleccione un grupo HA**.

b. Seleccione **Continuar** para ir al paso del equilibrador de carga.

Paso 2 de 6: Configurar punto final de equilibrio de carga

StorageGRID utiliza un balanceador de carga para gestionar la carga de trabajo desde aplicaciones cliente. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en varios nodos de almacenamiento.

Puede usar el servicio de equilibrador de carga de StorageGRID, que existe en todos los nodos de administración y puerta de enlace, o puede conectarse a un equilibrador de carga externo (de terceros). Se recomienda utilizar el equilibrador de carga de StorageGRID.

Para obtener más detalles sobre esta tarea, consulte "Consideraciones que tener en cuenta al equilibrio de carga".

Para usar el servicio de Equilibrador de Carga de StorageGRID, seleccione la pestaña **Equilibrador de Carga de StorageGRID** y, a continuación, cree o seleccione el punto final del equilibrador de carga que desea utilizar. Para usar un equilibrador de carga externo, selecciona la pestaña **Equilibrador de carga externo** y proporciona detalles sobre el sistema que ya has configurado.

Crear punto final

Pasos

1. Para crear un punto final de equilibrio de carga, selecciona **Crear punto final**.
2. Para el paso **Introducir detalles de punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Nombre descriptivo para el punto final.
Puerto	El puerto StorageGRID que desea usar para el equilibrio de carga. Este campo se establece por defecto en 10433 para el primer punto final que cree, pero puede introducir cualquier puerto externo no utilizado. Si introduce 80 o 443, el punto final se configura sólo en los nodos de Gateway, ya que estos puertos están reservados en los nodos de Admin. **Nota:** Los puertos utilizados por otros servicios de red no están permitidos. Consulte "Referencia de puerto de red".
Tipo de cliente	Debe ser **S3**.
Protocolo de red	Seleccione **HTTPS**. **Nota**: La comunicación con StorageGRID sin cifrado TLS es compatible, pero no se recomienda.

3. Para el paso **Select Binding mode**, especifique el modo de encuadernación. El modo de enlace controla cómo se accede al punto final mediante cualquier dirección IP o mediante direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final mediante la dirección IP de cualquier nodo de gateway o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice el ajuste **Global** (predeterminado) a menos que necesite restringir la accesibilidad de este extremo.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad para acceder a este extremo. Los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que seleccione para los puntos finales no se superpongan.

Modo	Descripción
Interfaces de nodos	Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo	En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este extremo.

4. Para el paso de acceso de arrendatario, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir todos los inquilinos (predeterminado)	Todas las cuentas de inquilino pueden usar este extremo para acceder a sus bloques.
Permitir arrendatarios seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este extremo para acceder a sus bloques.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este punto final para acceder a sus bloques. Todos los demás inquilinos pueden usar este extremo.

5. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Cargar certificado (recomendado)	Use esta opción para cargar un certificado de servidor firmado por CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Use esta opción para generar un certificado autofirmado. Consulte "Configurar puntos finales del equilibrador de carga" para obtener detalles sobre lo que se debe introducir.
Usar certificado StorageGRID S3 y Swift	Utilice esta opción solo si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID. Consulte "Configure los certificados API S3 y Swift" para obtener más detalles.

6. Seleccione **Finalizar** para volver al asistente de configuración de S3.
7. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Los cambios en el certificado de extremo pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Utilizar punto final de equilibrio de carga existente

Pasos

1. Para usar un punto final existente, seleccione su nombre en el **Seleccione un punto final de equilibrio de carga**.
2. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Utilizar equilibrador de carga externo

Pasos

1. Para utilizar un equilibrador de carga externo, complete los siguientes campos.

Campo	Descripción
FQDN	Nombre de dominio completo (FQDN) del equilibrador de carga externo.
Puerto	Número de puerto que utilizará la aplicación S3 para conectarse al equilibrador de carga externo.
Certificado	Copie el certificado del servidor para el equilibrador de carga externo y péguelo en este campo.

2. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Paso 3 de 6: Crear inquilino y bloque

Un inquilino es una entidad que puede utilizar aplicaciones S3 para almacenar y recuperar objetos en StorageGRID. Cada inquilino tiene sus propios usuarios, claves de acceso, bloques, objetos y un conjunto específico de funcionalidades. Debe crear el arrendatario antes de crear el depósito que utilizará la aplicación S3 para almacenar sus objetos.

Un bucket es un contenedor que se usa para almacenar los objetos y los metadatos de objetos de un inquilino. Aunque es posible que algunos inquilinos tengan muchos buckets, el asistente le ayuda a crear un inquilino y un bloque de la forma más rápida y sencilla. Puede utilizar el Gestor de inquilinos más adelante para agregar los depósitos adicionales que necesite.

Puede crear un nuevo inquilino para que lo utilice esta aplicación S3. De forma opcional, también puede crear un bucket para el nuevo arrendatario. Por último, puede permitir al asistente crear las claves de acceso S3 para el usuario raíz del inquilino.

Para obtener más detalles sobre esta tarea, consulte "Cree una cuenta de inquilino" y.. "Crear bloque de S3".

Pasos

1. Seleccione **Crear arrendatario**.
2. Para los pasos Enter details, introduzca la siguiente información.

Campo	Descripción
Nombre	Un nombre para la cuenta de inquilino. Los nombres de inquilinos no necesitan ser únicos. Cuando se crea la cuenta de arrendatario, recibe un ID de cuenta numérico único.

Campo	Descripción
Descripción (opcional)	Descripción para ayudar a identificar al inquilino.
Tipo de cliente	El tipo de protocolo de cliente que utilizará este inquilino. Para el asistente de configuración S3, se selecciona **S3** y el campo está desactivado.
Cuota de almacenamiento (opcional)	Si desea que este inquilino tenga una cuota de almacenamiento, un valor numérico para la cuota y las unidades.

3. Seleccione **continuar**.
4. Opcionalmente, seleccione cualquier permiso que desee que tenga este inquilino.

> Algunos de estos permisos tienen requisitos adicionales. Para obtener más información, seleccione el icono de ayuda de cada permiso.

Permiso	Si se ha seleccionado…
Permitir los servicios de plataforma	El inquilino puede usar servicios de plataforma S3 como CloudMirror. Consulte "Gestione servicios de plataformas para cuentas de inquilinos de S3".
Usar origen de identidad propio	El inquilino puede configurar y gestionar su propio origen de identidad para usuarios y grupos federados. Esta opción está desactivada si tiene "SSO configurado" Para su sistema StorageGRID.
Permitir selección S3	El inquilino puede emitir solicitudes de API S3 SelectObjectContent para filtrar y recuperar datos de objetos. Consulte "Gestione S3 Select para cuentas de inquilinos". **Importante**: Las solicitudes de SelectObjectContent pueden disminuir el rendimiento del equilibrador de carga para todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.
Utilizar conexión de federación de grid	El inquilino puede utilizar una conexión de federación de grid. Seleccionando esta opción: • Hace que este arrendatario y todos los grupos de arrendatarios y usuarios agregados a la cuenta se clonen desde esta cuadrícula (la cuadrícula *source*) a la otra cuadrícula de la conexión seleccionada (la cuadrícula *destination*). • Permite a este inquilino configurar la replicación entre grid entre bloques correspondientes en cada grid. Consulte "Gestione los inquilinos permitidos para la federación de grid".

5. Si seleccionó **Usar conexión de federación de grid**, seleccione una de las conexiones de federación de

grid disponibles.

6. Defina el acceso raíz para la cuenta de inquilino en función de si utiliza el sistema StorageGRID "federación de identidades", "Inicio de sesión único (SSO)", o ambos.

Opción	Haga esto
Si la federación de identidades no está activada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidades está activada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si se activan tanto la federación de identidades como el inicio de sesión único (SSO)	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

7. Si desea que el asistente cree el ID de clave de acceso y la clave de acceso secreta para el usuario root, seleccione **Crear clave de acceso S3 de usuario root automáticamente**.

   Seleccione esta opción si el único usuario para el arrendatario será el usuario root. Si otros usuarios usarán este inquilino, use el Gestor de inquilinos para configurar claves y permisos.

8. Seleccione **continuar**.
9. Para el paso de creación de depósito, opcionalmente cree un depósito para los objetos del inquilino. De lo contrario, seleccione **Crear inquilino sin cubo** para ir al paso de descarga de datos.

   Si S3 Object Lock está habilitado para la cuadrícula, el depósito creado en este paso no tiene S3 Object Lock habilitado. Si necesita usar un cubo de bloqueo de objetos S3 para esta aplicación S3, seleccione **Crear inquilino sin cubo**. A continuación, utilice Gestor de inquilinos para "cree el cucharón" en su lugar.

   a. Introduzca el nombre del depósito que utilizará la aplicación S3. Por ejemplo: `S3-bucket`.

      No puede cambiar el nombre del bloque después de crear el bloque.

   b. Seleccione la **Región** para este cubo.

      Utilice la región predeterminada (`us-east-1`) A menos que espere utilizar ILM en el futuro para filtrar objetos en función de la región del bloque.

   c. Seleccione **Activar el control de versiones de objetos** si desea almacenar cada versión de cada objeto en este depósito.

   d. Seleccione **Crear inquilino y cubo** y vaya al paso de descarga de datos.

Paso 4 de 6: Descargar datos

En el paso de descarga de datos, puede descargar uno o dos archivos para guardar los detalles de lo que acaba de configurar.

Pasos

1. Si seleccionó **Crear clave de acceso S3 de usuario root automáticamente**, realice una o ambas de las siguientes acciones:
   - Selecciona **Descargar claves de acceso** para descargar a. `.csv` El archivo que contiene el nombre de la cuenta de inquilino, el ID de clave de acceso y la clave de acceso secreta.
   - Seleccione el icono de copia () Para copiar el ID de clave de acceso y la clave de acceso secreta en el portapapeles.
2. Seleccione **Descargar valores de configuración** para descargar a. `.txt` archivo que contiene la configuración del extremo del balanceador de carga, el inquilino, el bloque y el usuario raíz.
3. Guarde esta información en una ubicación segura.

No cierre esta página hasta que haya copiado ambas claves de acceso. Las teclas no estarán disponibles después de cerrar esta página. Asegúrese de guardar esta información en una ubicación segura, ya que se puede utilizar para obtener datos de su sistema StorageGRID.

4. Si se le solicita, seleccione la casilla de verificación para confirmar que ha descargado o copiado las claves.
5. Seleccione **Continuar** para ir a la regla de ILM y paso de política.

Paso 5 de 6: Revise la regla de ILM y la política de ILM para S3

Las reglas de gestión de la vida útil de la información controlan la ubicación, la duración y el comportamiento de procesamiento de todos los objetos del sistema StorageGRID. La política de ILM incluida con StorageGRID hace dos copias replicadas de todos los objetos. Esta política está en vigor hasta que active al menos una nueva política.

Pasos

1. Revise la información proporcionada en la página.
2. Si desea agregar instrucciones específicas para los objetos que pertenecen al nuevo arrendatario o depósito, cree una nueva regla y una nueva política. Consulte "Cree la regla de ILM" y.. "Políticas de ILM: Información general".
3. Seleccione **He revisado estos pasos y entiendo lo que tengo que hacer**.
4. Seleccione la casilla de verificación para indicar que comprende qué hacer a continuación.
5. Selecciona **Continuar** para ir a **Resumen**.

Paso 6 de 6: Resumen de la revisión

Pasos

1. Revise el resumen.
2. Anote los detalles en los siguientes pasos, que describen la configuración adicional que puede ser necesaria antes de conectarse al cliente S3. Por ejemplo, si selecciona **Iniciar sesión como root**, accederá al gestor de inquilinos, donde podrá agregar usuarios de inquilinos, crear depósitos adicionales y actualizar la configuración del depósito.

3. Seleccione **Finalizar**.
4. Configure la aplicación mediante el archivo descargado de StorageGRID o los valores obtenidos manualmente.

Gestionar grupos de alta disponibilidad

Gestionar grupos de alta disponibilidad: Descripción general

Puede agrupar las interfaces de red de varios nodos de administrador y puerta de enlace en un grupo de alta disponibilidad (ha). Si la interfaz activa del grupo de alta disponibilidad falla, una interfaz de backup puede administrar la carga de trabajo.

¿Qué es un grupo de alta disponibilidad?

Puede usar grupos de alta disponibilidad para proporcionar conexiones de datos de alta disponibilidad para clientes S3 y Swift o proporcionar conexiones de alta disponibilidad a Grid Manager y Tenant Manager.

Cada grupo de alta disponibilidad proporciona acceso a los servicios compartidos en los nodos seleccionados.

- Los grupos de ALTA DISPONIBILIDAD que incluyen nodos de puerta de enlace, nodos de administrador o ambos proporcionan conexiones de datos con alta disponibilidad para los clientes S3 y Swift.
- Los grupos DE ALTA DISPONIBILIDAD que incluyen solo los nodos de administrador proporcionan conexiones de alta disponibilidad con el administrador de grid y el administrador de inquilinos.
- Un grupo de alta disponibilidad que sólo incluye dispositivos SG100 o SG1000 y nodos de software basados en VMware puede proporcionar conexiones de alta disponibilidad "Inquilinos de S3 que usan S3 Select".
  Se recomienda a los grupos de ALTA DISPONIBILIDAD cuando se usa S3 Select, pero no es obligatorio.

¿Cómo se crea un grupo de alta disponibilidad?

1. Debe seleccionar una interfaz de red para uno o más nodos de administrador o nodos de puerta de enlace. Puede usar una interfaz de red de cuadrícula (eth0), una interfaz de red de cliente (eth2), una interfaz VLAN o una interfaz de acceso que haya agregado al nodo.

   > No puede agregar una interfaz a un grupo de alta disponibilidad si tiene una dirección IP asignada por DHCP.

2. Se especifica una interfaz para ser la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.
3. El orden de prioridad de las interfaces de copia de seguridad se determina.
4. Asigne una a 10 direcciones IP virtuales (VIP) al grupo. Las aplicaciones cliente pueden utilizar cualquiera de estas direcciones VIP para conectarse a StorageGRID.

Para ver instrucciones, consulte "Configuración de grupos de alta disponibilidad".

¿Cuál es la interfaz activa?

Durante el funcionamiento normal, todas las direcciones VIP del grupo ha se añaden a la interfaz principal, que es la primera interfaz en el orden de prioridad. Siempre que la interfaz principal siga estando disponible, se utiliza cuando los clientes se conectan a cualquier dirección VIP del grupo. Es decir, durante el funcionamiento normal, la interfaz principal es la interfaz activa del grupo.

Del mismo modo, durante el funcionamiento normal, las interfaces de menor prioridad del grupo de alta disponibilidad actúan como interfaces de backup. Estas interfaces de copia de seguridad no se utilizan a menos que la interfaz primaria (actualmente activa) deje de estar disponible.

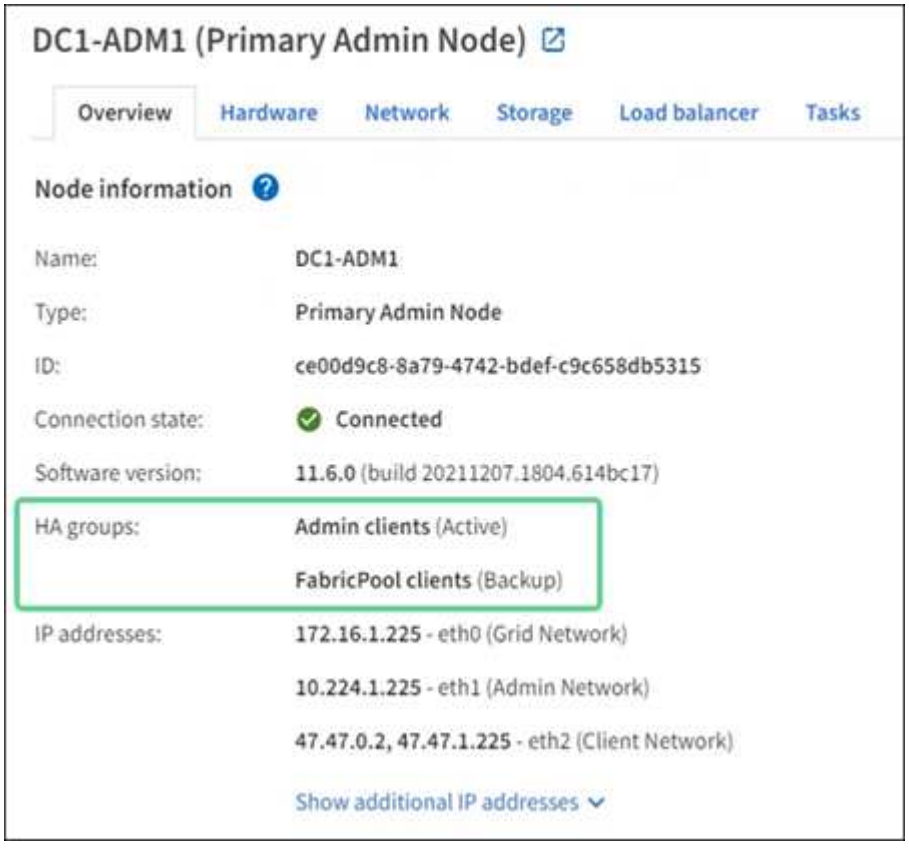
Ver el estado actual del grupo de alta disponibilidad de un nodo

Para ver si un nodo está asignado a un grupo ha y determinar su estado actual, seleccione **NODES** > ***node***.

Si la ficha **Descripción general** incluye una entrada para **grupos ha**, el nodo se asigna a los grupos ha enumerados. El valor después de que el nombre del grupo sea el estado actual del nodo del grupo de alta disponibilidad:

- **Activo**: El grupo ha se está alojando actualmente en este nodo.
- **Copia de seguridad**: El grupo ha no está utilizando actualmente este nodo; se trata de una interfaz de copia de seguridad.
- **Detenido**: El grupo HA no se puede alojar en este nodo porque el servicio High Availability (Keepalived) se ha detenido manualmente.
- **Fallo**: El grupo HA no se puede alojar en este nodo debido a uno o más de los siguientes:
  - El servicio Load Balancer (nginx-gw) no se está ejecutando en el nodo.
  - La interfaz eth0 o VIP del nodo está inactiva.
  - El nodo está inactivo.

En este ejemplo, el nodo de administración principal se ha añadido a dos grupos de alta disponibilidad. Este nodo es actualmente la interfaz activa del grupo de clientes de administración y una interfaz de respaldo del grupo de clientes de FabricPool.



¿Qué ocurre cuando falla la interfaz activa?

La interfaz que aloja actualmente las direcciones VIP es la interfaz activa. Si el grupo ha incluye más de una interfaz y la interfaz activa falla, las direcciones VIP se mueven a la primera interfaz de respaldo disponible en el orden de prioridad. Si falla esa interfaz, las direcciones VIP se mueven a la siguiente interfaz de respaldo disponible, etc.

La conmutación por error puede activarse por cualquiera de estas razones:

- El nodo en el que se configura la interfaz se desactiva.
- El nodo en el que se configura la interfaz pierde la conectividad con los demás nodos durante al menos 2 minutos.
- La interfaz activa se desactiva.
- El servicio Load Balancer se detiene.
- El servicio de alta disponibilidad se detiene.

> Es posible que la conmutación al respaldo no se active por errores de red externos al nodo que aloja la interfaz activa. Del mismo modo, los servicios para Grid Manager o el Gestor de inquilinos no activan la conmutación por error.

Por lo general, el proceso de recuperación tras fallos sólo se realiza en unos pocos segundos y es lo suficientemente rápido como para que las aplicaciones cliente tengan un impacto escaso y puedan confiar en los comportamientos normales de reintento para continuar con el funcionamiento.

Cuando se resuelve un fallo y hay una interfaz de mayor prioridad disponible de nuevo, las direcciones VIP se mueven automáticamente a la interfaz de mayor prioridad disponible.

¿Cómo se utilizan los grupos de alta disponibilidad?

Puede usar grupos de alta disponibilidad para proporcionar conexiones de alta disponibilidad a StorageGRID para datos de objetos y para uso administrativo.

- Un grupo de alta disponibilidad puede proporcionar conexiones administrativas de alta disponibilidad al administrador de grid o al administrador de inquilinos.
- Un grupo de alta disponibilidad puede proporcionar conexiones de datos de alta disponibilidad para clientes S3 y Swift.
- Un grupo de alta disponibilidad que contiene una sola interfaz le permite proporcionar muchas direcciones VIP y establecer explícitamente direcciones IPv6.

Un grupo de alta disponibilidad solo puede proporcionar alta disponibilidad si todos los nodos incluidos en el grupo proporcionan los mismos servicios. Cuando crea un grupo de alta disponibilidad, añada interfaces desde los tipos de nodos que proporcionan los servicios necesarios.

- **Admin Nodes**: Incluye el servicio Load Balancer y permite el acceso al Grid Manager o al arrendatario Manager.
- * Nodos de Gateway*: Incluye el servicio de Equilibrador de Carga.

Objetivo del grupo de alta disponibilidad	Añada nodos de este tipo al grupo de alta disponibilidad
Acceso a Grid Manager	• Nodo de administración principal (**primario**) • Nodos de administrador no primario **Nota:** el nodo de administración principal debe ser la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.
Acceso solo al administrador de inquilinos	• Nodos de administrador primario o no primario
Acceso al cliente de S3 o Swift: Servicio Load Balancer	• Nodos de administración • Nodos de puerta de enlace
Acceso de clientes S3 para "S3 Select"	• Aparatos SG100 o SG1000 • Nodos de software basados en VMware **Nota**: Se recomiendan los grupos DE HA cuando se usa S3 Select, pero no es necesario.

Limitaciones en el uso de grupos de alta disponibilidad con Grid Manager o Intenant Manager

Si falla un servicio de Grid Manager o de arrendatario Manager, no se activa la conmutación por error del grupo de alta disponibilidad.

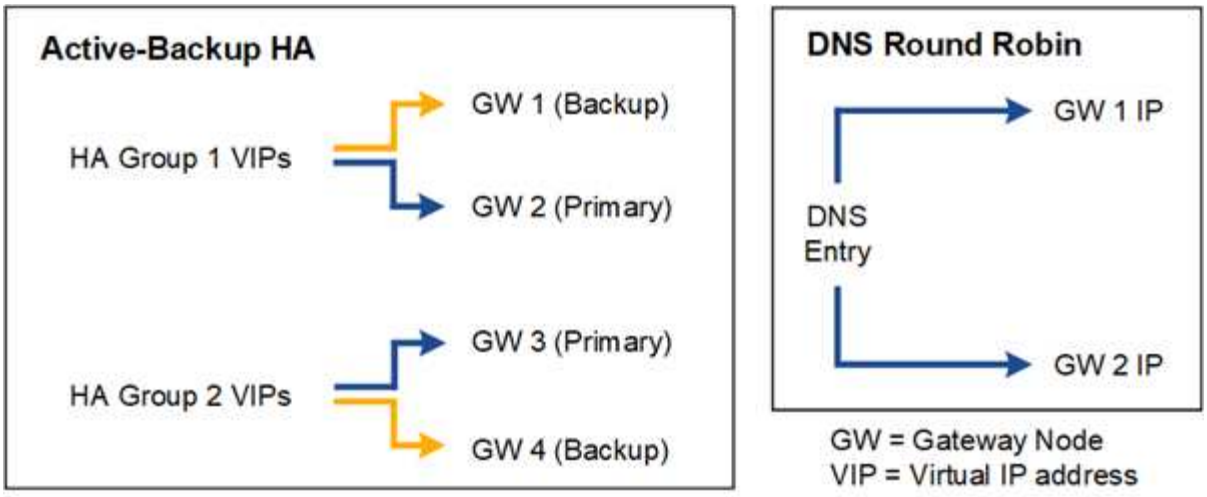
Si ha iniciado sesión en Grid Manager o en el arrendatario Manager cuando se produce la conmutación por error, ha cerrado sesión y debe volver a iniciar sesión para reanudar la tarea.

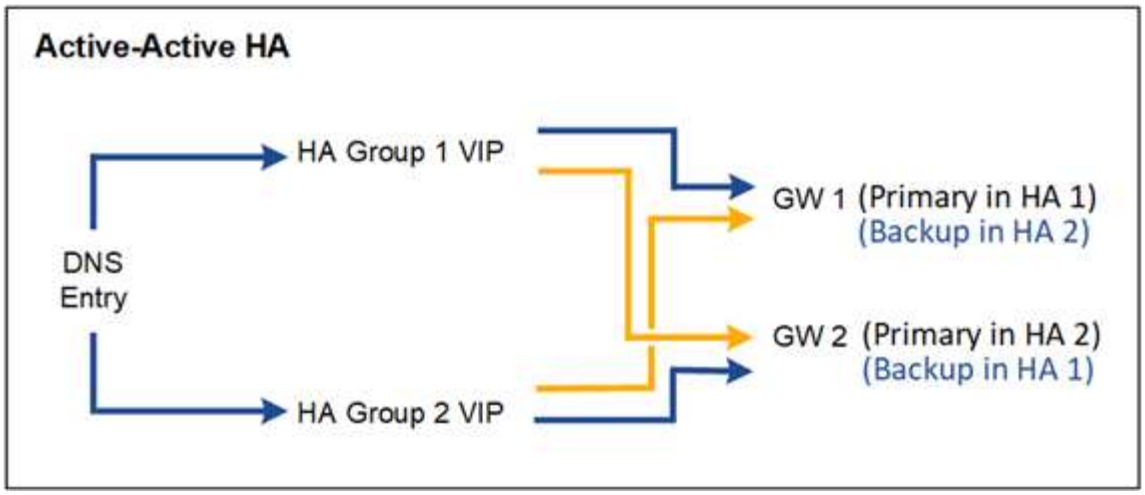
Algunos procedimientos de mantenimiento no se pueden realizar cuando el nodo de administración principal no está disponible. Durante la conmutación por error, puede utilizar Grid Manager para supervisar el sistema StorageGRID.

Opciones de configuración para grupos de alta disponibilidad

Los diagramas siguientes proporcionan ejemplos de diferentes formas de configurar grupos de alta disponibilidad. Cada opción tiene ventajas y desventajas.

En los diagramas, el azul indica la interfaz primaria del grupo de alta disponibilidad y el amarillo indica la interfaz de backup del grupo de alta disponibilidad.





La tabla resume las ventajas de cada configuración de alta disponibilidad que se muestra en el diagrama.

Configuración	Ventajas	Desventajas
Alta disponibilidad de Active-Backup	• Gestionada por StorageGRID sin dependencias externas. • Rápida recuperación tras fallos.	• Solo un nodo de un grupo de alta disponibilidad está activo. Al menos un nodo por grupo de alta disponibilidad estará inactivo.
Operación por turnos DNS	• Mayor rendimiento total. • Sin hosts inactivos.	• Conmutación al respaldo lenta, que puede depender del comportamiento del cliente. • Requiere la configuración del hardware fuera de StorageGRID. • Necesita una comprobación del estado implementada por el cliente.

Configuración	Ventajas	Desventajas
Alta disponibilidad activo-activo	• El tráfico se distribuye entre varios grupos de alta disponibilidad. • Alto rendimiento de agregado escalable con el número de grupos de alta disponibilidad. • Rápida recuperación tras fallos.	• Más complejo de configurar. • Requiere la configuración del hardware fuera de StorageGRID. • Necesita una comprobación del estado implementada por el cliente.

Configuración de grupos de alta disponibilidad

Puede configurar grupos de alta disponibilidad para proporcionar acceso de alta disponibilidad a los servicios en nodos de administración o de puerta de enlace.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".
- Si piensa utilizar una interfaz VLAN en un grupo de alta disponibilidad, ha creado la interfaz VLAN. Consulte "Configure las interfaces VLAN".
- Si planea utilizar una interfaz de acceso para un nodo en un grupo de alta disponibilidad, ha creado la interfaz:
  - **Red Hat Enterprise Linux (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
  - **Ubuntu o Debian (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
  - **Linux (después de instalar el nodo)**: "Linux: Añada tronco o interfaces de acceso a un nodo"
  - **VMware (después de instalar el nodo)**: "VMware: Añada tronco o interfaces de acceso a un nodo"

Crear un grupo de alta disponibilidad

Cuando crea un grupo de alta disponibilidad, selecciona una o varias interfaces y las organiza por orden de prioridad. A continuación, debe asignar una o varias direcciones VIP al grupo.

Una interfaz debe ser para que un nodo de puerta de enlace o un nodo de administrador se incluyan en un grupo de alta disponibilidad. Un grupo de alta disponibilidad solo puede usar una interfaz para cualquier nodo concreto; sin embargo, se pueden usar otras interfaces para el mismo nodo en otros grupos de alta disponibilidad.

Acceda al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
2. Seleccione **Crear**.

Introduzca los detalles del grupo de alta disponibilidad

Pasos

1. Proporcione un nombre único para el grupo de alta disponibilidad.
2. De forma opcional, puede introducir una descripción para el grupo de alta disponibilidad.

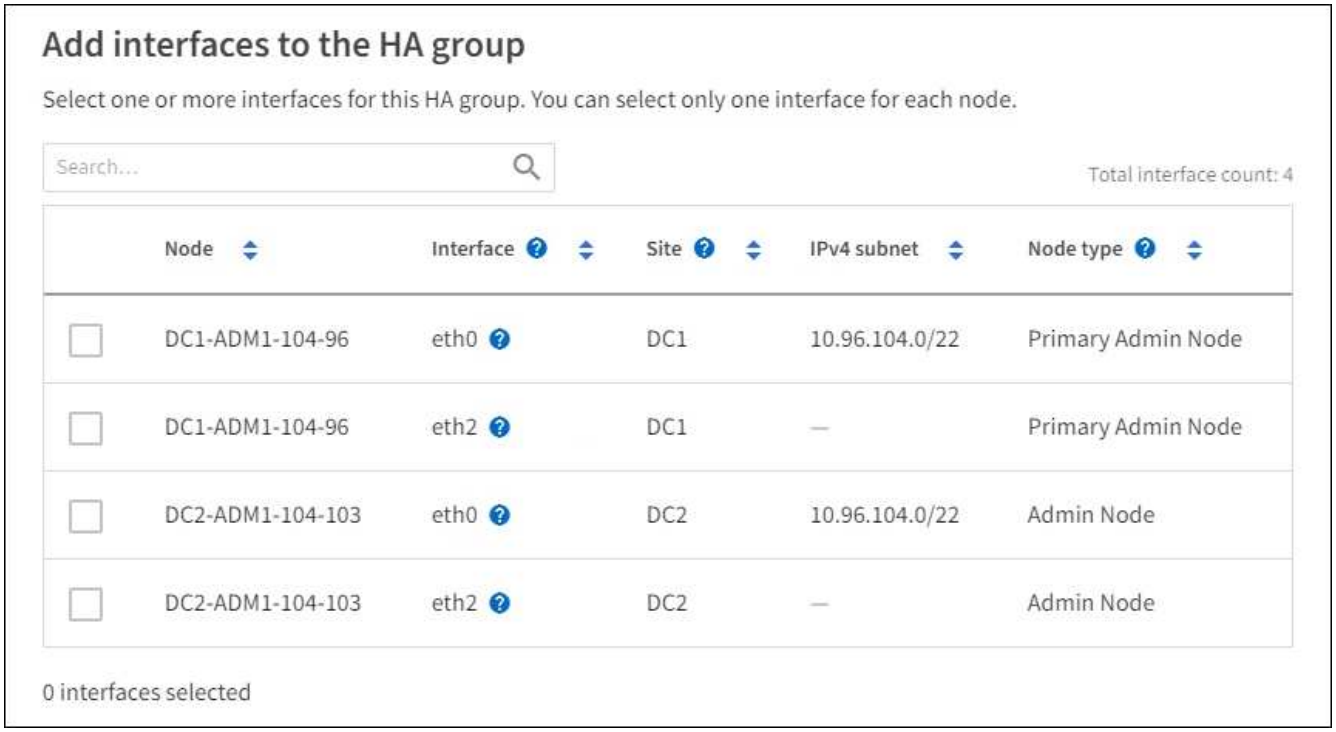
3. Seleccione **continuar**.

Añada interfaces al grupo de alta disponibilidad

Pasos

1. Seleccione una o varias interfaces para añadirlas a este grupo de alta disponibilidad.

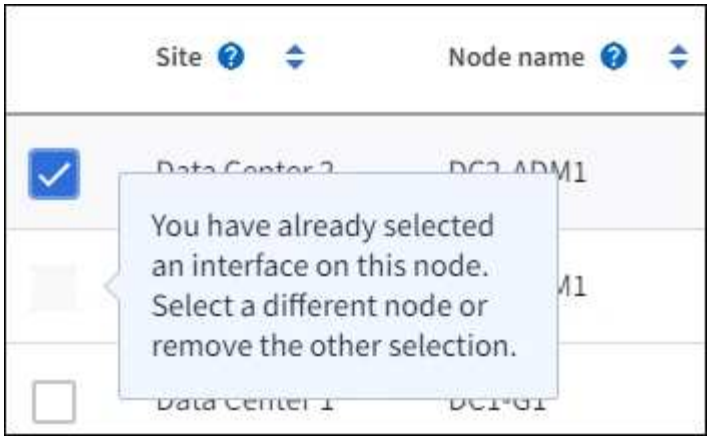
   Utilice los encabezados de columna para ordenar las filas o introduzca un término de búsqueda para localizar las interfaces más rápidamente.



> Después de crear una interfaz VLAN, espere hasta 5 minutos para que la nueva interfaz aparezca en la tabla.

Directrices para seleccionar interfaces

- Debe seleccionar al menos una interfaz.
- Solo puede seleccionar una interfaz para un nodo.
- Si el grupo ha es para la protección de alta disponibilidad de los servicios Admin Node, que incluyen Grid Manager y el inquilino Manager, seleccione interfaces sólo en nodos de administrador.
- Si el grupo de alta disponibilidad está para la protección de alta disponibilidad de tráfico de cliente S3 o Swift, seleccione interfaces en nodos de administrador, nodos de puerta de enlace o ambos.
- Si selecciona interfaces en diferentes tipos de nodos, aparece una nota informativa. Se le recuerda que si se produce una conmutación al respaldo, los servicios que proporciona el nodo que antes estaba activo podrían no estar disponibles en el nodo recién activo. Por ejemplo, un nodo de puerta de enlace de backup no puede ofrecer una protección de alta disponibilidad de los servicios de nodo de administración. Del mismo modo, un nodo de administración de copia de seguridad no puede realizar todos los procedimientos de mantenimiento que puede proporcionar el nodo de administración primario.
- Si no puede seleccionar una interfaz, su casilla de verificación está desactivada. La sugerencia de herramienta proporciona más información.



- No puede seleccionar una interfaz si su valor de subred o puerta de enlace entra en conflicto con otra interfaz seleccionada.
- No puede seleccionar una interfaz configurada si no tiene una dirección IP estática.

2. Seleccione **continuar**.

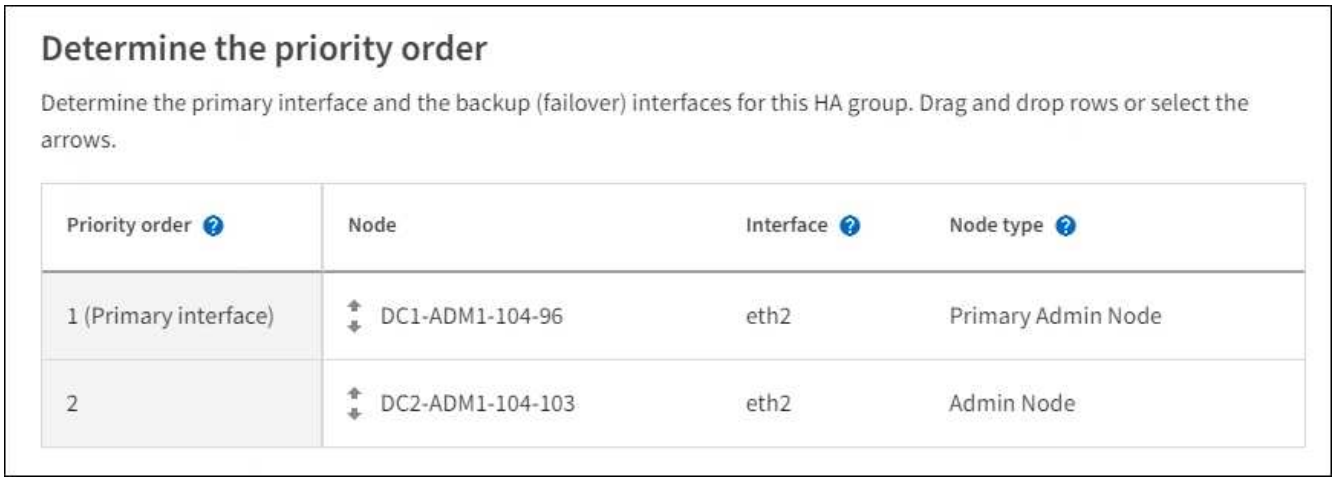
Determinar el orden de prioridad

Si el grupo HA incluye más de una interfaz, puede determinar cuál es la interfaz principal y cuáles son las interfaces de backup (failover). Si la interfaz principal falla, las direcciones VIP se mueven a la interfaz de mayor prioridad que está disponible. Si falla esa interfaz, las direcciones VIP pasan a la siguiente interfaz de mayor prioridad que esté disponible, etc.

Pasos

1. Arrastre filas en la columna **Orden de prioridad** para determinar la interfaz principal y cualquier interfaz de respaldo.

   La primera interfaz de la lista es la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.



> Si el grupo ha proporciona acceso a Grid Manager, debe seleccionar una interfaz en el nodo de administración principal para que sea la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

2. Seleccione **continuar**.

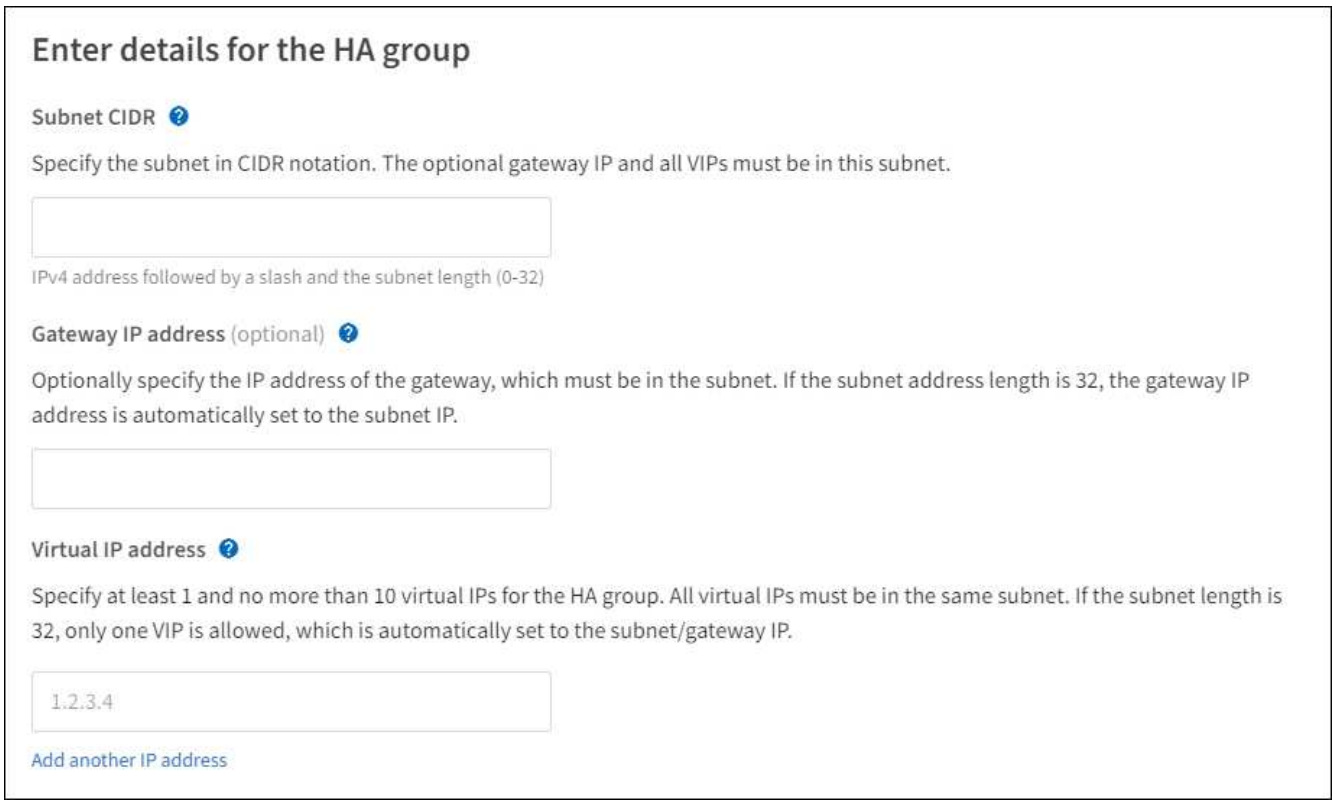
Introduzca las direcciones IP

Pasos

1. En el campo **CIDR de subred**, especifique la subred VIP en notación CIDR --una dirección IPv4 seguida de una barra y la longitud de subred (0-32).

   La dirección de red no debe tener ningún bit de host configurado. Por ejemplo: `192.16.0.0/22`.

   > Si utiliza un prefijo de 32 bits, la dirección de red VIP también funciona como dirección de puerta de enlace y dirección VIP.



2. De manera opcional, si alguno de los clientes S3, Swift, administrativos o de arrendatario accederá a estas direcciones VIP desde una subred diferente, introduzca la **dirección IP de la puerta de enlace**. La dirección de la puerta de enlace debe estar en la subred VIP.

   Los usuarios de cliente y administrador utilizarán esta puerta de enlace para acceder a las direcciones IP virtuales.

3. Introduzca al menos una y como máximo diez direcciones VIP para la interfaz activa en el grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP y todas estarán activas al mismo tiempo en la interfaz activa.

   Debe proporcionar al menos una dirección IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

4. Seleccione **Crear grupo ha** y seleccione **Finalizar**.

   El grupo ha se ha creado y ahora puede utilizar las direcciones IP virtuales configuradas.

Siguientes pasos

Si utilizará este grupo de ha para el equilibrio de carga, cree un extremo de equilibrio de carga para determinar el puerto y el protocolo de red y para conectar los certificados necesarios. Consulte "Configurar puntos finales del equilibrador de carga".

Editar un grupo de alta disponibilidad

Puede editar un grupo de alta disponibilidad para cambiar su nombre y descripción, agregar o quitar interfaces, cambiar el orden de prioridad o agregar o actualizar direcciones IP virtuales.

Por ejemplo, es posible que deba editar un grupo de alta disponibilidad si desea quitar el nodo asociado a una interfaz seleccionada en un procedimiento de retirada del sitio o nodo.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.

   La página grupos de alta disponibilidad muestra todos los grupos de alta disponibilidad existentes.

2. Seleccione la casilla de comprobación del grupo de alta disponibilidad que desea editar.
3. Realice una de las siguientes acciones, según lo que desee actualizar:
   - Seleccione **acciones** > **Editar dirección IP virtual** para agregar o eliminar direcciones VIP.
   - Seleccione **acciones** > **Editar grupo ha** para actualizar el nombre o la descripción del grupo, agregar o quitar interfaces, cambiar el orden de prioridad o agregar o quitar direcciones VIP.
4. Si ha seleccionado **Editar dirección IP virtual**:
   a. Actualice las direcciones IP virtuales del grupo de alta disponibilidad.
   b. Seleccione **Guardar**.
   c. Seleccione **Finalizar**.
5. Si ha seleccionado **Editar grupo ha**:
   a. Si lo desea, actualice el nombre o la descripción del grupo.
   b. Opcionalmente, seleccione o desactive las casillas de verificación para agregar o eliminar interfaces.

      > Si el grupo ha proporciona acceso a Grid Manager, debe seleccionar una interfaz en el nodo de administración principal para que sea la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal

   c. Opcionalmente, arrastre Filas para cambiar el orden de prioridad de la interfaz principal y cualquier interfaz de backup de este grupo de alta disponibilidad.
   d. De manera opcional, actualice las direcciones IP virtuales.
   e. Seleccione **Guardar** y, a continuación, seleccione **Finalizar**.

Eliminar un grupo de alta disponibilidad

Puede eliminar uno o varios grupos de alta disponibilidad al mismo tiempo.

No puede eliminar un grupo de alta disponibilidad si está vinculado a un extremo de equilibrador de carga. Para eliminar un grupo de alta disponibilidad, debe eliminarlo de los extremos de equilibrio de carga que lo utilicen.

Para evitar que se produzcan interrupciones en el cliente, actualice las aplicaciones cliente S3 o Swift afectadas antes de quitar un grupo de alta disponibilidad. Actualice cada cliente para que se conecte mediante otra dirección IP, por ejemplo, la dirección IP virtual de un grupo ha diferente o la dirección IP configurada para una interfaz durante la instalación.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
2. Revise la columna **Load Balancer Endpoints** para cada grupo HA que desee eliminar. Si se muestra algún punto final del equilibrador de carga:
   a. Vaya a **CONFIGURATION** > **Network** > **Load Balancer Endpoints**.
   b. Seleccione la casilla de verificación para el punto final.
   c. Seleccione **acciones** > **Editar modo de enlace de punto final**.
   d. Actualice el modo de enlace para eliminar el grupo HA.
   e. Seleccione **Guardar cambios**.
3. Si no aparece ningún punto final del equilibrador de carga, seleccione la casilla de verificación de cada grupo de alta disponibilidad que desee quitar.
4. Selecciona **Acciones** > **Eliminar grupo HA**.
5. Revise el mensaje y seleccione **Eliminar grupo ha** para confirmar su selección.

   Se eliminan todos los grupos de alta disponibilidad seleccionados. Aparecerá un banner verde de éxito en la página grupos de alta disponibilidad.

Gestione el equilibrio de carga

Consideraciones que tener en cuenta al equilibrio de carga

Es posible utilizar el balanceo de carga para manejar cargas de trabajo de procesamiento y recuperación de clientes S3 y Swift.

¿Qué es el equilibrio de carga?

Cuando una aplicación cliente guarda o recupera datos de un sistema StorageGRID, StorageGRID utiliza un balanceador de carga para gestionar la carga de trabajo de ingesta y recuperación. El equilibrio de carga maximiza la velocidad y la capacidad de conexión mediante la distribución de la carga de trabajo entre varios nodos de almacenamiento.

El servicio de equilibrador de carga de StorageGRID se instala en todos los nodos de administrador y en todos los nodos de puerta de enlace, y ofrece balanceo de carga de capa 7. Realiza la terminación de las solicitudes de cliente de Seguridad de capa de transporte (TLS), inspecciona las solicitudes y establece nuevas conexiones seguras a los nodos de almacenamiento.

El servicio Load Balancer de cada nodo funciona de forma independiente cuando se reenvía tráfico de clientes a los nodos de almacenamiento. Mediante un proceso de ponderación, el servicio Load Balancer envía más solicitudes a los nodos de almacenamiento con una mayor disponibilidad de CPU.

Aunque el servicio StorageGRID Load Balancer es el mecanismo de equilibrio de carga recomendado, puede que en su lugar desee integrar un equilibrador de carga de terceros. Si quiere más información, póngase en contacto con su representante de cuenta de NetApp o consulte "TR-4626: Equilibradores de carga globales y de terceros de StorageGRID".

¿Cuántos nodos de equilibrio de carga se necesitan?

Como práctica recomendada general, cada sitio del sistema StorageGRID debe incluir dos o más nodos con el servicio de equilibrador de carga. Por ejemplo, un sitio puede incluir dos nodos de puerta de enlace, o bien un nodo de administrador y un nodo de puerta de enlace. Asegúrese de que dispone de una infraestructura adecuada de red, hardware o virtualización para cada nodo de equilibrio de carga, ya sea para dispositivos de servicios SG100 o SG1000, nodos de configuración básica o nodos basados en máquinas virtuales (VM).

¿Qué es un extremo de equilibrador de carga?

Un punto final de equilibrio de carga define el puerto y el protocolo de red (HTTPS o HTTP) que utilizarán las solicitudes de aplicación cliente entrantes y salientes para acceder a los nodos que contienen el servicio de equilibrio de carga. El extremo también define el tipo de cliente (S3 o Swift), el modo de enlace y, opcionalmente, una lista de inquilinos permitidos o bloqueados.

Para crear un punto final de equilibrio de carga, seleccione **CONFIGURACIÓN** > **Red** > **Puntos finales de equilibrio de carga** o complete el asistente de configuración de FabricPool y S3. Para obtener instrucciones:

- "Configurar puntos finales del equilibrador de carga"
- "Use el asistente de configuración de S3"
- "Use el asistente de configuración de FabricPool"

Consideraciones para el puerto

El puerto para un punto final de equilibrio de carga es por defecto 10433 para el primer punto final que cree, pero puede especificar cualquier puerto externo no utilizado entre 1 y 65535. Si utiliza el puerto 80 o 443, el punto final utilizará el servicio Equilibrador de Carga sólo en los nodos de Gateway. Estos puertos están reservados en los nodos de administrador. Si utiliza el mismo puerto para más de un punto final, debe especificar un modo de enlace diferente para cada punto final.

Los puertos utilizados por otros servicios de grid no están permitidos. Consulte "Referencia de puerto de red".

Consideraciones para el protocolo de red

En la mayoría de los casos, las conexiones entre las aplicaciones cliente y StorageGRID deben utilizar el cifrado de seguridad de la capa de transporte (TLS). Aunque no se recomienda la conexión a StorageGRID sin cifrado TLS, especialmente en entornos de producción. Al seleccionar el protocolo de red para el punto final del equilibrador de carga StorageGRID, debe seleccionar **HTTPS**.

Consideraciones sobre los certificados de punto final del equilibrador de carga

Si selecciona **HTTPS** como protocolo de red para el punto final del equilibrador de carga, debe proporcionar un certificado de seguridad. Puede utilizar cualquiera de estas tres opciones al crear el punto final del equilibrador de carga:

- **Sube un certificado firmado (recomendado)**. Este certificado puede estar firmado por una entidad de certificación (CA) de confianza pública o una entidad de certificación (CA) privada. El uso de un certificado de servidor de CA de confianza pública para proteger la conexión es la práctica recomendada. A

diferencia de los certificados generados, los certificados firmados por una CA pueden rotarse de forma no disruptiva, lo que puede ayudar a evitar problemas de caducidad.

Debe obtener los siguientes archivos antes de crear el punto final del equilibrador de carga:

  - El archivo de certificado del servidor personalizado.
  - El archivo de claves privadas del certificado de servidor personalizado.
  - De manera opcional, un paquete de CA de los certificados de cada entidad emisora intermedia.

- **Generar un certificado autofirmado**.
- **Utilice el certificado global StorageGRID S3 y Swift**. Debe cargar o generar una versión personalizada de este certificado antes de poder seleccionarlo para el punto final del equilibrador de carga. Consulte "Configure los certificados API S3 y Swift".

¿Qué valores necesito?

Para crear el certificado, debe conocer todos los nombres de dominio y las direcciones IP que utilizarán las aplicaciones cliente S3 o Swift para acceder al extremo.

La entrada **Subject DN** (Nombre Distinguido) para el certificado debe incluir el nombre de dominio completo que la aplicación cliente utilizará para StorageGRID. Por ejemplo:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Según sea necesario, el certificado puede utilizar comodines para representar los nombres de dominio totalmente cualificados de todos los nodos de administración y nodos de gateway que ejecutan el servicio de equilibrio de carga. Por ejemplo: `*.storagegrid.example.com` utiliza el comodín * que se va a representar `adm1.storagegrid.example.com` y.. `gn1.storagegrid.example.com`.

Si planea utilizar S3 solicitudes virtuales de estilo hospedado, el certificado también debe incluir una entrada **Nombre Alternativo** para cada una "Nombre de dominio de punto final S3" ha configurado, incluidos los nombres comodín. Por ejemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

> Si utiliza caracteres comodín para los nombres de dominio, revise la "Directrices de refuerzo para certificados de servidor".

También debe definir una entrada DNS para cada nombre en el certificado de seguridad.

¿Cómo se gestionan los certificados que caducan?

> Si el certificado utilizado para proteger la conexión entre la aplicación S3 y StorageGRID caduca, la aplicación podría perder temporalmente el acceso a StorageGRID.

Para evitar problemas de caducidad de certificados, siga las siguientes prácticas recomendadas:

- Monitoree cuidadosamente cualquier alerta que advierta de fechas de vencimiento de certificados que se

acercan, como el **Caducidad del certificado de punto final del equilibrador de carga** y **Caducidad del certificado de servidor global para las alertas S3 y Swift API**.

- Mantenga siempre sincronizadas las versiones del certificado de la aplicación StorageGRID y S3. Si reemplaza o renueva el certificado utilizado para un punto final de equilibrio de carga, debe reemplazar o renovar el certificado equivalente utilizado por la aplicación S3.
- Utilice un certificado de CA firmado públicamente. Si utiliza un certificado firmado por una CA, puede sustituir certificados próximos a caducar de forma no disruptiva.
- Si generó un certificado StorageGRID autofirmado y ese certificado está a punto de caducar, debe reemplazar manualmente el certificado tanto en StorageGRID como en la aplicación S3 antes de que caduque el certificado existente.

Consideraciones sobre el modo de enlace

El modo de enlace le permite controlar qué direcciones IP se pueden utilizar para acceder a un punto final de equilibrio de carga. Si un punto final utiliza un modo de enlace, las aplicaciones cliente solo pueden acceder al punto final si utilizan una dirección IP permitida o su nombre de dominio completo (FQDN) correspondiente. Las aplicaciones cliente que utilizan cualquier otra dirección IP o FQDN no pueden acceder al punto final.

Puede especificar cualquiera de los siguientes modos de enlace:

- **Global** (por defecto): Las aplicaciones cliente pueden acceder al punto final utilizando la dirección IP de cualquier Nodo de Gateway o Nodo de Administración, la dirección IP virtual (VIP) de cualquier grupo HA en cualquier red, o un FQDN correspondiente. Utilice esta configuración a menos que necesite restringir la accesibilidad de un punto final.
- **IPs virtuales de grupos HA**. Las aplicaciones cliente deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad.
- **Interfaces de nodo**. Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas.
- **Tipo de nodo**. En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace.

Consideraciones para el acceso de inquilinos

El acceso de inquilino es una función de seguridad opcional que le permite controlar qué cuentas de inquilino de StorageGRID pueden usar un extremo de equilibrador de carga para acceder a sus buckets. Puede permitir que todos los inquilinos accedan a un punto final (valor predeterminado) o puede especificar una lista de los inquilinos permitidos o bloqueados para cada punto final.

Puede utilizar esta función para proporcionar un mejor aislamiento de seguridad entre los inquilinos y sus extremos. Por ejemplo, puede utilizar esta función para asegurarse de que los materiales de alto secreto o altamente clasificados propiedad de un arrendatario permanezcan completamente inaccesibles para otros arrendatarios.

> Para fines de control de acceso, el inquilino se determina a partir de las claves de acceso utilizadas en la solicitud del cliente, si no se proporcionan claves de acceso como parte de la solicitud (como con acceso anónimo), el propietario del depósito se utiliza para determinar el inquilino.

Ejemplo de acceso de inquilinos

Para entender cómo funciona esta característica de seguridad, considere el siguiente ejemplo:

1. Ha creado dos puntos finales de equilibrio de carga, de la siguiente manera:
   - **Punto final público**: Utiliza el puerto 10443 y permite el acceso a todos los inquilinos.
   - **Top SECRET** punto final: Utiliza el puerto 10444 y permite el acceso al inquilino **Top SECRET** solamente. Todos los demás inquilinos tienen bloqueado el acceso a este punto final.
2. La `top-secret.pdf` Está en un cubo propiedad del inquilino **Top secret**.

Para acceder al `top-secret.pdf`, Un usuario en el inquilino **Top secret** puede emitir una solicitud GET a. `https://w.x.y.z:10444/top-secret.pdf`. Como este inquilino puede usar el extremo 10444, el usuario puede acceder al objeto. Sin embargo, si un usuario que pertenece a cualquier otro arrendatario emite la misma solicitud a la misma URL, recibe un mensaje de acceso denegado inmediato. Se deniega el acceso aunque las credenciales y la firma sean válidas.

Disponibilidad de CPU

El servicio Load Balancer en cada nodo de administración y nodo de puerta de enlace funciona de forma independiente cuando se reenvía tráfico de S3 o Swift a los nodos de almacenamiento. Mediante un proceso de ponderación, el servicio Load Balancer envía más solicitudes a los nodos de almacenamiento con una mayor disponibilidad de CPU. La información de carga de CPU del nodo se actualiza cada pocos minutos, pero es posible que la ponderación se actualice con mayor frecuencia. A todos los nodos de almacenamiento se les asigna un valor de peso base mínimo, incluso si un nodo informa de un uso del 100 % o no informa de su uso.

En algunos casos, la información acerca de la disponibilidad de CPU se limita al sitio donde se encuentra el servicio Load Balancer.

Configurar puntos finales del equilibrador de carga

Los extremos de equilibrador de carga determinan los puertos y los protocolos de red que los clientes S3 y Swift pueden utilizar al conectarse al equilibrador de carga StorageGRID en los nodos de puerta de enlace y administración. También puede utilizar puntos finales para acceder a Grid Manager, Tenant Manager o ambos.

> Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".
- Ha revisado el "consideraciones que tener en cuenta al equilibrio de carga".
- Si anteriormente ha reasignado un puerto que tiene intención de utilizar para el extremo de equilibrio de carga, tiene "se ha eliminado el mapa de puertos".
- Ha creado cualquier grupo de alta disponibilidad que desee utilizar. Se recomiendan los grupos de ALTA DISPONIBILIDAD, pero no es obligatorio. Consulte "Gestión de grupos de alta disponibilidad".
- Si el punto final del equilibrador de carga será utilizado por "Inquilinos de S3 para S3 Select", No debe utilizar las direcciones IP ni las FQDN de ningún nodo de configuración básica. Sólo se permiten los

dispositivos SG100 o SG1000 y los nodos de software basados en VMware para los extremos de equilibrador de carga utilizados para S3 Select.

- Ha configurado las interfaces VLAN que desea utilizar. Consulte "Configure las interfaces VLAN".
- Si crea un extremo de HTTPS (recomendado), tiene la información del certificado de servidor.

> Los cambios en el certificado de extremo pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

  - Para cargar un certificado, necesita el certificado de servidor, la clave privada de certificado y, opcionalmente, un bundle de CA.
  - Para generar un certificado, se necesitan todos los nombres de dominio y las direcciones IP que utilizarán los clientes S3 o Swift para acceder al extremo. También debe conocer el asunto (nombre distintivo).
  - Si desea usar el certificado API de StorageGRID S3 y Swift (que también se puede usar para conexiones directamente a nodos de almacenamiento), ya sustituyó el certificado predeterminado por un certificado personalizado firmado por una autoridad de certificado externa. Consulte "Configure los certificados API S3 y Swift".

Cree un extremo de equilibrador de carga

Cada extremo de balanceador de carga de cliente S3 o Swift especifica un puerto, un tipo de cliente (S3 o Swift) y un protocolo de red (HTTP o HTTPS). Los extremos de balanceo de carga de la interfaz de gestión especifican un puerto, un tipo de interfaz y una red de cliente que no es de confianza.

Acceda al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**.
2. Para crear un punto final para un cliente S3 o Swift, seleccione la pestaña Cliente **S3 o Swift**.
3. Para crear un punto final para acceder a Grid Manager, Tenant Manager o ambos, seleccione la pestaña **Interfaz de administración**.
4. Seleccione **Crear**.

Introduzca los detalles de los extremos

Pasos

1. Seleccione las instrucciones adecuadas para introducir los detalles del tipo de punto final que desea crear.

Cliente S3 o Swift

Campo	Descripción
Nombre	Nombre descriptivo para el punto final, que aparecerá en la tabla de la página Load equilibrer Endpoints.
Puerto	El puerto StorageGRID que desea usar para el equilibrio de carga. Este campo se establece por defecto en 10433 para el primer punto final que cree, pero puede introducir cualquier puerto externo no utilizado de 1 a 65535. Si ingresa **80** o **8443**, el punto final se configura solo en los nodos de Gateway, a menos que haya liberado el puerto 8443. A continuación, puede utilizar el puerto 8443 como punto final S3 y el puerto se configurará en los nodos Gateway y Admin.
Tipo de cliente	Tipo de aplicación cliente que utilizará este extremo, ya sea **S3** o **Swift**.
Protocolo de red	El protocolo de red que utilizarán los clientes al conectarse a este extremo. • Seleccione **HTTPS** para una comunicación segura cifrada con TLS (recomendado). Debe asociar un certificado de seguridad para poder guardar el extremo. • Seleccione **HTTP** para una comunicación no cifrada y menos segura. Utilice HTTP sólo para una cuadrícula que no sea de producción.

Interfaz de gestión

Campo	Descripción
Nombre	Nombre descriptivo para el punto final, que aparecerá en la tabla de la página Load equilibrer Endpoints.
Puerto	El puerto StorageGRID que desea utilizar para acceder al Administrador de grid, el Administrador de inquilinos o ambos. • Grid Manager: **8443** • Administrador de Inquilinos: **9443** • Tanto Grid Manager como Tenant Manager: **443** **Nota**: Puede utilizar estos puertos preestablecidos u otros puertos disponibles.
Tipo de interfaz	Seleccione el botón de opción de la interfaz StorageGRID a la que accederá desde este punto final.

Campo	Descripción
Red cliente no confiable	Seleccione **Sí** si este punto final debe ser accesible para las redes de clientes que no sean de confianza. De lo contrario, seleccione **No**. Cuando selecciona **Sí**, el puerto está abierto en todas las redes cliente que no sean de confianza. **Nota**: Solo puede configurar un puerto para que esté abierto o cerrado a las redes de clientes que no sean de confianza al crear el punto final del equilibrador de carga.

1. Seleccione **continuar**.

Seleccione un modo de enlace

Pasos

1. Seleccione un modo de enlace para el punto final para controlar cómo se accede al punto final mediante cualquier dirección IP o mediante direcciones IP e interfaces de red específicas.

   Algunos modos de vinculación están disponibles para extremos de cliente o para extremos de interfaz de gestión. Aquí se enumeran todos los modos para ambos tipos de punto final.

Modo	Descripción
Global (por defecto para puntos finales de cliente)	Los clientes pueden acceder al punto final mediante la dirección IP de cualquier nodo de gateway o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice la configuración **Global** a menos que necesite restringir la accesibilidad de este punto final.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad para acceder a este extremo. Los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que seleccione para los puntos finales no se superpongan.
Interfaces de nodos	Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo (solo extremos de cliente)	En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este extremo.

Modo	Descripción
Todos los nodos de administración (predeterminado para los extremos de la interfaz de gestión)	Los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración para acceder a este extremo.

Si más de un punto final utiliza el mismo puerto, StorageGRID utiliza este orden de prioridad para decidir qué punto final utilizar: **IP virtuales de grupos HA** > **Interfaces de nodo** > **Tipo de nodo** > **Global**.

Si va a crear extremos de la interfaz de gestión, solo se permiten los nodos de administrador.

2. Si ha seleccionado **IP virtuales de grupos ha**, seleccione uno o más grupos ha.

   Si va a crear extremos de interfaz de gestión, seleccione VIP asociadas sólo a nodos de administración.

3. Si ha seleccionado **interfaces de nodo**, seleccione una o más interfaces de nodo para cada nodo de administración o nodo de puerta de enlace que desee asociar con este extremo.
4. Si seleccionó **Tipo de nodo**, seleccione Nodos de administración, que incluye tanto el nodo de administración principal como cualquier nodo de administración no principal, o Nodos de puerta de enlace.

Controle el acceso de inquilinos

Un extremo de la interfaz de gestión puede controlar el acceso de los inquilinos solo cuando el extremo tiene el Tipo de interfaz de gestor de inquilinos.

Pasos

1. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir todos los inquilinos (predeterminado)	Todas las cuentas de inquilino pueden usar este extremo para acceder a sus bloques. Debe seleccionar esta opción si aún no ha creado ninguna cuenta de arrendatario. Después de agregar cuentas de arrendatario, puede editar el punto final del equilibrador de carga para permitir o bloquear cuentas específicas.
Permitir arrendatarios seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este extremo para acceder a sus bloques.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este punto final para acceder a sus bloques. Todos los demás inquilinos pueden usar este extremo.

2. Si está creando un punto final **HTTP**, no necesita adjuntar un certificado. Seleccione **Crear** para agregar el nuevo punto final del equilibrador de carga. A continuación, vaya a. Después de terminar. De lo contrario, seleccione **continuar** para adjuntar el certificado.

Adjunte el certificado

Pasos

1. Si está creando un extremo **HTTPS**, seleccione el tipo de certificado de seguridad que desea asociar al extremo.

   El certificado protege las conexiones entre los clientes S3 y Swift y el servicio Load Balancer en los nodos de Admin Node o de Gateway.

   - **Cargar certificado**. Seleccione esta opción si tiene certificados personalizados para cargar.
   - **Generar certificado**. Seleccione esta opción si tiene los valores necesarios para generar un certificado personalizado.
   - **Utilice los certificados StorageGRID S3 y Swift**. Seleccione esta opción si desea usar el certificado API global S3 y Swift, que también se puede usar para las conexiones directamente con nodos de almacenamiento.

     No puede seleccionar esta opción a menos que haya sustituido el certificado de API S3 y Swift predeterminado, firmado por la CA de grid, por un certificado personalizado firmado por una entidad de certificación externa. Consulte "Configure los certificados API S3 y Swift".

   - **Utilice el certificado de interfaz de gestión**. Seleccione esta opción si desea usar el certificado de interfaz de gestión global, que también se puede utilizar para conexiones directas a los nodos de administración.

2. Si no está usando los certificados StorageGRID S3 y Swift, cargue o genere el certificado.

Cargue el certificado

a. Seleccione **cargar certificado**.

b. Cargue los archivos de certificado de servidor requeridos:

- **Certificado de servidor**: El archivo de certificado de servidor personalizado en codificación PEM.
- **Clave privada de certificado**: Archivo de clave privada de certificado de servidor personalizado (`.key`).

> Las claves privadas EC deben ser de 224 bits o más. Las claves privadas RSA deben ser de 2048 bits o más.

- **Paquete CA**: Un único archivo opcional que contiene los certificados de cada entidad emisora de certificados intermedia (CA). 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.

c. Expanda **Detalles del certificado** para ver los metadatos de cada certificado que haya cargado. Si cargó un paquete de CA opcional, cada certificado aparece en su propia pestaña.

- Seleccione **Descargar certificado** para guardar el archivo de certificado o seleccione **Descargar paquete de CA** para guardar el paquete de certificados.

  Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

  Por ejemplo: `storagegrid_certificate.pem`

- Seleccione **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

d. Seleccione **Crear**.
Se crea el punto final del equilibrador de carga. El certificado personalizado se utiliza para todas las conexiones nuevas subsiguientes entre los clientes S3 y Swift, o bien para la interfaz de gestión y el extremo.

Generar certificado

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o varios nombres de dominio completos que se deben incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
IP	Una o más direcciones IP que se incluirán en el certificado.

Campo	Descripción
Asunto (opcional)	X,509 Asunto o nombre distinguido (DN) del propietario del certificado. Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la dirección IP como nombre común del asunto (CN).
Días válidos	Núm. De días después de la creación que caduca el certificado.
Agregue extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de claves y uso de claves ampliado se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. **Nota**: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes antiguos cuando los certificados incluyen estas extensiones.

c. Seleccione **generar**.

d. Seleccione **Detalles del certificado** para ver los metadatos del certificado generado.

   - Seleccione **Descargar certificado** para guardar el archivo de certificado.

     Especifique el nombre del archivo de certificado y la ubicación de descarga. Guarde el archivo con la extensión `.pem`.

   Por ejemplo: `storagegrid_certificate.pem`

   - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado para pegarlo en otro lugar.

e. Seleccione **Crear**.

   Se crea el punto final del equilibrador de carga. El certificado personalizado se utiliza para todas las conexiones nuevas subsiguientes entre los clientes S3 y Swift, o bien para la interfaz de gestión y este extremo.

Después de terminar

Pasos

1. Si utiliza un DNS, asegúrese de que el DNS incluya un registro para asociar el nombre de dominio completo (FQDN) de StorageGRID a cada dirección IP que utilizarán los clientes para realizar conexiones.

   La dirección IP que introduzca en el registro DNS depende de si se utiliza un grupo de alta disponibilidad de nodos con balanceo de carga:

   - Si ha configurado un grupo de alta disponibilidad, los clientes se conectarán a las direcciones IP virtuales de dicho grupo de alta disponibilidad.

- Si no está utilizando un grupo HA, los clientes se conectarán al servicio de equilibrador de carga de StorageGRID mediante la dirección IP de un nodo de puerta de enlace o nodo de administración.

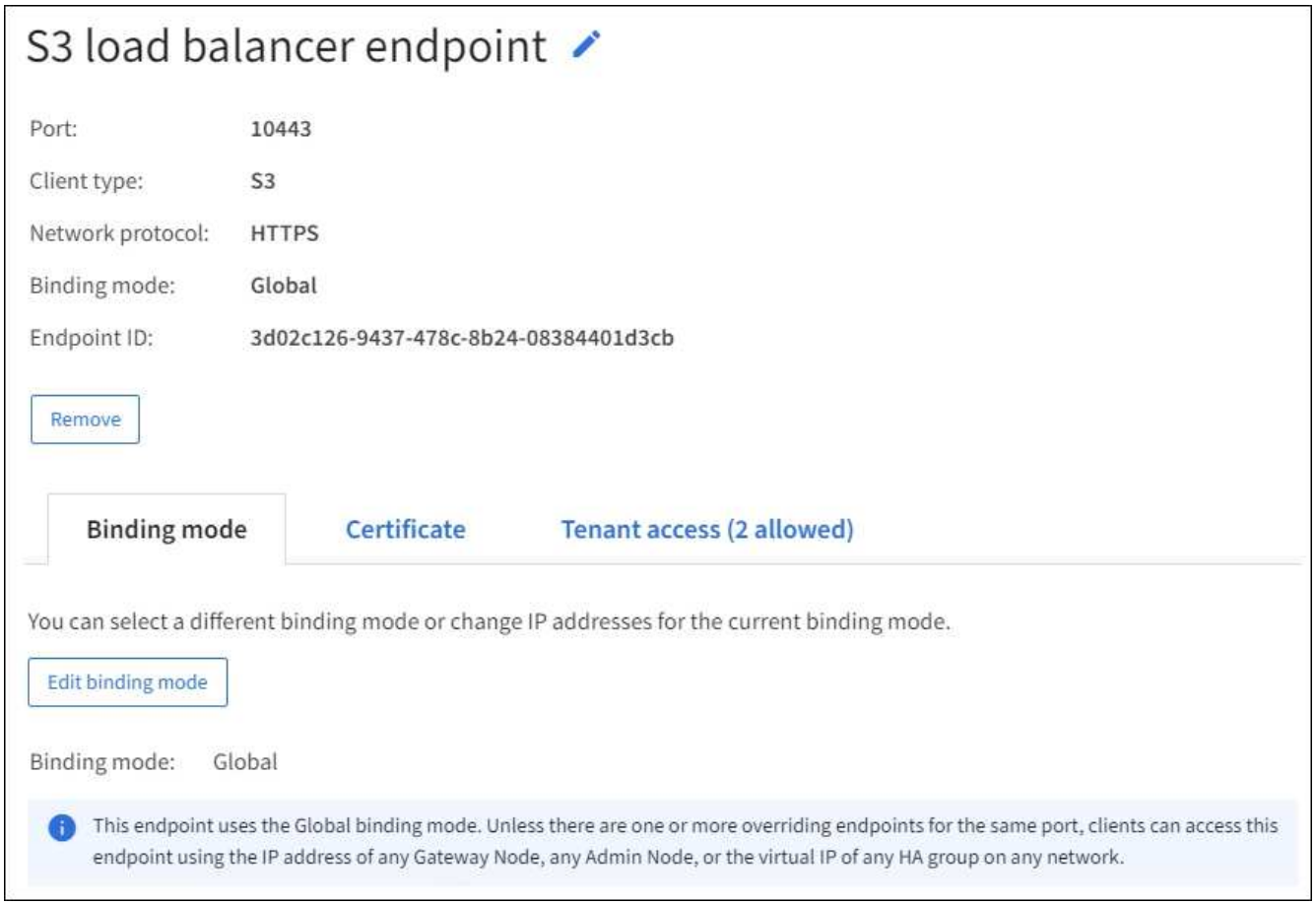
  También debe asegurarse de que el registro DNS hace referencia a todos los nombres de dominio de extremo requeridos, incluidos los nombres de comodín.

2. Proporcione a los clientes S3 y Swift la información necesaria para conectarse al extremo:
   - Número de puerto
   - Nombre de dominio o dirección IP completos
   - Los detalles de certificado necesarios

Ver y editar puntos finales del equilibrador de carga

Puede ver detalles de los extremos de equilibrador de carga existentes, incluidos los metadatos de certificado para un extremo protegido. Puede cambiar determinados valores para un punto final.

- Para ver información básica de todos los puntos finales de equilibrio de carga, revise las tablas en la página Puntos Finales de Equilibrador de Carga.
- Para ver todos los detalles acerca de un extremo específico, incluidos los metadatos del certificado, seleccione el nombre del extremo en la tabla. La información que se muestra varía en función del tipo de punto final y de cómo se configura.



- Para editar un punto final, utilice el menú **Acciones** de la página Puntos Finales de Equilibrador de Carga.

Si pierde acceso a Grid Manager al editar el puerto de un extremo de interfaz de gestión, actualice la URL y el puerto para recuperar el acceso.

Después de editar un extremo, es posible que deba esperar hasta 15 minutos para que los cambios se apliquen a todos los nodos.

Tarea	Menú Actions	Detalles
Editar el nombre del extremo	a. Seleccione la casilla de verificación para el punto final. b. Seleccione **acciones** > **Editar nombre de punto final**. c. Introduzca el nuevo nombre. d. Seleccione **Guardar**.	a. Seleccione el nombre del extremo para mostrar los detalles. b. Seleccione el icono de edición . c. Introduzca el nuevo nombre. d. Seleccione **Guardar**.
Edite el puerto de punto final	a. Seleccione la casilla de verificación para el punto final. b. Selecciona **Acciones** > **Editar puerto de punto final** c. Introduzca un número de puerto válido. d. Seleccione **Guardar**.	*n/a*
Edite el modo de enlace de punto final	a. Seleccione la casilla de verificación para el punto final. b. Seleccione **acciones** > **Editar modo de enlace de punto final**. c. Actualice el modo de enlace según sea necesario. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del extremo para mostrar los detalles. b. Seleccione **Editar modo de enlace**. c. Actualice el modo de enlace según sea necesario. d. Seleccione **Guardar cambios**.
Editar certificado de extremo	a. Seleccione la casilla de verificación para el punto final. b. Seleccione **acciones** > **Editar certificado de punto final**. c. Cargue o genere un nuevo certificado personalizado o comience a usar el certificado global S3 y Swift, según sea necesario. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del extremo para mostrar los detalles. b. Seleccione la ficha **Certificado**. c. Seleccione **Editar certificado**. d. Cargue o genere un nuevo certificado personalizado o comience a usar el certificado global S3 y Swift, según sea necesario. e. Seleccione **Guardar cambios**.

Tarea	Menú Actions	Detalles
Editar el acceso de inquilinos	a. Seleccione la casilla de verificación para el punto final. b. Selecciona **Acciones** > **Editar acceso de inquilino**. c. Elija una opción de acceso diferente, seleccione o elimine arrendatarios de la lista, o realice ambas acciones. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del extremo para mostrar los detalles. b. Seleccione la pestaña **Acceso de inquilino**. c. Selecciona **Editar acceso de inquilino**. d. Elija una opción de acceso diferente, seleccione o elimine arrendatarios de la lista, o realice ambas acciones. e. Seleccione **Guardar cambios**.

Retire los extremos del equilibrador de carga

Puede eliminar uno o varios puntos finales mediante el menú **acciones** o puede eliminar un único punto final de la página de detalles.

> Para evitar que se produzcan interrupciones en el cliente, actualice las aplicaciones cliente S3 o Swift afectadas antes de eliminar un extremo de equilibrio de carga. Actualice cada cliente para que se conecte utilizando un puerto asignado a otro extremo de equilibrador de carga. Asegúrese de actualizar también la información de certificado necesaria.

> Si pierde el acceso a Grid Manager al eliminar un extremo de interfaz de gestión, actualice la dirección URL.

- Para eliminar uno o varios puntos finales:
  a. En la página Equilibrador de Carga, seleccione la casilla de verificación de cada punto final que desee eliminar.
  b. Seleccione **acciones** > **Quitar**.
  c. Seleccione **OK**.
- Para eliminar un extremo de la página de detalles:
  a. Desde la página Load equilibrador. seleccione el nombre del extremo.
  b. Seleccione **Quitar** en la página de detalles.
  c. Seleccione **OK**.

Configure los nombres de dominio de punto final S3

Para admitir S3 solicitudes de estilo hospedado virtual, debe utilizar Grid Manager para configurar la lista de S3 nombres de dominio de punto final a los que se conectan los clientes S3.

> El uso de una dirección IP para un nombre de dominio de punto final no es compatible. Las próximas versiones impedirán esta configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Ha confirmado que no hay una actualización de grid en curso.

> No realice ningún cambio en la configuración del nombre de dominio cuando haya una actualización de cuadrícula en curso.

Acerca de esta tarea

Para habilitar a los clientes que usen nombres de dominio extremo de S3, debe realizar todas las siguientes acciones:

- Use Grid Manager para añadir los nombres de dominio de extremo S3 al sistema StorageGRID.
- Asegúrese de que el "Certificado que el cliente utiliza para las conexiones HTTPS a StorageGRID" está firmado para todos los nombres de dominio que el cliente requiere.

  Por ejemplo, si el extremo es `s3.company.com`, Debe asegurarse de que el certificado utilizado para las conexiones HTTPS incluye `s3.company.com` Nombre alternativo (SAN) del asunto comodín del extremo y del extremo: `*.s3.company.com`.

- Configure el servidor DNS que utiliza el cliente. Incluya registros DNS para las direcciones IP que los clientes utilizan para realizar conexiones y asegúrese de que los registros hacen referencia a todos los nombres de dominio de punto final S3 necesarios, incluidos los nombres comodín.

> Los clientes se pueden conectar a StorageGRID mediante la dirección IP de un nodo de puerta de enlace, un nodo de administrador o un nodo de almacenamiento, o bien mediante la conexión a la dirección IP virtual de un grupo de alta disponibilidad. Debe comprender cómo se conectan las aplicaciones cliente a la cuadrícula para que incluya las direcciones IP correctas en los registros DNS.

Los clientes que usan conexiones HTTPS (recomendadas) a la cuadrícula pueden usar cualquiera de los siguientes certificados:

- Los clientes que se conectan a un extremo de equilibrador de carga pueden utilizar un certificado personalizado para ese extremo. Cada punto final de equilibrio de carga se puede configurar para reconocer diferentes nombres de dominio de punto final S3.
- Los clientes que se conectan a un extremo de balanceador de carga o directamente a un nodo de almacenamiento pueden personalizar el certificado de API global S3 y Swift para que incluya todos los nombres de dominio de extremo S3 requeridos.

> Si no agrega nombres de dominio de punto final S3 y la lista está vacía, se deshabilitará el soporte para S3 solicitudes de estilo hospedado virtual.

Agregue un nombre de dominio de punto final S3

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **S3 nombres de dominio de punto final**.
2. Introduzca el nombre de dominio en el campo **Nombre de dominio 1**. Seleccione **Agregar otro nombre de dominio** para agregar más nombres de dominio.

3. Seleccione **Guardar**.
4. Asegúrese de que los certificados de servidor que utilizan los clientes coinciden con los nombres de dominio de punto final S3 necesarios.
   - Si los clientes se conectan a un punto final del equilibrador de carga que utiliza su propio certificado, "actualice el certificado asociado al punto final".
   - Si los clientes se conectan a un extremo de balanceador de carga que utiliza el certificado de API S3 y Swift global o directamente a los nodos de almacenamiento, "Actualice el certificado de API global S3 y Swift".
5. Agregue los registros DNS necesarios para garantizar que se puedan resolver las solicitudes de nombres de dominio de extremo.

Resultado

Ahora, cuando los clientes utilizan el extremo *`bucket.s3.company.com`*, El servidor DNS resuelve el punto final correcto y el certificado autentica el punto final como se esperaba.

Cambie el nombre de un nombre de dominio de punto final S3

Si cambia un nombre utilizado por las aplicaciones S3, las solicitudes de estilo hospedado virtual fallarán.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **S3 nombres de dominio de punto final**.
2. Seleccione el campo de nombre de dominio que desea editar y realice los cambios necesarios.
3. Seleccione **Guardar**.
4. Selecciona **Sí** para confirmar tu cambio.

Suprimir un nombre de dominio de punto final S3

Si elimina un nombre utilizado por las aplicaciones S3, las solicitudes de estilo hospedado virtual fallarán.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **S3 nombres de dominio de punto final**.
2. Seleccione el icono de eliminar ✕ junto al nombre de dominio.
3. Seleccione **Sí** para confirmar la eliminación.

Información relacionada

- "USE LA API DE REST DE S3"
- "Ver direcciones IP"
- "Configuración de grupos de alta disponibilidad"

Resumen: Direcciones IP y puertos para conexiones cliente

Para almacenar o recuperar objetos, las aplicaciones cliente S3 y Swift se conectan al servicio de equilibrio de carga, que se incluye en todos los nodos de administración y de puerta de enlace, o al servicio de enrutador de distribución local (LDR), que se incluye en todos los nodos de almacenamiento.

Las aplicaciones cliente se pueden conectar a StorageGRID mediante la dirección IP de un nodo de cuadrícula y el número de puerto del servicio en ese nodo. Opcionalmente, puede crear grupos de alta

disponibilidad (HA) de nodos de equilibrio de carga para proporcionar conexiones altamente disponibles que utilicen direcciones IP virtuales (VIP). Si desea conectarse a StorageGRID con un nombre de dominio completo (FQDN) en lugar de una dirección IP o VIP, puede configurar entradas de DNS.

Esta tabla resume las distintas formas en que los clientes pueden conectarse a StorageGRID y las direcciones IP y los puertos que se utilizan para cada tipo de conexión. Si ya ha creado extremos del balanceador de carga y grupos de alta disponibilidad (HA), consulte Dónde encontrar direcciones IP Para localizar estos valores en Grid Manager.

Dónde se realiza la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
Grupo de ALTA DISPONIBILIDAD	Equilibrador de carga	La dirección IP virtual de un grupo de alta disponibilidad	Puerto asignado al punto final del equilibrador de carga
Nodo de administración	Equilibrador de carga	La dirección IP del nodo de administrador	Puerto asignado al punto final del equilibrador de carga
Nodo de puerta de enlace	Equilibrador de carga	La dirección IP del nodo de puerta de enlace	Puerto asignado al punto final del equilibrador de carga
Nodo de almacenamiento	LDR	La dirección IP del nodo de almacenamiento	Puertos S3 predeterminados: • HTTPS: 18082 • HTTP: 18084 Puertos Swift predeterminados: • HTTPS: 18083 • HTTP:18085

URL de ejemplo

Para conectar una aplicación cliente al punto final del equilibrador de carga de un grupo HA de nodos de gateway, utilice una URL estructurada como se muestra a continuación:

`https://VIP-of-HA-group:LB-endpoint-port`

Por ejemplo, si la dirección IP virtual del grupo HA es 192.0.2.5 y el número de puerto del extremo del equilibrador de carga es 10443, una aplicación podría utilizar la siguiente URL para conectarse a StorageGRID:

`https://192.0.2.5:10443`

Dónde encontrar direcciones IP

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Para encontrar la dirección IP de un nodo de grid:
   a. Selecciona **NODOS**.
   b. Seleccione el nodo de administrador, Gateway Node o Storage Node al que desea conectarse.
   c. Seleccione la ficha **Descripción general**.
   d. En la sección Node Information, tenga en cuenta las direcciones IP del nodo.
   e. Seleccione **Mostrar más** para ver las direcciones IPv6 y las asignaciones de interfaz.

      Puede establecer conexiones desde aplicaciones cliente a cualquiera de las direcciones IP de la lista:

      - **Eth0:** Red Grid
      - **Eth1:** Red de administración (opcional)
      - **Eth2:** Red cliente (opcional)

      > Si va a ver un nodo de administrador o un nodo de puerta de enlace y es el nodo activo de un grupo de alta disponibilidad, en eth2 se muestra la dirección IP virtual del grupo de alta disponibilidad.

3. Para buscar la dirección IP virtual de un grupo de alta disponibilidad:
   a. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
   b. En la tabla, tenga en cuenta la dirección IP virtual del grupo ha.
4. Para buscar el número de puerto de un extremo Load Balancer:
   a. Seleccione **CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**.
   b. Tenga en cuenta el número de puerto del punto final que desea utilizar.

      > Si el número de puerto es 80 o 443, el punto final se configura sólo en los nodos de Gateway, ya que esos puertos están reservados en los nodos Admin. Todos los demás puertos están configurados tanto en los nodos de puerta de enlace como en los de administración.

   c. Seleccione el nombre del punto final de la tabla.
   d. Confirme que el **Client type** (S3 o Swift) coincide con la aplicación cliente que utilizará el punto final.

Administrar redes y conexiones

Configurar ajustes de red: Información general

Puede configurar varios ajustes de red desde el Gestor de cuadrícula para ajustar el funcionamiento del sistema StorageGRID.

Configure las interfaces VLAN

Puede hacerlo "Cree interfaces de LAN virtual (VLAN)" para aislar y crear particiones del tráfico con el fin de mejorar la seguridad, la flexibilidad y el rendimiento. Cada interfaz de VLAN está asociada con una o varias interfaces principales en los nodos de administración y de puerta de enlace. Puede utilizar interfaces VLAN en

grupos de alta disponibilidad y en extremos de equilibrador de carga para segregar el tráfico cliente o administrador por aplicación o inquilino.

Directivas de clasificación de tráfico

Puede utilizar "políticas de clasificación de tráfico" para identificar y gestionar diferentes tipos de tráfico de red, incluido el tráfico relacionado con buckets específicos, inquilinos, subredes de cliente o extremos de equilibrador de carga. Estas políticas pueden ayudar a limitar y supervisar el tráfico.

Directrices para redes StorageGRID

Puede utilizar Grid Manager para configurar y administrar redes y conexiones StorageGRID.

Consulte "Configure las conexiones de clientes S3 y Swift" Para aprender a conectar clientes S3 o Swift.

Redes StorageGRID predeterminadas

De forma predeterminada, StorageGRID admite tres interfaces de red por nodo de grid, lo que permite configurar las redes para cada nodo de grid individual de modo que se ajusten a sus requisitos de seguridad y acceso.

Para obtener más información acerca de la topología de red, consulte "Directrices sobre redes".

Red Grid

Obligatorio. La red de red se utiliza para todo el tráfico interno de StorageGRID. Proporciona conectividad entre todos los nodos de la cuadrícula, en todos los sitios y subredes.

Red de administración

Opcional. La red de administración suele utilizarse para la administración y el mantenimiento del sistema. También se puede utilizar para el acceso a protocolos de cliente. La red de administración suele ser una red privada y no es necesario que se pueda enrutar entre sitios.

Red cliente

Opcional. La red cliente es una red abierta que se suele utilizar para proporcionar acceso a aplicaciones cliente S3 y Swift, de modo que la red Grid se pueda aislar y proteger. La red de cliente puede comunicarse con cualquier subred accesible a través de la puerta de enlace local.

Directrices

- Cada nodo StorageGRID requiere una interfaz de red dedicada, dirección IP, máscara de subred y pasarela para cada red a la que se asigna.
- Un nodo de grid no puede tener más de una interfaz en una red.
- Se admite una sola puerta de enlace, por red y cada nodo de grid, y debe estar en la misma subred que el nodo. Si es necesario, puede implementar un enrutamiento más complejo en la puerta de enlace.
- En cada nodo, cada red asigna una interfaz de red específica.

Red	Nombre de la interfaz
Cuadrícula	eth0
Admin (opcional)	eth1
Cliente (opcional)	eth2

- Si el nodo está conectado a un dispositivo StorageGRID, se utilizan puertos específicos para cada red. Para obtener más información, consulte las instrucciones de instalación del dispositivo.
- La ruta predeterminada se genera automáticamente, por nodo. Si eth2 está habilitado, 0.0.0.0/0 utiliza la red cliente en eth2. Si eth2 no está habilitado, 0.0.0.0/0 utiliza la red de cuadrícula en eth0.
- La red cliente no se pone en funcionamiento hasta que el nodo de grid se ha Unido a la cuadrícula
- La red de administrador se puede configurar durante la puesta en marcha del nodo de grid para permitir el acceso a la interfaz de usuario de la instalación antes de que la cuadrícula esté totalmente instalada.

Interfaces opcionales

Opcionalmente, se pueden añadir interfaces adicionales a un nodo. Por ejemplo, puede agregar una interfaz troncal a un nodo de administración o de puerta de enlace, para poder utilizar "Interfaces de VLAN" para segregar el tráfico que pertenece a diferentes aplicaciones o arrendatarios. O bien, puede que desee añadir una interfaz de acceso para utilizarla en un "Grupo de alta disponibilidad".

Para añadir enlaces troncales o interfaces de acceso, consulte lo siguiente:

- **VMware (después de instalar el nodo)**: "VMware: Añada tronco o interfaces de acceso a un nodo"
  - **Red Hat Enterprise Linux (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
  - **Ubuntu o Debian (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
  - **RHEL, Ubuntu o Debian (después de instalar el nodo)**: "Linux: Añada tronco o interfaces de acceso a un nodo"

Ver direcciones IP

Puede ver la dirección IP de cada nodo de grid en el sistema StorageGRID. Luego, puede usar esta dirección IP para iniciar sesión en el nodo de la cuadrícula en la línea de comandos y realizar diversos procedimientos de mantenimiento.

Antes de empezar

Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".

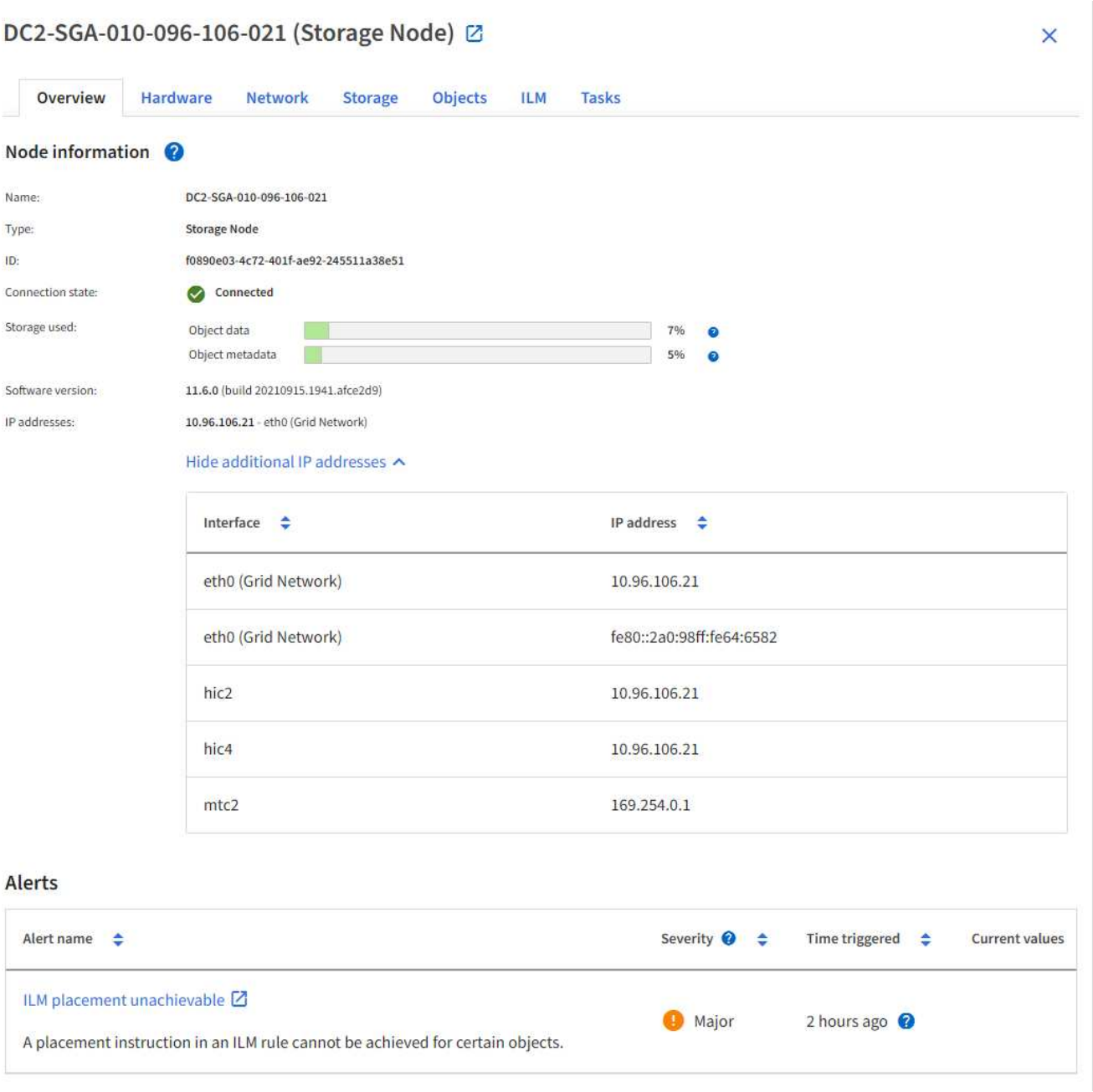
Acerca de esta tarea

Para obtener más información sobre cómo cambiar direcciones IP, consulte "Configurar las direcciones IP".

Pasos

1. Seleccione **NODES** > ***grid node*** > **Descripción general**.
2. Seleccione **Mostrar más** a la derecha del título direcciones IP.

   Las direcciones IP de ese nodo de grid se enumeran en una tabla.



Configure las interfaces VLAN

Puede crear interfaces de LAN virtual (VLAN) en nodos de administrador y de puerta de enlace, y usarlas en grupos de alta disponibilidad y extremos de equilibrador de carga para aislar y dividir el tráfico para garantizar la seguridad, la flexibilidad y el rendimiento.

Consideraciones sobre las interfaces VLAN

- Para crear una interfaz de VLAN, introduzca un ID de VLAN y elija una interfaz principal en uno o varios nodos.
- Se debe configurar una interfaz padre como interfaz troncal en el conmutador.
- Una interfaz principal puede ser Grid Network (eth0), Client Network (eth2) o una interfaz troncal adicional para la máquina virtual o el host con configuración básica (por ejemplo, ens256).

- Para cada interfaz de VLAN, solo puede seleccionar una interfaz principal para un nodo determinado. Por ejemplo, no puede utilizar la interfaz de red de grid y la interfaz de red de cliente en el mismo nodo de gateway que la interfaz principal para la misma VLAN.
- Si la interfaz de VLAN es para el tráfico del nodo de administración, que incluye tráfico relacionado con el administrador de grid y el administrador de inquilinos, seleccione interfaces sólo en nodos de administración.
- Si la interfaz de VLAN es para el tráfico de clientes S3 o Swift, seleccione interfaces en nodos de administrador o nodos de puerta de enlace.
- Si necesita agregar interfaces de línea externa, consulte lo siguiente para obtener más información:
  - **VMware (después de instalar el nodo)**: "VMware: Añada tronco o interfaces de acceso a un nodo"
  - **RHEL (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
  - **Ubuntu o Debian (antes de instalar el nodo)**: "Crear archivos de configuración del nodo"
  - **RHEL, Ubuntu o Debian (después de instalar el nodo)**: "Linux: Añada tronco o interfaces de acceso a un nodo"

Cree una interfaz VLAN

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".
- Se ha configurado una interfaz de línea externa en la red y está conectada al nodo de máquina virtual o Linux. Conoce el nombre de la interfaz troncal.
- Conoce el ID de la VLAN que desea configurar.

Acerca de esta tarea

El administrador de red podría haber configurado una o más interfaces troncales y una o varias VLAN para separar el tráfico de administración o cliente que pertenezca a diferentes aplicaciones o inquilinos. Cada VLAN se identifica por un ID o etiqueta numéricos. Por ejemplo, la red puede utilizar VLAN 100 para el tráfico FabricPool y VLAN 200 para una aplicación de archivado.

Puede utilizar Grid Manager para crear interfaces VLAN que permitan a los clientes acceder a StorageGRID en una VLAN específica. Cuando se crean interfaces VLAN, se especifica el identificador de VLAN y se seleccionan las interfaces principales (troncales) en uno o varios nodos.

Acceda al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **interfaces VLAN**.
2. Seleccione **Crear**.

Introduzca los detalles de las interfaces de VLAN

Pasos

1. Especifique el ID de la VLAN en la red. Puede introducir cualquier valor entre 1 y 4094.

   Los ID de VLAN no tienen por qué ser únicos. Por ejemplo, puede utilizar el identificador de VLAN 200 para el tráfico de administración en un sitio y el mismo identificador de VLAN para el tráfico de cliente en otro sitio. Puede crear interfaces VLAN independientes con diferentes conjuntos de interfaces principales

en cada sitio. Sin embargo, dos interfaces de VLAN con el mismo ID no pueden compartir la misma interfaz en un nodo.
Si especifica un ID que ya se ha utilizado, aparecerá un mensaje.

2. De manera opcional, introduzca una breve descripción para la interfaz de VLAN.
3. Seleccione **continuar**.

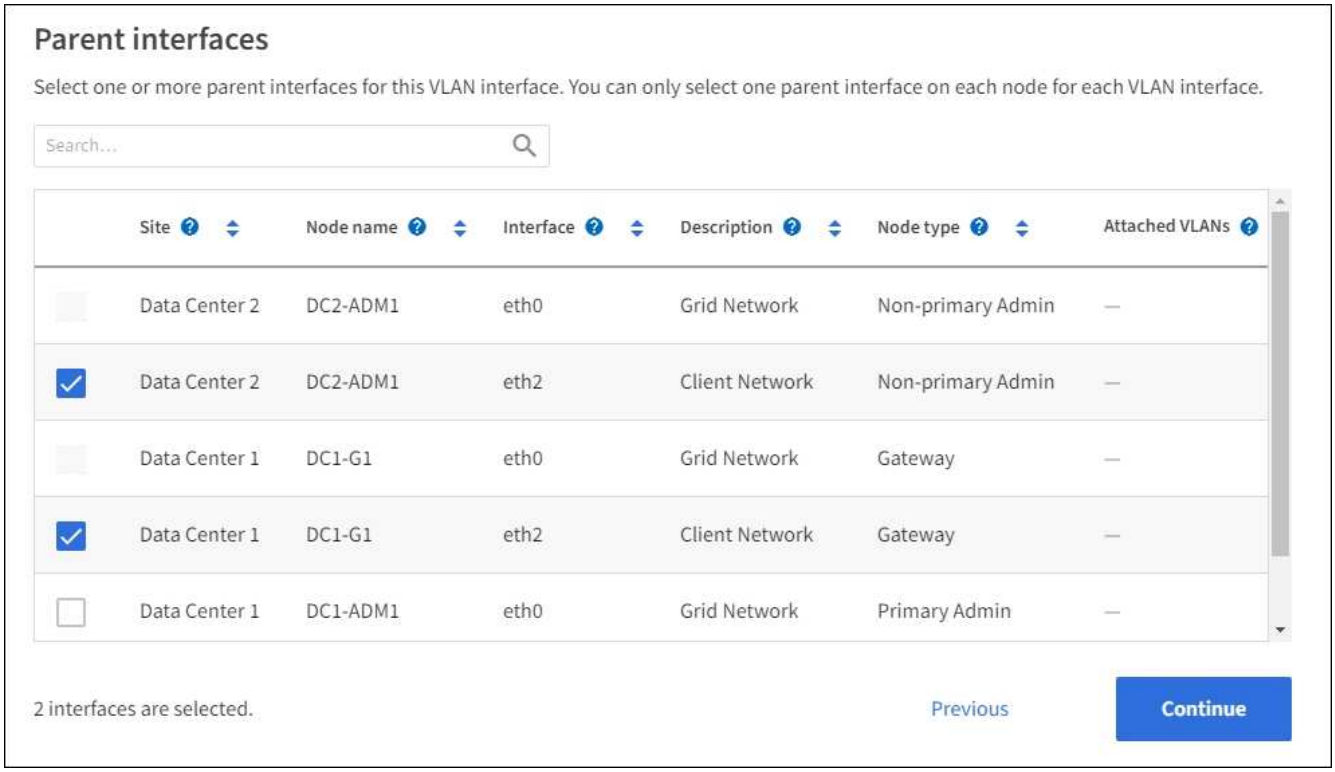
Elija interfaces padre

En la tabla, se enumeran las interfaces disponibles para todos los nodos de administrador y los nodos de puerta de enlace en cada sitio del grid. Las interfaces de la red de administración (eth1) no se pueden utilizar como interfaces principales y no se muestran.

Pasos

1. Seleccione una o varias interfaces primarias para asociar esta VLAN.

   Por ejemplo, es posible que desee conectar una VLAN a la interfaz de red de cliente (eth2) para un nodo de puerta de enlace y un nodo de administrador.



2. Seleccione **continuar**.

Confirme la configuración

Pasos

1. Revise la configuración y realice cualquier cambio.
   - Si necesita cambiar el ID de VLAN o la descripción, seleccione **introducir detalles de VLAN** en la parte superior de la página.
   - Si necesita cambiar una interfaz padre, seleccione **elegir interfaces padre** en la parte superior de la página o seleccione **anterior**.

- Si necesita quitar una interfaz principal, seleccione la papelera .

2. Seleccione **Guardar**.
3. Espere hasta 5 minutos para que la nueva interfaz aparezca como una selección en la página grupos de alta disponibilidad y aparezca en la tabla * interfaces de red* para el nodo (**NODES** > ***nodo de interfaz principal*** > **Red**).

Edite una interfaz VLAN

Cuando edite una interfaz de VLAN, puede realizar los siguientes tipos de cambios:

- Cambie el ID o la descripción de la VLAN.
- Agregar o quitar interfaces principales.

Por ejemplo, es posible que desee quitar una interfaz principal de una interfaz VLAN si va a retirar el nodo asociado.

Tenga en cuenta lo siguiente:

- No puede cambiar un ID de VLAN si la interfaz VLAN se utiliza en un grupo de alta disponibilidad.
- No puede quitar una interfaz principal si se utiliza esa interfaz principal en un grupo de alta disponibilidad.

  Por ejemplo, supongamos que la VLAN 200 está conectada a las interfaces principales de los nodos A y B. Si un grupo de alta disponibilidad utiliza la interfaz VLAN 200 para el nodo A y la interfaz eth2 para el nodo B, puede eliminar la interfaz principal no utilizada para el nodo B, pero no puede quitar la interfaz principal usada para el nodo A.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **interfaces VLAN**.
2. Seleccione la casilla de comprobación de la interfaz de VLAN que desea editar. A continuación, seleccione **acciones** > **Editar**.
3. Si lo desea, actualice el ID de VLAN o la descripción. A continuación, seleccione **continuar**.

   No se puede actualizar un identificador de VLAN si la VLAN se utiliza en un grupo de alta disponibilidad.

4. Opcionalmente, active o desactive las casillas de verificación para agregar interfaces principales o para eliminar las interfaces no utilizadas. A continuación, seleccione **continuar**.
5. Revise la configuración y realice cualquier cambio.
6. Seleccione **Guardar**.

Quite una interfaz VLAN

Puede eliminar una o varias interfaces VLAN.

No puede quitar una interfaz VLAN si actualmente se utiliza en un grupo de alta disponibilidad. Para poder eliminarlo, debe quitar la interfaz VLAN del grupo ha.

Para evitar cualquier interrupción en el tráfico de cliente, considere realizar una de las siguientes acciones:

- Añada una nueva interfaz VLAN al grupo de alta disponibilidad antes de eliminar esta interfaz de VLAN.
- Cree un nuevo grupo de alta disponibilidad que no utilice esta interfaz VLAN.

- Si la interfaz VLAN que desea quitar tiene actualmente la interfaz activa, edite el grupo de alta disponibilidad. Mueva la interfaz de VLAN que desea quitar a la parte inferior de la lista de prioridades. Espere hasta que se establezca la comunicación en la nueva interfaz principal y, a continuación, quite la interfaz antigua del grupo de alta disponibilidad. Por último, elimine la interfaz de VLAN en ese nodo.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **interfaces VLAN**.
2. Seleccione la casilla de comprobación de cada interfaz de VLAN que desea quitar. A continuación, seleccione **acciones** > **Eliminar**.
3. Seleccione **Sí** para confirmar su selección.

   Se eliminan todas las interfaces VLAN seleccionadas. Se muestra un banner verde de éxito en la página de interfaces de VLAN.

Administrar directivas de clasificación de tráfico

Gestionar políticas de clasificación de tráfico: Información general

Para mejorar sus ofertas de calidad de servicio (QoS), puede crear normativas de clasificación del tráfico para identificar y supervisar distintos tipos de tráfico de red. Estas políticas pueden ayudar a limitar y supervisar el tráfico.

Las políticas de clasificación del tráfico se aplican a los extremos en el servicio StorageGRID Load Balancer para los nodos de puerta de enlace y los nodos de administración. Para crear directivas de clasificación de tráfico, debe haber creado ya puntos finales de equilibrador de carga.

Reglas de coincidencia

Cada directiva de clasificación de tráfico contiene una o más reglas coincidentes para identificar el tráfico de red relacionado con una o varias de las siguientes entidades:

- Cucharones
- Subred
- Inquilino
- Puntos finales del equilibrador de carga

StorageGRID supervisa el tráfico que coincide con cualquier regla dentro de la política de acuerdo con los objetivos de la regla. Cualquier tráfico que coincida con cualquier regla de una directiva se gestiona mediante dicha directiva. A la inversa, puede establecer reglas que coincidan con todo el tráfico excepto una entidad especificada.

Limitación del tráfico

Opcionalmente, puede agregar los siguientes tipos de límite a una política:

- Ancho de banda de agregado
- Ancho de banda por solicitud
- Solicitudes simultáneas
- Tasa de solicitud

Los valores límite se aplican por cada equilibrador de carga. Si el tráfico se distribuye de forma simultánea entre varios equilibradores de carga, las tasas máximas totales son un múltiplo de los límites de velocidad que especifique.

> Puede crear políticas para limitar el ancho de banda agregado o para limitar el ancho de banda por solicitud. Sin embargo, la StorageGRID no puede limitar ambos tipos de ancho de banda a la vez. Los límites de ancho de banda agregados pueden imponer un impacto adicional mínimo en el rendimiento en el tráfico no limitado.

Para límites de ancho de banda agregados o por solicitud, las solicitudes se transmiten de entrada o salida a la velocidad establecida. StorageGRID sólo puede aplicar una velocidad, por lo que la política más específica, por tipo de matrcher, es la aplicada. El ancho de banda consumido por la solicitud no cuenta en comparación con otras políticas que coincidan menos específicas que contengan políticas de límite de ancho de banda agregado. Para todos los demás tipos de límites, las solicitudes de clientes se retrasan 250 milisegundos y reciben una respuesta de reducción lenta de 503 para las solicitudes que exceden cualquier límite de directiva coincidente.

En Grid Manager, puede ver los gráficos de tráfico y comprobar que las directivas están aplicando los límites de tráfico que espera.

Utilice las políticas de clasificación del tráfico con los SLA

Puede utilizar políticas de clasificación del tráfico junto con los límites de capacidad y protección de datos para aplicar acuerdos de nivel de servicio (SLA) que ofrezcan detalles sobre la capacidad, la protección de datos y el rendimiento.

El siguiente ejemplo muestra tres niveles de un acuerdo de nivel de servicio. Puede crear políticas de clasificación del tráfico para alcanzar los objetivos de rendimiento de cada nivel de SLA.

Nivel de servicio	Capacidad	Protección de datos	El máximo rendimiento permitido	Coste
Oro	1 PB de almacenamiento permitido	Regla de 3 copia de ILM	25 000 solicitudes/s 5 GB/s (40 Gbps) de ancho de banda	por mes
Plata	Capacidad de almacenamiento de 250 TB	2 regla de copia de ILM	10 K solicitudes/seg Ancho de banda de 1.25 GB/s (10 Gbps)	$$ al mes
Bronce	100 TB de almacenamiento permitido	2 regla de copia de ILM	5 K solicitudes/seg 1 GB/s (8 Gbps) de ancho de banda	$ al mes

Cree directivas de clasificación de tráfico

Puede crear políticas de clasificación del tráfico si desea supervisar y, de manera opcional, limitar el tráfico de red por bloque, periodo de reunión, CIDR, extremo de

equilibrador de carga o inquilino. De manera opcional, puede establecer límites para una política en función del ancho de banda, el número de solicitudes simultáneas o la tasa de solicitudes.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".
- Ha creado cualquier punto final de equilibrador de carga que desee que coincida.
- Ha creado los inquilinos que desea que coincidan.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.
2. Seleccione **Crear**.
3. Introduzca un nombre y una descripción (opcional) para la política y seleccione **Continuar**.

   Por ejemplo, describa a qué se aplica esta política de clasificación del tráfico y a qué se limitará.

4. Seleccione **Añadir regla** y especifique los siguientes detalles para crear una o más reglas de coincidencia para la política. Cualquier política que cree debe tener al menos una regla de coincidencia. Seleccione **continuar**.

Campo	Descripción
Tipo	Seleccione los tipos de tráfico a los que se aplica la regla de coincidencia. Los tipos de tráfico son bucket, bucket regex, CIDR, load balancer endpoint y tenant.
Valor de coincidencia	Introduzca el valor que coincida con el tipo seleccionado. • Bucket: Introduzca uno o más nombres de bucket. • Bucket Regex: Introduzca una o más expresiones regulares utilizadas para hacer coincidir un juego de nombres de cubos. La expresión regular no está anclada. Utilice el anclaje ^ para que coincida al principio del nombre del cubo y utilice el anclaje $ para que coincida al final del nombre. La coincidencia de expresiones regulares admite un subconjunto de sintaxis PCRE (expresión regular compatible con Perl). • CIDR: Introduzca una o más subredes IPv4, en notación CIDR, que coincida con la subred deseada. • Punto final de equilibrio de carga: Seleccione un nombre de punto final. Estos son los puntos finales del equilibrador de carga definidos en "Configurar puntos finales del equilibrador de carga". • Tenant: La coincidencia de inquilinos utiliza el ID de clave de acceso. Si la solicitud no contiene un identificador de clave de acceso (por ejemplo, acceso anónimo), la propiedad del bloque al que se accede se utiliza para determinar el inquilino.

Campo	Descripción
Coincidencia inversa	Si desea hacer coincidir todo el tráfico de red *excepto* tráfico consistente con el valor Tipo y Coincidencia que acaba de definir, seleccione la casilla de verificación **Coincidencia inversa**. De lo contrario, deje la casilla de verificación desactivada. Por ejemplo, si desea que esta política se aplique a todos los puntos finales excepto a uno de los de equilibrio de carga, especifique el punto final de equilibrio de carga que se va a excluir y seleccione **Coincidencia inversa**. Para una directiva que contiene varios matchers donde al menos uno es un matcher inverso, tenga cuidado de no crear una política que coincida con todas las solicitudes.

5. Opcionalmente, seleccione **Agregar un límite** y seleccione los siguientes detalles para agregar uno o más límites para controlar el tráfico de red que coincide con una regla.

> StorageGRID recopila métricas incluso si no agrega ningún límite, para que pueda comprender las tendencias del tráfico.

Campo	Descripción
Tipo	El tipo de límite que desea aplicar al tráfico de red coincidente con la regla. Por ejemplo, puede limitar el ancho de banda o la tasa de solicitud. **Nota**: Puede crear políticas para limitar el ancho de banda agregado o limitar el ancho de banda por solicitud. Sin embargo, la StorageGRID no puede limitar ambos tipos de ancho de banda a la vez. Cuando se utiliza el ancho de banda agregado, el ancho de banda por solicitud no está disponible. Por el contrario, cuando se utiliza el ancho de banda por solicitud, el ancho de banda agregado no estará disponible. Los límites de ancho de banda agregados pueden imponer un impacto adicional mínimo en el rendimiento en el tráfico no limitado. Para los límites de ancho de banda, StorageGRID aplica la política que mejor se adapte al tipo de conjunto de límites. Por ejemplo, si tiene una directiva que limita el tráfico en una sola dirección, entonces el tráfico en la dirección opuesta será ilimitado, aunque haya tráfico que coincida con las directivas adicionales que tengan límites de ancho de banda. StorageGRID implanta las «mejores» coincidencias para los límites de ancho de banda en el siguiente orden: • Dirección IP exacta (/máscara 32) • Nombre exacto del cucharón • Regex. Cucharón • Inquilino • Extremo • Coincidencias CIDR no exactas (no /32) • Coincidencias inversas

Campo	Descripción
Se aplica a.	Si este límite se aplica a las solicitudes de lectura del cliente (GET o HEAD) o las solicitudes de escritura (PUT, POST o DELETE).
Valor	El valor al que se limitará el tráfico de red, en función de la unidad que seleccione. Por ejemplo, introduzca 10 y seleccione MiB/s para evitar que el tráfico de red que coincide con esta regla supere los 10 MiB/s. **Nota**: Dependiendo de la configuración de unidades, las unidades disponibles serán binarias (por ejemplo, GiB) o decimales (por ejemplo, GB). Para cambiar la configuración de unidades, seleccione la lista desplegable de usuario en la parte superior derecha del Administrador de cuadrícula y, a continuación, seleccione **Preferencias de usuario**.
Unidad	La unidad que describe el valor introducido.

Por ejemplo, si desea crear un límite de ancho de banda de 40 GB/s para un nivel de SLA, cree dos límites de ancho de banda agregados: GET/HEAD at 40 GB/s y PUT/POST/DELETE at 40 GB/s.

6. Seleccione **continuar**.
7. Lea y revise la política de clasificación de tráfico. Utilice el botón **Anterior** para volver atrás y realizar los cambios necesarios. Cuando esté satisfecho con la política, seleccione **Guardar y continuar**.

   El tráfico de clientes S3 y Swift ahora se maneja de acuerdo con la política de clasificación del tráfico.

Después de terminar

"Ver las métricas de tráfico de red" para verificar que las políticas están aplicando los límites de tráfico que espera.

Edite la política de clasificación de tráfico

Puede editar una directiva de clasificación de tráfico para cambiar su nombre o descripción, o para crear, editar o eliminar cualquier regla o límite para la directiva.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

Pasos

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

   Aparece la página Políticas de clasificación de tráfico y las políticas existentes se muestran en una tabla.

2. Edite la política mediante el menú Acciones o la página de detalles. Consulte "crear políticas de clasificación de tráfico" para qué entrar.

Menú Actions

a. Seleccione la casilla de verificación de la política.

b. Selecciona **Acciones** > **Editar**.

Detalles

a. Seleccione el nombre de la política.

b. Seleccione el botón **Editar** junto al nombre de la política.

3. Para el paso Introducir nombre de política, edite opcionalmente el nombre o la descripción de la política y seleccione **Continuar**.
4. Para el paso Agregar reglas de coincidencia, opcionalmente agregue una regla o edite el **Tipo** y **Valor de coincidencia** de la regla existente, y seleccione **Continuar**.
5. Para el paso Establecer límites, opcionalmente agregue, edite o elimine un límite, y seleccione **Continuar**.
6. Revise la política actualizada y seleccione **Guardar y continuar**.

   Los cambios realizados en la directiva se guardan y el tráfico de red se gestiona de acuerdo con las directivas de clasificación del tráfico. Puede ver los gráficos de tráfico y comprobar que las directivas están aplicando los límites de tráfico que espera.

Eliminar una directiva de clasificación de tráfico

Puede eliminar una política de clasificación de tráfico si ya no la necesita. Asegúrese de eliminar la política correcta porque no se puede recuperar una política al eliminarla.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

Pasos

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

   Aparece la página Políticas de clasificación de tráfico con las políticas existentes enumeradas en una tabla.

2. Elimine la política mediante el menú Acciones o la página de detalles.

   Menú Actions

   a. Seleccione la casilla de verificación de la política.

   b. Seleccione **acciones** > **Quitar**.

   Página de detalles de política

   a. Seleccione el nombre de la política.

   b. Seleccione el botón **Eliminar** junto al nombre de la política.

3. Seleccione **Sí** para confirmar que desea eliminar la política.

La directiva se elimina.

Ver las métricas de tráfico de red

Puede supervisar el tráfico de red mediante los gráficos que están disponibles en la página de políticas de clasificación del tráfico.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Acceso raíz o cuentas de inquilino".

Acerca de esta tarea

Para cualquier política de clasificación de tráfico existente, puede ver métricas para el servicio de equilibrio de carga para determinar si la política está limitando correctamente el tráfico en toda la red. Los datos de los gráficos pueden ayudarle a determinar si necesita ajustar la política.

Incluso si no se establecen límites para una política de clasificación del tráfico, se recopilan las métricas y los gráficos proporcionan información útil para comprender las tendencias del tráfico.

Pasos

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

   Aparece la página Políticas de clasificación de tráfico y las políticas existentes se muestran en la tabla.

2. Seleccione el nombre de la política de clasificación de tráfico para la que desea ver las métricas.
3. Seleccione la pestaña **Métricas**.

   Aparecen los gráficos de política de clasificación de tráfico. Los gráficos muestran métricas solo para el tráfico que coincide con la directiva seleccionada.

   Los siguientes gráficos se incluyen en la página.

   - Tasa de solicitud: Este gráfico proporciona la cantidad de ancho de banda que coincide con esta política manejada por todos los equilibradores de carga. Los datos recibidos incluyen cabeceras de solicitud para todas las solicitudes y tamaño de datos de cuerpo para las respuestas que tienen datos de cuerpo. Enviado incluye cabeceras de respuesta para todas las solicitudes y tamaño de datos de cuerpo de respuesta para las solicitudes que incluyen datos de cuerpo en la respuesta.

     > Cuando se completan las solicitudes, este gráfico sólo muestra el uso del ancho de banda. Para solicitudes de objetos lentas o grandes, el ancho de banda instantáneo real puede diferir de los valores indicados en este gráfico.

   - Tasa de respuesta de error: Este gráfico proporciona una tasa aproximada a la que las solicitudes que coinciden con esta política devuelven errores (código de estado HTTP >= 400) a los clientes.
   - Duración media de la solicitud (sin error): Este gráfico proporciona una duración media de las solicitudes correctas que coinciden con esta política.
   - Uso de ancho de banda de política: Este gráfico proporciona la cantidad de ancho de banda que coincide con esta política manejada por todos los equilibradores de carga. Los datos recibidos incluyen cabeceras de solicitud para todas las solicitudes y tamaño de datos de cuerpo para las respuestas que tienen datos de cuerpo. Enviado incluye cabeceras de respuesta para todas las solicitudes y tamaño de datos de cuerpo de respuesta para las solicitudes que incluyen datos de cuerpo en la respuesta.

4. Coloque el cursor sobre un gráfico de líneas para ver una ventana emergente de valores en una parte específica del gráfico.
5. Seleccione **Grafana dashboard** justo debajo del título de Métricas para ver todos los gráficos de una política. Además de los cuatro gráficos de la pestaña **Métricas**, puedes ver dos gráficos más:
   - Ratio de solicitud de escritura por tamaño de objeto: Ratio de solicitudes DE PUT/POST/DELETE que coincidan con esta política. El posicionamiento en una celda individual muestra las tasas por segundo. Las tasas que se muestran en la vista flotante se truncan en números enteros y pueden informar de 0 cuando hay solicitudes que no sean cero en el bloque.
   - Tasa de solicitud de lectura por tamaño de objeto: La tasa de SOLICITUDES DE OBTENCIÓN/CABECERA que coinciden con esta política. El posicionamiento en una celda individual muestra las tasas por segundo. Las tasas que se muestran en la vista flotante se truncan en números enteros y pueden informar de 0 cuando hay solicitudes que no sean cero en el bloque.
6. También puede acceder a los gráficos desde el menú **SUPPORT**.
   a. Seleccione **SUPPORT** > **Tools** > **Metrics**.
   b. Selecciona **Política de clasificación de tráfico** en la sección **Grafana**.
   c. Seleccione la política en el menú en la parte superior izquierda de la página.
   d. Coloque el cursor sobre un gráfico para ver una ventana emergente que muestra la fecha y hora de la muestra, los tamaños de los objetos que se agregan al recuento y el número de solicitudes por segundo durante ese período de tiempo.

      Las directivas de clasificación del tráfico se identifican por su ID. Los ID de política se muestran en la página de políticas de clasificación de tráfico.
7. Analice los gráficos para determinar con qué frecuencia la política limita el tráfico y si necesita ajustar la política.

Cifrados compatibles para conexiones TLS salientes

El sistema StorageGRID es compatible con un conjunto limitado de conjuntos de cifrado para conexiones TLS (seguridad de la capa de transporte) con los sistemas externos utilizados para la federación de identidades y los pools de almacenamiento en cloud.

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3 para conexiones a sistemas externos que se utilizan para la federación de identidades y los pools de almacenamiento en cloud.

Se han seleccionado los cifrados TLS compatibles con sistemas externos para garantizar la compatibilidad con una gama de sistemas externos. La lista supera la lista de cifrados que se admiten con aplicaciones cliente S3 o Swift. Para configurar los cifrados, vaya a **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD** y seleccione **Políticas TLS y SSH**.

> ⓘ Las opciones de configuración de TLS, como las versiones de protocolos, los cifrados, los algoritmos de intercambio de claves y los algoritmos MAC, no se pueden configurar en StorageGRID. Si tiene solicitudes específicas sobre esta configuración, póngase en contacto con su representante de cuenta de NetApp.

Ventajas de las conexiones HTTP activas, inactivas y simultáneas

La forma en que se configuran las conexiones HTTP puede afectar el rendimiento del sistema StorageGRID. Las configuraciones varían en función de si la conexión HTTP está activa o inactiva o si tiene varias conexiones simultáneas.

Puede identificar las ventajas en el rendimiento de los siguientes tipos de conexiones HTTP:

- Conexiones HTTP inactivas
- Conexiones HTTP activas
- Conexiones HTTP simultáneas

Ventajas de mantener abiertas las conexiones HTTP inactivas

Debe mantener las conexiones HTTP abiertas incluso cuando las aplicaciones cliente están inactivas para permitir que las aplicaciones cliente realicen transacciones posteriores a través de la conexión abierta. Basándose en las mediciones del sistema y en la experiencia de integración, debe mantener abierta una conexión HTTP inactiva durante un máximo de 10 minutos. StorageGRID puede cerrar automáticamente una conexión HTTP que se mantenga abierta y inactiva durante más de 10 minutos.

Las conexiones HTTP abiertas y inactivas proporcionan las siguientes ventajas:

- Menor latencia desde el momento en que el sistema StorageGRID determina que debe realizar una transacción HTTP hasta el momento en que el sistema StorageGRID puede realizar la transacción

  La latencia reducida es la ventaja principal, especialmente por la cantidad de tiempo necesario para establecer las conexiones TCP/IP y TLS.

- Aumento de la velocidad de transferencia de datos mediante la preparación del algoritmo de inicio lento TCP/IP con transferencias realizadas previamente
- Notificación instantánea de varias clases de condiciones de fallo que interrumpen la conectividad entre la aplicación cliente y el sistema StorageGRID

Determinar durante cuánto tiempo mantener abierta una conexión inactiva-es un intercambio entre las ventajas del inicio lento que se asocia a la conexión existente y la asignación ideal de la conexión a los recursos internos del sistema.

Ventajas de las conexiones HTTP activas

Para conexiones directas a nodos de almacenamiento, debe limitar la duración de una conexión HTTP activa a un máximo de 10 minutos, incluso si la conexión HTTP realiza transacciones continuamente.

La determinación de la duración máxima de la apertura de una conexión es un intercambio-entre los beneficios de la persistencia de la conexión y la asignación ideal de la conexión a los recursos internos del sistema.

Para las conexiones de cliente a los nodos de almacenamiento, la limitación de las conexiones HTTP activas proporciona las siguientes ventajas:

- Permite un balanceo de carga óptimo en el sistema StorageGRID.

  Con el tiempo, es posible que una conexión HTTP ya no sea óptima a medida que cambian los requisitos de equilibrio de carga. El sistema realiza su mejor equilibrio de carga cuando las aplicaciones cliente establecen una conexión HTTP independiente para cada transacción, pero esto niega las ganancias

mucho más valiosas asociadas con conexiones persistentes.

- Permite a las aplicaciones cliente dirigir transacciones HTTP a servicios LDR que tengan espacio disponible.
- Permite iniciar los procedimientos de mantenimiento.

  Algunos procedimientos de mantenimiento se inician solo después de que se completen todas las conexiones HTTP en curso.

En el caso de las conexiones cliente al servicio Load Balancer, limitar la duración de las conexiones abiertas puede ser útil para permitir que algunos procedimientos de mantenimiento se inicien con rapidez. Si la duración de las conexiones de cliente no es limitada, es posible que las conexiones activas tarden varios minutos en finalizarse automáticamente.

Ventajas de las conexiones HTTP simultáneas

Debe mantener abiertas varias conexiones TCP/IP al sistema StorageGRID para permitir el paralelismo, lo que aumenta el rendimiento. El número óptimo de conexiones paralelas depende de diversos factores.

Las conexiones HTTP simultáneas proporcionan las siguientes ventajas:

- Latencia reducida

  Las transacciones pueden iniciarse inmediatamente en lugar de esperar a que se completen otras transacciones.

- Aumento de la productividad

  El sistema StorageGRID puede realizar transacciones paralelas y aumentar el rendimiento global de las transacciones.

Las aplicaciones cliente deben establecer varias conexiones HTTP. Cuando una aplicación cliente tiene que realizar una transacción, puede seleccionar y utilizar inmediatamente cualquier conexión establecida que no esté procesando actualmente una transacción.

Antes de que el rendimiento empiece a degradarse, cada topología de los sistemas StorageGRID tiene un rendimiento máximo diferente para transacciones y conexiones simultáneas. El rendimiento máximo depende de factores como los recursos informáticos, los recursos de red, los recursos de almacenamiento y los enlaces WAN. También son factores que influyen en el número de servidores y servicios y el número de aplicaciones que admite el sistema StorageGRID.

A menudo, los sistemas StorageGRID admiten varias aplicaciones cliente. Debe tener esto en cuenta al determinar el número máximo de conexiones simultáneas que utiliza una aplicación cliente. Si la aplicación cliente consta de varias entidades de software que cada una establece conexiones al sistema StorageGRID, debe agregar todas las conexiones a través de las entidades. Es posible que tenga que ajustar el número máximo de conexiones simultáneas en las siguientes situaciones:

- La topología del sistema StorageGRID afecta al número máximo de transacciones y conexiones simultáneas que puede admitir el sistema.
- Las aplicaciones cliente que interactúan con el sistema StorageGRID a través de una red con ancho de banda limitado pueden tener que reducir el grado de concurrencia para garantizar que las transacciones individuales se completen en un tiempo razonable.
- Cuando muchas aplicaciones cliente comparten el sistema StorageGRID, puede que tenga que reducir el

nivel de concurrencia para evitar superar los límites del sistema.

Separación de grupos de conexiones HTTP para operaciones de lectura y escritura

Puede utilizar pools independientes de conexiones HTTP para operaciones de lectura y escritura y controlar la cantidad de un pool que debe utilizar para cada uno. Los grupos separados de conexiones HTTP le permiten controlar mejor las transacciones y equilibrar las cargas.

Las aplicaciones cliente pueden crear cargas que sean dominantes de la recuperación (lectura) o del almacén (escritura). Con grupos separados de conexiones HTTP para transacciones de lectura y escritura, puede ajustar la cantidad de cada pool que se va a dedicar a transacciones de lectura o escritura.

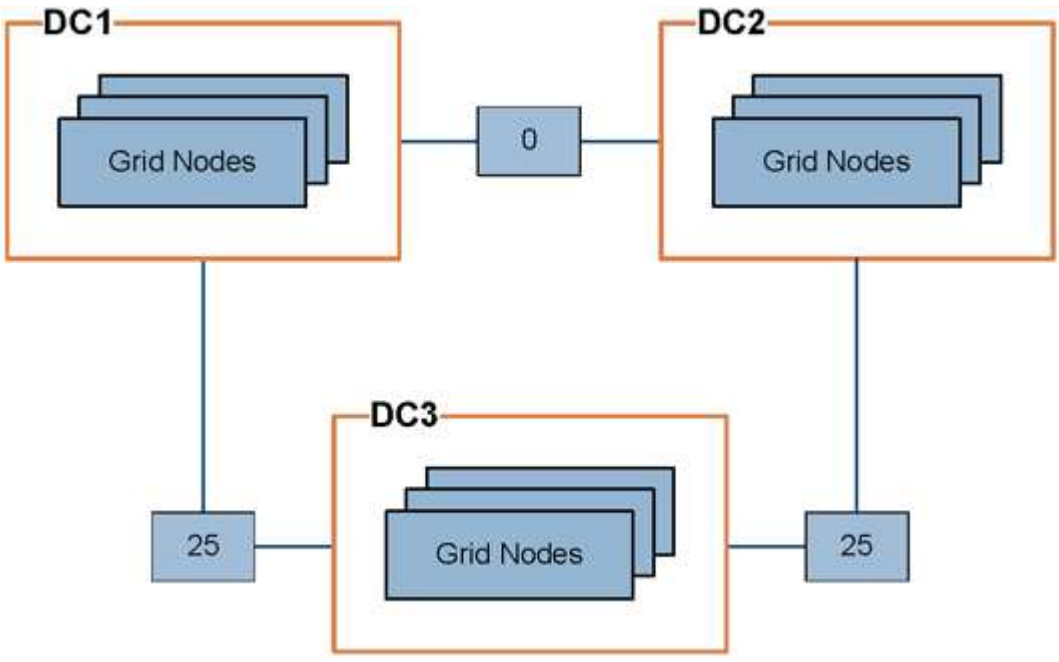
Gestionar costes de enlaces

Los costes de enlace le permiten priorizar qué sitio de centro de datos proporciona un servicio solicitado cuando existen dos o más centros de datos. Puede ajustar los costes de vínculo para reflejar la latencia entre los sitios.

¿Qué son los costes de enlace?

- Los costes de enlace se utilizan para priorizar qué copia de objetos se utiliza para llevar a cabo las recuperaciones de objetos.
- Los costes de enlace los utiliza la API de gestión de grid y la API de gestión de inquilinos para determinar qué servicios StorageGRID internos utilizar.
- Los costes de enlace los utiliza el servicio de equilibrio de carga en los nodos de administración y de gateway para dirigir las conexiones de cliente. Consulte "Consideraciones que tener en cuenta al equilibrio de carga".

El diagrama muestra una cuadrícula de tres sitios con costes de enlace configurados entre sitios:



- El servicio Load Balancer en los nodos de administración y de puerta de enlace distribuye equitativamente las conexiones de los clientes a todos los nodos de almacenamiento en el mismo sitio del centro de datos y a cualquier sitio del centro de datos con un coste de enlace de 0.

En el ejemplo, un nodo de puerta de enlace en el sitio del centro de datos 1 (DC1) distribuye igualmente conexiones de cliente a nodos de almacenamiento en DC1 y a nodos de almacenamiento en DC2. Un nodo de puerta de enlace en DC3 envía conexiones de cliente sólo a los nodos de almacenamiento en DC3.

- Al recuperar un objeto que existe como varias copias replicadas, StorageGRID recupera la copia en el centro de datos que tiene el coste de enlace más bajo.

  En el ejemplo, si una aplicación cliente de DC2 recupera un objeto almacenado tanto en DC1 como en DC3, el objeto se recupera de DC1, porque el coste del enlace de DC1 a DC2 es 0, que es inferior al coste del enlace de DC3 a DC2 (25).

Los costes de enlace son números relativos arbitrarios sin unidad de medida específica. Por ejemplo, un costo de enlace de 50 se utiliza de forma menos preferente que un costo de enlace de 25. En la tabla se muestran los costes de los enlaces más utilizados.

Enlace	Coste del enlace	Notas
Entre sitios físicos del centro de datos	25 (predeterminado)	Centros de datos conectados por un enlace WAN.
Entre las ubicaciones lógicas del centro de datos en la misma ubicación física	0	Centros de datos lógicos en el mismo edificio físico o campus conectados por una LAN.

Actualizar costes de enlace

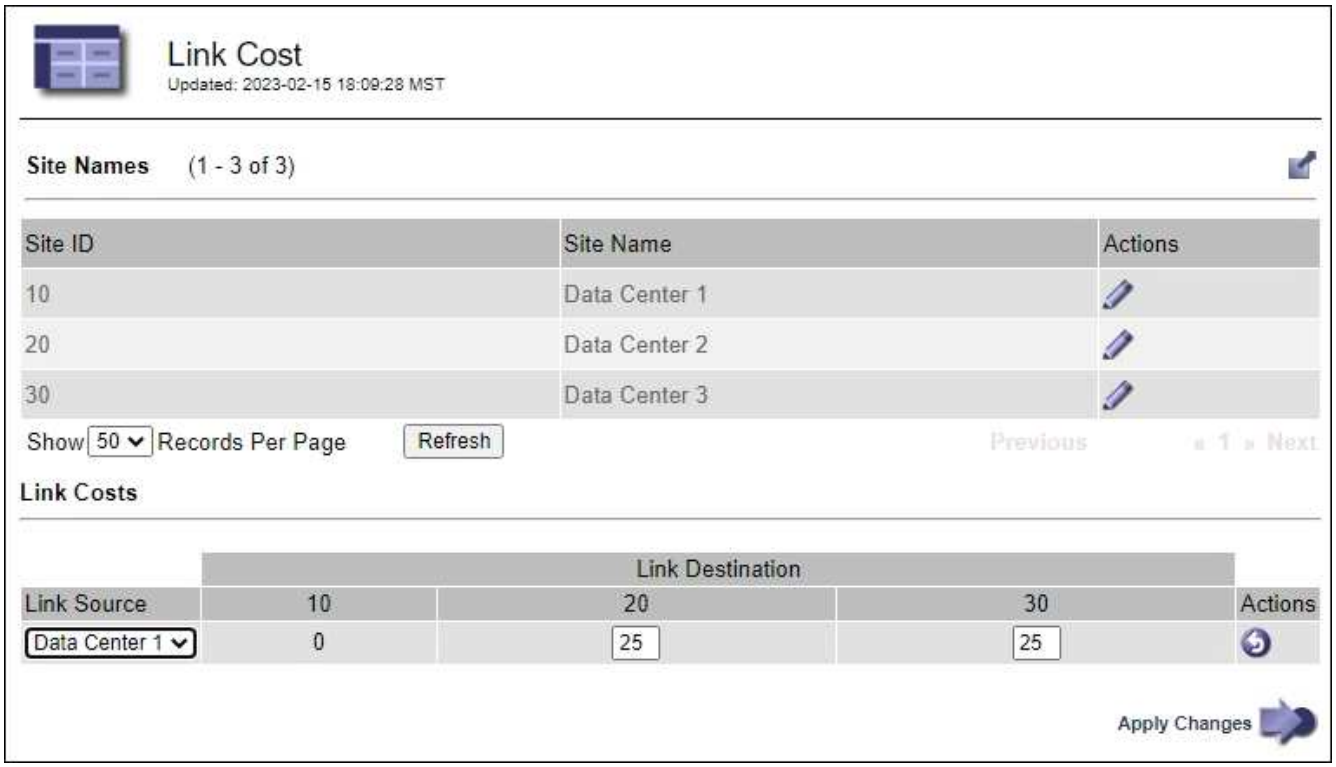
Puede actualizar los costes de enlace entre los sitios de centros de datos para reflejar la latencia entre los sitios.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de configuración de la página de topología de cuadrícula".

Pasos

1. Selecciona **SOPORTE** > **OTRO** > **Costo de enlace**.



2. Seleccione un sitio en **origen de enlace** e introduzca un valor de coste entre 0 y 100 en **destino de enlace**.

   No puede cambiar el coste del enlace si el origen es el mismo que el destino.

   Para cancelar los cambios, seleccione **Revert**.

3. Seleccione **aplicar cambios**.

Utilice AutoSupport

Utilice AutoSupport: Descripción general

La función AutoSupport permite que StorageGRID envíe paquetes de estado y estado al soporte técnico de NetApp.

El uso de AutoSupport puede acelerar significativamente la determinación y resolución de problemas. El soporte técnico también puede supervisar las necesidades de almacenamiento del sistema y ayudarle a determinar si necesita añadir nodos o sitios nuevos. De manera opcional, puede configurar paquetes AutoSupport para que se envíen a otro destino.

StorageGRID tiene dos tipos de AutoSupport:

StorageGRID AutoSupport

Informa de problemas de software de StorageGRID. Habilitado de forma predeterminada la primera vez que se instala StorageGRID. Puede hacerlo "Cambie la configuración predeterminada de AutoSupport" si es necesario.

Si StorageGRID AutoSupport no está activado, aparece un mensaje en el panel de control de Grid Manager. El mensaje incluye un enlace a la página de configuración de AutoSupport. Si cierra el mensaje, no volverá a aparecer hasta que se borre la caché del explorador, aunque AutoSupport permanezca deshabilitado.

AutoSupport de hardware del dispositivo

Informa de los problemas del dispositivo StorageGRID. Debe "Configure el AutoSupport de hardware en cada dispositivo".

¿Qué es Active IQ?

Active IQ es un asesor digital basado en cloud que aprovecha el análisis predictivo y los conocimientos de la comunidad de la base instalada de NetApp. Sus evaluaciones de riesgos continuas, las alertas predictivas, las directrices prescriptivas y las acciones automatizadas le ayudan a evitar problemas antes de que se produzcan, lo que mejora el estado del sistema y aumenta la disponibilidad del sistema.

Si desea usar las consolas y la funcionalidad de Active IQ en el sitio de soporte de NetApp, debe habilitar AutoSupport.

"Documentación del asesor digital de Active IQ"

Información incluida en el paquete AutoSupport

Un paquete AutoSupport contiene los siguientes archivos XML y detalles.

Nombre de archivo	Campos	Descripción
AUTOSUPPORT-HISTORY.XML	Núm. De secuencia de AutoSupport Destino para esta AutoSupport Evento de activación Estado de entrega Intentos de entrega AutoSupport Asunto URI de entrega Último error Nombre de archivo DE AutoSupport PUT Hora de generación AutoSupport Tamaño comprimido AutoSupport descomprimido Tamaño Tiempo Total de Recopilación (ms)	Archivo de historial de AutoSupport

Nombre de archivo	Campos	Descripción
AUTOSUPPORT.XML	Nodo Protocolo para contactar con el soporte URL de soporte para HTTP/HTTPS Dirección de soporte Estado de OnDemand de AutoSupport URL de servidor OnDemand de AutoSupport Intervalo de sondeo de AutoSupport OnDemand	Archivo de estado de AutoSupport. Proporciona detalles del protocolo utilizado, la URL y la dirección de soporte técnico, el intervalo de sondeo y OnDemand AutoSupport si se habilita o se deshabilita.
BUCKETS.XML	ID de bloque ID de cuenta Versión de compilación Configuración de restricción de ubicación Conformidad activada Configuración de conformidad S3 Bloqueo de objetos activado S3 Configuración de bloqueo de objetos Configuración de consistencia CORS activado Configuración de CORS Hora del último acceso activada Política activada Configuración de Política Notificaciones activadas Configuración de notificaciones Cloud Mirror habilitado Configuración de Cloud Mirror Búsqueda activada Configuración de búsqueda ACL de lectura de Swift activada Configuración de ACL de lectura de Swift ACL de Swift Write activada Configuración de ACL de Swift Write Etiquetado de buckets activado Configuración de etiquetado de bloques Configuración de control de versiones	Proporciona estadísticas y detalles de configuración a nivel de bloque. Ejemplo de configuración de bloques que incluyen servicios de plataforma, cumplimiento de normativas y coherencia de bloques.

Nombre de archivo	Campos	Descripción
GRID-CONFIGURATIONS.XML	ID de atributo Nombre de atributo Valor Índice ID de tabla Nombre de la tabla	Archivo de información de configuración de toda la cuadrícula. Contiene información sobre certificados de grid, espacio reservado de metadatos, ajustes de configuración de todo el grid (cumplimiento, bloqueo de objetos S3, compresión de objetos, alertas, syslog, y configuración de ILM), detalles del perfil de código de borrado, nombre DNS, "Nombre de NMS", y más.
GRID-SPEC.XML	Especificaciones de cuadrícula, XML sin procesar	Se utiliza para configurar e implementar StorageGRID. Contiene especificaciones de cuadrícula, IP del servidor NTP, IP del servidor DNS, topología de red y perfiles de hardware de los nodos.
GRID-TASKS.XML	Nodo Ruta de servicio ID de atributo Nombre de atributo Valor Índice ID de tabla Nombre de tabla	Archivo de estado de tareas de cuadrícula (procedimientos de mantenimiento). Proporciona detalles de las tareas activas, terminadas, completadas, fallidas y pendientes de la cuadrícula.
ILM-STATUS.XML	Nodo Ruta de servicio ID de atributo Nombre de atributo Valor Índice ID de tabla Nombre de tabla	Archivo de información de métricas de ILM. Contiene tasas de evaluación de ILM para cada nodo y métricas de todo el grid.
ILM.XML	XML sin procesar de ILM	Archivo de política activa de ILM. Contiene detalles sobre las políticas de ILM activas, como el ID de pool de almacenamiento, el comportamiento de ingesta, los filtros, las reglas y la descripción.
LOG.TGZ	*n/a*	Archivo de registro descargable. Contiene `bycast-err.log` y.. `servermanager.log` de cada nodo.

Nombre de archivo	Campos	Descripción
MANIFIESTO.XML	Orden de recogida Nombre de archivo de contenido AutoSupport para estos datos Descripción de este elemento de datos Cantidad de bytes recopilados Tiempo dedicado a recopilar Estado de este elemento de datos Descripción del error Tipo de contenido AutoSupport para estos datos +	Contiene metadatos AutoSupport y descripciones breves de todos los archivos XML de AutoSupport.
NMS-ENTITIES.XML	Índice de atributos Entidad OID ID de nodo ID de modelo de dispositivo Versión del modelo del dispositivo Nombre de entidad	Agrupe y las entidades de servicio en la "Árbol de NMS". Proporciona detalles de topología de cuadrícula. El nodo se puede determinar en función de los servicios que se ejecutan en el nodo.
OBJECT-STATUS.XML	Nodo Ruta de servicio ID de atributo Nombre de atributo Valor Índice ID de tabla Nombre de tabla	Estado del objeto, incluido el estado de exploración en segundo plano, la transferencia activa, la velocidad de transferencia, el total de transferencias, la velocidad de eliminación, fragmentos dañados, objetos perdidos, objetos faltantes, intento de reparación, velocidad de exploración, período de adquisición estimado, estado de finalización de reparación y más.
SERVER-STATUS.XML	Nodo Ruta de servicio ID de atributo Nombre de atributo Valor Índice ID de tabla Nombre de tabla	Archivo de eventos y configuraciones del servidor. Contiene estos detalles de cada nodo: Tipo de plataforma, sistema operativo, memoria instalada, memoria disponible, conectividad de almacenamiento, número de serie del chasis del dispositivo de almacenamiento, número de unidades fallidas de la controladora de almacenamiento, temperatura del chasis de la controladora de computación, hardware de computación, número de serie de la controladora de computación, fuente de alimentación, tamaño de unidad, tipo de unidad y más.

Nombre de archivo	Campos	Descripción
SERVICE-STATUS.XML	Nodo Ruta de servicio ID de atributo Nombre de atributo Valor Índice ID de tabla Nombre de tabla	Archivo de información del nodo de servicio. Contiene detalles tales como espacio de tabla asignado, espacio de tabla libre, métricas de la base de datos de Reaper, duración de la reparación de segmentos, duración del trabajo de reparación, reinicios automáticos de trabajos, terminación automática de trabajos, y mucho más.
STORAGE-GRADES.XML	ID de grado de almacenamiento Nombre de grado de almacenamiento ID del nodo de almacenamiento Ruta del nodo de almacenamiento	Archivo de definiciones de grado de almacenamiento para cada nodo de almacenamiento.
SUMMARY-ATTRIBUTES.XML	Grupo OID Ruta de grupo ID de atributo de resumen Nombre de atributo de resumen Valor Índice ID de tabla Nombre de tabla	Datos de estado del sistema de alto nivel que resumen la información de uso de StorageGRID. Proporciona detalles como el nombre de grid, los nombres de sitios, la cantidad de nodos de almacenamiento por grid y por sitio, tipo de licencia, capacidad y uso de la licencia, términos de soporte del software y detalles de las operaciones de S3 y Swift.
SYSTEM-ALARM.XML	Nodo Ruta de servicio Gravedad Atributo con alarma Nombre de atributo Estado Valor Tiempo de activación Confirme la hora	Alarmas de nivel del sistema (anticuadas) y datos de estado utilizados para indicar actividades anormales o posibles problemas.

Nombre de archivo	Campos	Descripción
SYSTEM-ALERTS.XML	Nombre Gravedad Nombre de nodo Estado de alerta Nombre del sitio Tiempo de activación de alerta Tiempo de resolución de alerta ID de regla ID de nodo ID del sitio Silenciado Otras anotaciones Otras etiquetas	Alertas actuales del sistema que indican posibles problemas en el sistema StorageGRID.
USERAGENTS.XML	Agente de usuario Número de días Total de Solicitudes HTTP Bytes totales ingeridos Total de bytes recuperados Solicitudes de PUT OBTENER solicitudes Eliminar solicitudes Solicitudes de CABEZA Enviar solicitudes OPCIONES Solicitudes Tiempo Medio de Solicitud (ms) Tiempo Medio de Solicitud de PUT (ms) Tiempo Medio de Solicitud de OBTENCIÓN (ms) Tiempo Medio de Solicitud de SUPRESIÓN (ms) Tiempo medio de solicitud de CABEZAL (ms) Tiempo Medio de Solicitud POSTERIOR (ms) Tiempo Medio de Solicitud de OPCIONES (ms)	Estadísticas basadas en los agentes de usuario de la aplicación. Por ejemplo, el número de operaciones PUT/GET/DELETE/HEAD por agente de usuario y el tamaño total de bytes de cada operación.
DATOS-CON-ENCABEZADOX.	X-netapp-asup-generated-on X-netapp-asup-hostname X-netapp-asup-os-version X-netapp-asup-serial-num X-netapp-asup-Subject X-netapp-asup-system-id X-netapp-asup-model-name +	Datos de encabezados AutoSupport.

Configure AutoSupport

De forma predeterminada, la función StorageGRID AutoSupport se habilita cuando se instala por primera vez StorageGRID. Sin embargo, debe configurar el AutoSupport de hardware en cada dispositivo. Según sea necesario, puede cambiar la configuración de AutoSupport.

Si desea cambiar la configuración de StorageGRID AutoSupport, realice los cambios sólo en el nodo de administración principal. Debe Configure el AutoSupport de hardware en cada aparato.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".
- Si va a utilizar HTTPS para enviar paquetes AutoSupport, ha proporcionado acceso a Internet saliente al nodo de administración principal, ya sea directamente o "utilizando un servidor proxy" (no se requieren conexiones entrantes).
- Si se selecciona HTTP en la página StorageGRID AutoSupport, se ha configurado un servidor proxy para reenviar paquetes AutoSupport como HTTPS. Los servidores AutoSupport de NetApp rechazarán los paquetes enviados mediante HTTP.

  "Obtenga más información sobre la configuración de los ajustes de proxy de administración".

- Si utilizará SMTP como protocolo para paquetes de AutoSupport, habrá configurado un servidor de correo SMTP. La misma configuración del servidor de correo se utiliza para las notificaciones de correo electrónico de alarma (sistema heredado).

Acerca de esta tarea

Puede usar cualquier combinación de las siguientes opciones para enviar paquetes de AutoSupport al soporte técnico:

- **Semanal**: Envía automáticamente paquetes AutoSupport una vez por semana. Valor predeterminado: Activado.
- **Activado por eventos**: Envía automáticamente paquetes AutoSupport cada hora o cuando ocurran eventos significativos del sistema. Valor predeterminado: Activado.
- **On Demand**: Permite al soporte técnico solicitar que tu sistema StorageGRID envíe paquetes AutoSupport automáticamente, lo cual es útil cuando están trabajando activamente en un problema (requiere protocolo de transmisión HTTPS AutoSupport). Ajuste predeterminado: Desactivado.
- **Activado por el usuario**: Envía manualmente paquetes AutoSupport en cualquier momento.

Especifique el protocolo para paquetes AutoSupport

Puede usar cualquiera de los siguientes protocolos para enviar paquetes de AutoSupport:

- **HTTPS**: Es la configuración predeterminada y recomendada para nuevas instalaciones. Este protocolo utiliza el puerto 443. Si desea Habilite la función AutoSupport On Demand, Debe utilizar HTTPS.
- **HTTP**: Si selecciona HTTP, debe configurar un servidor proxy para reenviar paquetes AutoSupport como HTTPS. Los servidores AutoSupport de NetApp rechazan los paquetes enviados mediante HTTP. Este protocolo utiliza el puerto 80.
- **SMTP**: Utilice esta opción si desea que los paquetes de AutoSupport sean enviados por correo electrónico. Si utiliza SMTP como protocolo para paquetes AutoSupport, debe configurar un servidor de

correo SMTP en la página Configuración de correo electrónico heredado (**SUPPORT** > **Alarmas (legacy)** > **Configuración de correo electrónico heredado**).

El protocolo configurado se utiliza para enviar todos los tipos de paquetes de AutoSupport.

Pasos

1. Selecciona **SUPPORT** > **Herramientas** > **AutoSupport** > **Ajustes**.
2. Seleccione el protocolo que desea usar para enviar paquetes de AutoSupport.
3. Si seleccionó **HTTPS**, seleccione si desea usar un certificado de soporte NetApp (certificado TLS) para proteger la conexión con el servidor de soporte técnico.
   - **Verificar certificado** (por defecto): Asegura que la transmisión de los paquetes AutoSupport sea segura. El certificado de soporte de NetApp ya está instalado con el software StorageGRID.
   - **No verificar certificado**: Seleccione esta opción sólo cuando tenga un buen motivo para no utilizar la validación de certificados, como cuando haya un problema temporal con un certificado.
4. Seleccione **Guardar**. Todos los paquetes semanales, activados por el usuario y activados por eventos se envían mediante el protocolo seleccionado.

Deshabilite el AutoSupport semanal

De manera predeterminada, el sistema StorageGRID se configura para enviar un paquete de AutoSupport al soporte técnico una vez a la semana.

Para determinar cuándo se enviará el paquete AutoSupport semanal, vaya a la pestaña **AutoSupport** > **Resultados**. En la sección **AutoSupport semanal**, mira el valor de **Próxima hora programada**.

Es posible deshabilitar el envío automático de paquetes de AutoSupport semanales en cualquier momento.

Pasos

1. Selecciona **SUPPORT** > **Herramientas** > **AutoSupport** > **Ajustes**.
2. Desactive la casilla de verificación **Activar AutoSupport semanal**.
3. Seleccione **Guardar**.

Deshabilite el AutoSupport activado por eventos

De manera predeterminada, el sistema StorageGRID se configura para enviar un paquete AutoSupport al soporte técnico cada hora, cuando se produce una alerta importante u otro evento importante del sistema.

Puede deshabilitar la AutoSupport activada por eventos en cualquier momento.

Pasos

1. Selecciona **SUPPORT** > **Herramientas** > **AutoSupport** > **Ajustes**.
2. Desactive la casilla de verificación **Activar AutoSupport desencadenado por eventos**.
3. Seleccione **Guardar**.

Habilite AutoSupport bajo demanda

AutoSupport On Demand puede ayudar a resolver problemas en los que el soporte técnico está trabajando activamente.

De manera predeterminada, AutoSupport On Demand está deshabilitado. Al habilitar esta función, el soporte

técnico puede solicitar que el sistema StorageGRID envíe paquetes AutoSupport automáticamente. El soporte técnico también puede establecer el intervalo de sondeo para AutoSupport en consultas bajo demanda.

El soporte técnico no puede habilitar ni deshabilitar AutoSupport On Demand.

Pasos

1. Selecciona **SUPPORT** > **Herramientas** > **AutoSupport** > **Ajustes**.
2. Seleccione **HTTPS** para el protocolo.
3. Seleccione la casilla de verificación **Activar AutoSupport semanal**.
4. Seleccione la casilla de verificación **Activar AutoSupport On Demand**.
5. Seleccione **Guardar**.

   AutoSupport On Demand está habilitado y el soporte técnico puede enviar solicitudes AutoSupport On Demand a StorageGRID.

Desactive las comprobaciones de actualizaciones de software

De forma predeterminada, StorageGRID se pone en contacto con NetApp para determinar si hay actualizaciones de software disponibles para su sistema. Si hay disponible una revisión o versión nueva de StorageGRID, se muestra la nueva versión en la página actualización de StorageGRID.

Según sea necesario, puede desactivar opcionalmente la comprobación de actualizaciones de software. Por ejemplo, si el sistema no tiene acceso WAN, debe desactivar la comprobación para evitar errores de descarga.

Pasos

1. Selecciona **SUPPORT** > **Herramientas** > **AutoSupport** > **Ajustes**.
2. Desactive la casilla de verificación **Comprobar si hay actualizaciones de software**.
3. Seleccione **Guardar**.

Añada un destino de AutoSupport adicional

Cuando se habilita AutoSupport, se envían paquetes de estado y estado al soporte técnico. Puede especificar un destino adicional para todos los paquetes de AutoSupport.

Para verificar o cambiar el protocolo utilizado para enviar paquetes AutoSupport, consulte las instrucciones a. Especifique el protocolo para paquetes AutoSupport.

> No puede usar el protocolo SMTP para enviar paquetes AutoSupport a un destino adicional.

Pasos

1. Selecciona **SUPPORT** > **Herramientas** > **AutoSupport** > **Ajustes**.
2. Selecciona **Activar destino AutoSupport adicional**.
3. Especifique lo siguiente:

   Nombre del hostl

   Nombre de host o dirección IP del servidor de un servidor de destino AutoSupport adicional.

   > Puede introducir solo un destino adicional.

Puerto

Puerto utilizado para conectarse a un servidor de destino AutoSupport adicional. El valor predeterminado es el puerto 80 para HTTP o el puerto 443 para HTTPS.

Validación de certificado

Si se utiliza un certificado TLS para proteger la conexión al destino adicional.

- Seleccione **Verificar certificado** para utilizar la validación del certificado.
- Seleccione **No verificar certificado** para enviar sus paquetes AutoSupport sin validación de certificado.

  Seleccione esta opción sólo cuando tenga un buen motivo para no utilizar la validación de certificados, como cuando haya un problema temporal con un certificado.

4. Si seleccionó **Verificar certificado**, haga lo siguiente:
   a. Busque la ubicación del certificado de CA.
   b. Cargue el archivo de certificado de CA.

   Aparecen los metadatos del certificado de CA.
5. Seleccione **Guardar**.

   Todos los futuros paquetes de AutoSupport semanales, activados por eventos y activados por el usuario se enviarán al destino adicional.

Configurar AutoSupport para dispositivos

AutoSupport para dispositivos informa de problemas de hardware de StorageGRID y StorageGRID AutoSupport informa de problemas de software de StorageGRID, con una excepción: En el caso del sistema SGF6112, StorageGRID AutoSupport informa de problemas de hardware y software. Tiene que configurar AutoSupport en cada dispositivo, excepto en SGF6112, que no requiere una configuración adicional. AutoSupport se ha implantado de forma diferente en dispositivos de servicios y dispositivos de almacenamiento.

Se utiliza SANtricity para habilitar AutoSupport para cada dispositivo de almacenamiento. Es posible configurar SANtricity AutoSupport durante la configuración inicial del dispositivo o después de haber instalado un dispositivo:

- Para dispositivos SG6000 y SG5700, "Configure AutoSupport en SANtricity System Manager"

Los paquetes AutoSupport de los dispositivos E-Series se pueden incluir en StorageGRID AutoSupport si se configura la entrega de AutoSupport mediante proxy en "System Manager de SANtricity".

StorageGRID AutoSupport no informa de problemas de hardware, como fallos de DIMM o de tarjeta de interfaz del host (HIC). Sin embargo, algunos fallos de componentes pueden desencadenarse "alertas de hardware". En el caso de dispositivos StorageGRID con un controlador de administración de placa base (BMC), como SG100, SG1000, SG6060 o SGF6024, puede configurar capturas de correo electrónico y SNMP para informar de fallos de hardware:

- "Configurar notificaciones por correo electrónico para las alertas de BMC"
- "Configurar los ajustes de SNMP para BMC" Para la controladora SG6000-CN o los dispositivos de servicios SG100 y SG1000

Información relacionada

"Soporte de NetApp"

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

- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Debe tener el acceso root u otro permiso de configuración de grid.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **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 se realiza correctamente, se actualizan los valores **resultado más reciente** y **tiempo más reciente** de la ficha **resultados**. Si hay un problema, el valor **Resultado más reciente** se actualiza a “Error” y StorageGRID no intenta enviar el paquete AutoSupport de nuevo.

   > Después de enviar un paquete AutoSupport activado por el usuario, actualice la página AutoSupport en el explorador al cabo de 1 minuto para acceder a los resultados más recientes.

Solucionar problemas de paquetes AutoSupport

Si se produce un error al intentar enviar un paquete AutoSupport, el sistema StorageGRID realiza diferentes acciones según el tipo de paquete AutoSupport. Puede comprobar el estado de los paquetes AutoSupport seleccionando **SUPPORT** > **Herramientas** > **AutoSupport** > **Resultados**.

Cuando el paquete AutoSupport no se envía, aparece “Failure” en la pestaña **Results** de la página **AutoSupport**.

> Si configuró un servidor proxy para reenviar paquetes AutoSupport a NetApp, debería hacerlo "compruebe que los valores de configuración del servidor proxy son correctos".

Fallo del paquete AutoSupport semanal

Si no se puede enviar un paquete AutoSupport semanal, el sistema StorageGRID realiza las siguientes acciones:

1. Actualiza el atributo de resultado más reciente a Reintentando.
2. Intenta reenviar el paquete AutoSupport 15 veces cada cuatro minutos durante una hora.
3. Después de una hora de errores de envío, actualiza el atributo de resultado más reciente a error.
4. Intenta enviar un paquete de AutoSupport de nuevo a la siguiente hora programada.
5. Mantiene la programación regular de AutoSupport si el paquete falla porque el servicio NMS no está

disponible y si un paquete se envía antes de que pasen los siete días.

6. Cuando el servicio NMS vuelve a estar disponible, envía un paquete AutoSupport inmediatamente si un paquete no se ha enviado durante siete días o más.

Error del paquete AutoSupport activado por el usuario o activado por un evento

Si no se envía un paquete de AutoSupport activado por el usuario o activado por un evento, el sistema StorageGRID realiza las siguientes acciones:

1. Muestra un mensaje de error si se conoce el error. Por ejemplo, si un usuario selecciona el protocolo SMTP sin proporcionar la configuración de correo electrónico correcta, se muestra el siguiente error: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. No intenta enviar el paquete de nuevo.
3. Registra el error en `nms.log`.

Si se produce un error y SMTP es el protocolo seleccionado, compruebe que el servidor de correo electrónico del sistema StorageGRID está configurado correctamente y que el servidor de correo electrónico está en ejecución (**SUPPORT** > **Alarmas (heredado)** > **> Configuración de correo electrónico heredado**). El siguiente mensaje de error puede aparecer en la página AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Aprenda cómo "configure los ajustes del servidor de correo electrónico".

Corrija un error de paquete AutoSupport

Si se produce un error y SMTP es el protocolo seleccionado, compruebe que el servidor de correo electrónico del sistema StorageGRID está configurado correctamente y que el servidor de correo electrónico se está ejecutando. El siguiente mensaje de error puede aparecer en la página AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envíe los paquetes AutoSupport de E-Series a través de StorageGRID

Puede enviar los paquetes AutoSupport de E-Series SANtricity System Manager al soporte técnico a través de un nodo de administración de StorageGRID en lugar de con el puerto de gestión del dispositivo de almacenamiento.

Consulte "AutoSupport de hardware E-Series" Para obtener más información sobre el uso de AutoSupport con dispositivos E-Series.

Antes de empezar

- Se ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso de administrador o de dispositivo de almacenamiento".
- Ha configurado SANtricity AutoSupport:
  - Para dispositivos SG6000 y SG5700, "Configure AutoSupport en SANtricity System Manager"

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

Acerca de esta tarea

Los paquetes AutoSupport de E-Series contienen detalles del hardware de almacenamiento y son más específicos que otros paquetes de AutoSupport enviados por el sistema StorageGRID.

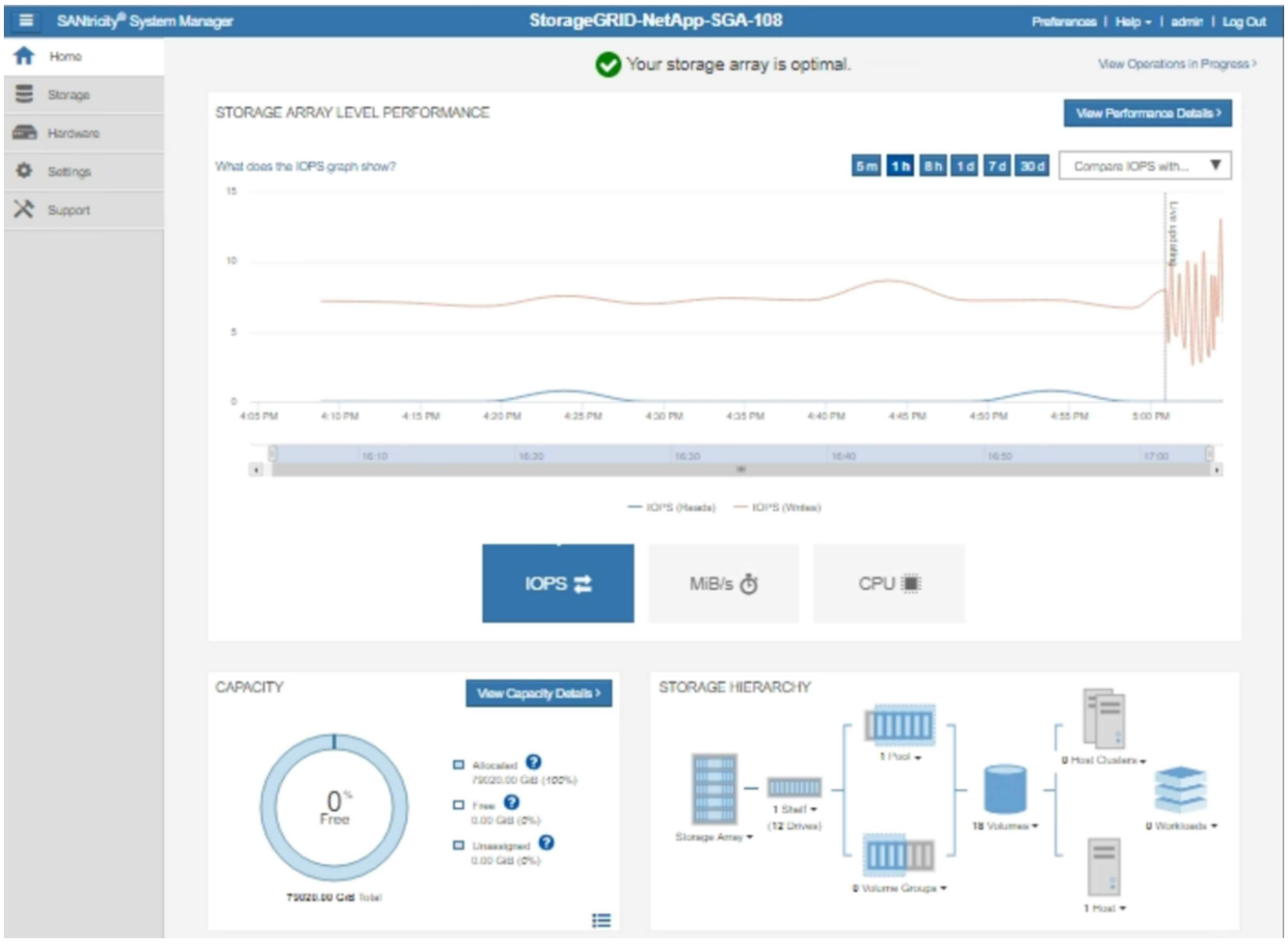
Es posible configurar una dirección de servidor proxy especial en SANtricity System Manager para transmitir paquetes AutoSupport a través de un nodo de administración de StorageGRID sin el uso del puerto de gestión del dispositivo. Los paquetes AutoSupport transmitidos de esta manera los envía el "Nodo de administración de remitente preferido", y usan cualquiera "configuración de proxy de administración" Que se han configurado en Grid Manager.

> Este procedimiento solo es para configurar un servidor proxy StorageGRID para paquetes AutoSupport E-Series. Si quiere más información sobre la configuración de la serie AutoSupport de E-Series, consulte "Documentación de SANtricity y E-Series de NetApp".

Pasos

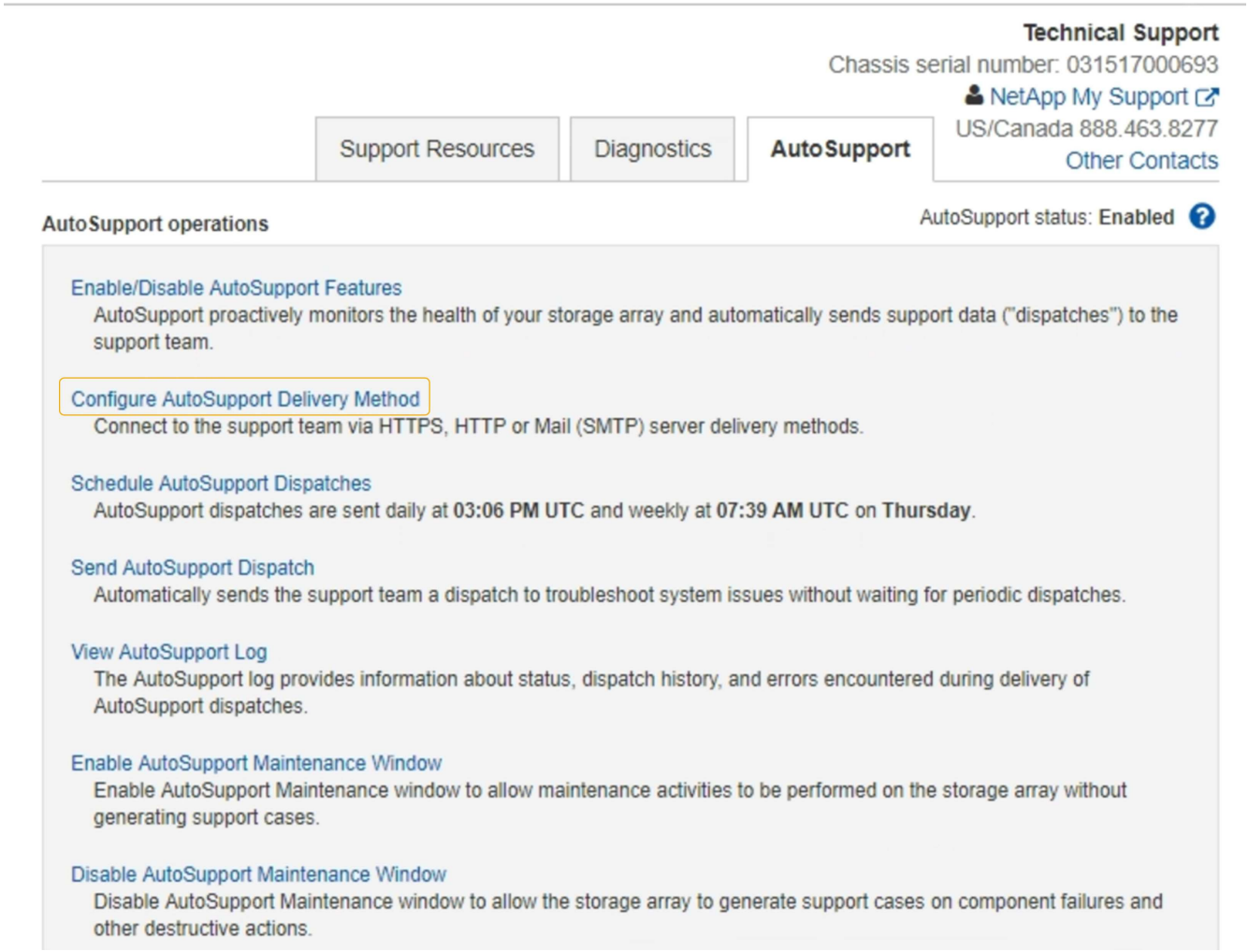
1. En Grid Manager, seleccione **NODES**.
2. En la lista de nodos que aparece a la izquierda, seleccione el nodo del dispositivo de almacenamiento que desea configurar.
3. Seleccione **Administrador del sistema SANtricity**.

   Se mostrará la página de inicio de SANtricity System Manager.



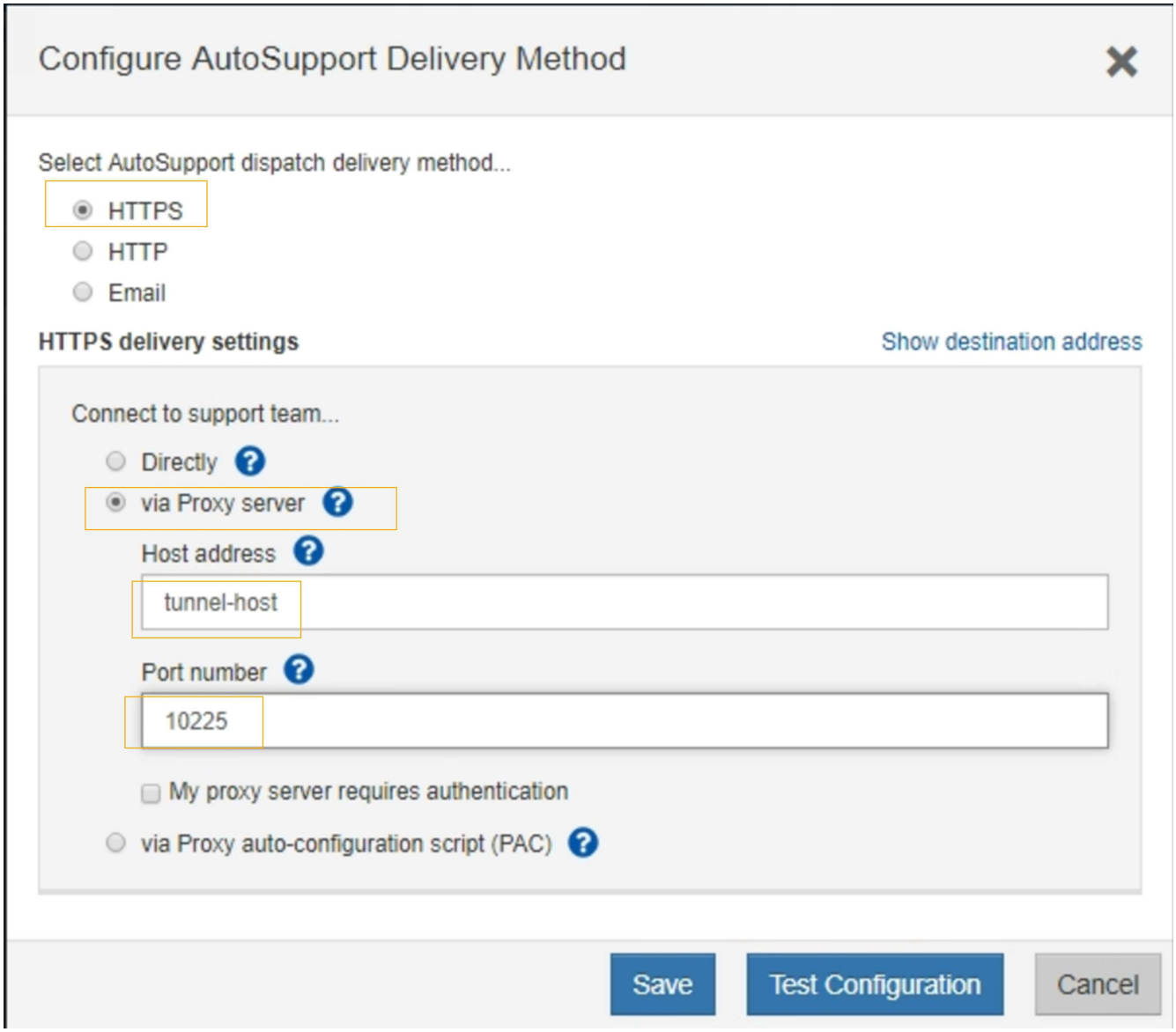
4. Seleccione **SUPPORT** > **Support Center** > **AutoSupport**.

Se muestra la página de operaciones AutoSupport.



5. Seleccione **Configurar método de entrega de AutoSupport**.

   Se muestra la página Configurar método de entrega de AutoSupport.



6. Seleccione **HTTPS** para el método de entrega.

   El certificado que habilita HTTPS está preinstalado.

7. Seleccione **a través del servidor proxy**.
8. Introduzca `tunnel-host` Para la **Dirección de host**.

   `tunnel-host` Es la dirección especial para usar un nodo de administración para enviar paquetes AutoSupport E-Series.

9. Introduzca `10225` Para el **número de puerto**.

   `10225` Es el número de puerto del servidor proxy StorageGRID que recibe paquetes AutoSupport de la controladora E-Series del dispositivo.

10. Seleccione **Configuración de prueba** para probar el enrutamiento y la configuración del servidor proxy AutoSupport.

    Si es correcto, aparece un mensaje en un banner verde que indica que se ha verificado la configuración

de AutoSupport.

Si la prueba falla, se muestra un mensaje de error en un banner rojo. Compruebe la configuración de DNS de StorageGRID y la red, asegúrese del "Nodo de administración de remitente preferido" Puede conectarse al sitio de soporte de NetApp y volver a intentar la prueba.

11. Seleccione **Guardar**.

    Se guardará la configuración y se mostrará un mensaje de confirmación: Se configuró el método de entrega de AutoSupport.

Gestione nodos de almacenamiento

Gestionar nodos de almacenamiento: Información general

Los nodos de almacenamiento proporcionan servicios y capacidad de almacenamiento en disco. La gestión de nodos de almacenamiento conlleva lo siguiente:

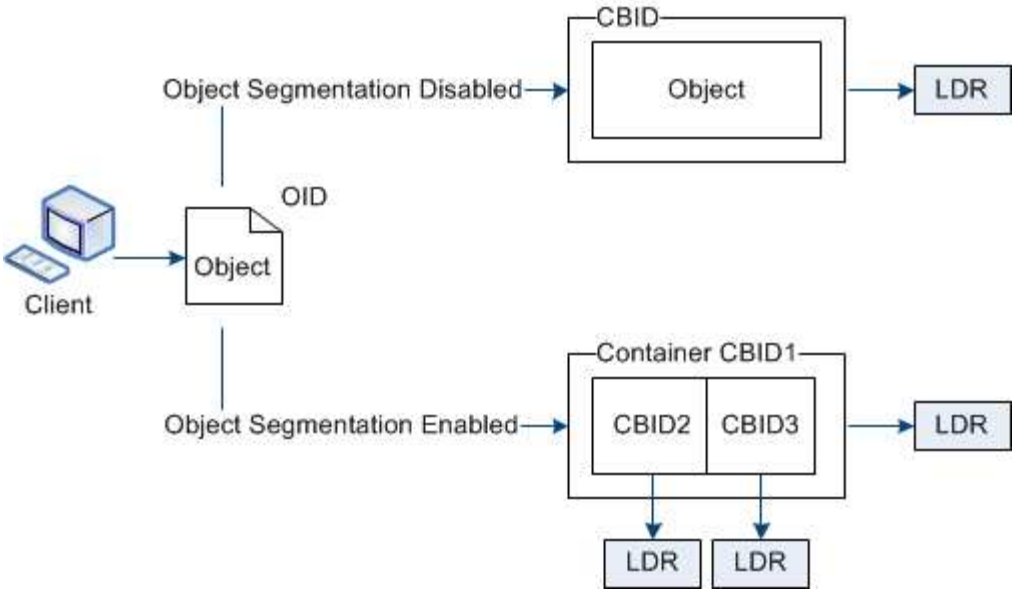
- Gestión de las opciones de almacenamiento
- Comprender qué son las marcas de agua del volumen de almacenamiento y cómo se pueden utilizar anulaciones de Marca de agua para controlar cuando los nodos de almacenamiento pasan a ser de sólo lectura
- Supervisar y gestionar el espacio usado para los metadatos de objetos
- Configuración de la configuración global de los objetos almacenados
- Aplicar las opciones de configuración del nodo de almacenamiento
- Gestión de nodos de almacenamiento completos

Utilice las opciones de almacenamiento

¿Qué es la segmentación de objetos?

La segmentación de objetos es el proceso de dividir un objeto en una colección de objetos más pequeños de tamaño fijo para optimizar el uso de recursos y almacenamiento para objetos grandes. La carga de varias partes de S3 también crea objetos segmentados, con un objeto que representa cada parte.

Cuando un objeto se procesa en el sistema StorageGRID, el servicio LDR divide el objeto en segmentos y crea un contenedor de segmentos que enumera la información de encabezado de todos los segmentos como contenido.



Al recuperar un contenedor de segmentos, el servicio LDR reúne el objeto original de sus segmentos y devuelve el objeto al cliente.

El contenedor y los segmentos no se almacenan necesariamente en el mismo nodo de almacenamiento. El contenedor y los segmentos pueden almacenarse en cualquier nodo de almacenamiento dentro del pool de almacenamiento especificado en la regla de ILM.

El sistema StorageGRID trata cada segmento de forma independiente y contribuye al recuento de atributos como objetos gestionados y objetos almacenados. Por ejemplo, si un objeto almacenado en el sistema StorageGRID se divide en dos segmentos, el valor de objetos gestionados aumenta en tres una vez completada la ingesta, de la siguiente manera:

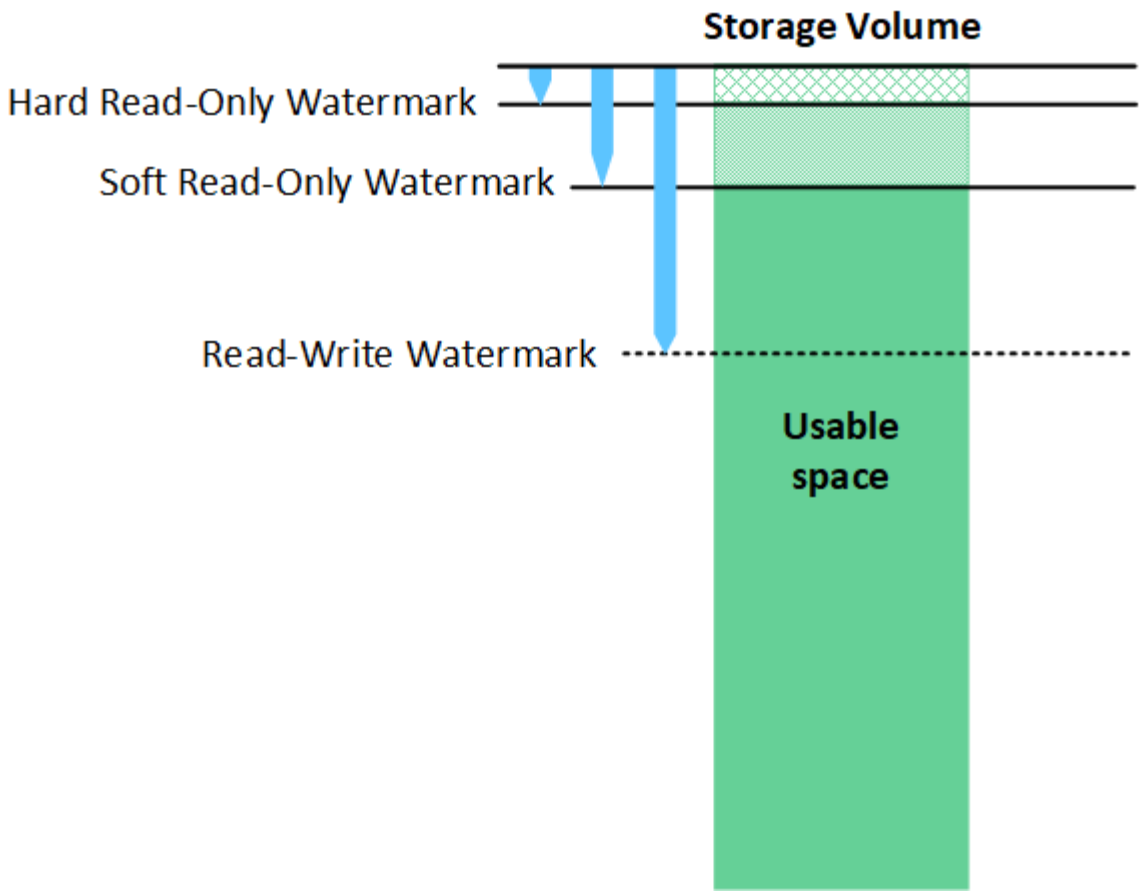
```
segment container + segment 1 + segment 2 = three stored objects
```

Puede mejorar el rendimiento al manejar objetos grandes asegurándose de que:

- Cada puerta de enlace y cada nodo de almacenamiento tiene suficiente ancho de banda de red para el rendimiento requerido. Por ejemplo, configure redes de cliente y de cuadrícula independientes en interfaces Ethernet de 10 Gbps.
- Se ponen en marcha suficientes nodos de pasarela y almacenamiento para el rendimiento requerido.
- Cada nodo de almacenamiento tiene suficiente rendimiento de I/O de disco para el rendimiento requerido.

¿Qué son las marcas de agua del volumen de almacenamiento?

StorageGRID usa tres marcas de agua de volúmenes de almacenamiento para garantizar que los nodos de almacenamiento pasan de forma segura a un estado de solo lectura antes de que se ejecuten con un espacio mínimo y para permitir que los nodos de almacenamiento que se hayan migrado al estado de solo lectura se vuelvan a escribir.



Las marcas de agua del volumen de almacenamiento solo se aplican al espacio utilizado para los datos de objetos replicados y codificados por borrado. Para obtener más información acerca del espacio reservado para los metadatos de objetos en el volumen 0, vaya a. "Gestione el almacenamiento de metadatos de objetos".

¿Qué es la Marca de agua blanda de sólo lectura?

Marca de agua de sólo lectura suave del volumen de almacenamiento es la primera Marca de agua que indica que el espacio utilizable de un nodo de almacenamiento para los datos del objeto se está llenando.

Si cada volumen de un nodo de almacenamiento tiene menos espacio libre que la Marca de agua de solo lectura suave de ese volumen, el nodo de almacenamiento pasará al *modo de solo lectura*. El modo de solo lectura significa que el nodo de almacenamiento anuncia servicios de solo lectura al resto del sistema StorageGRID, pero completa todas las solicitudes de escritura pendientes.

Por ejemplo, supongamos que cada volumen de un nodo de almacenamiento tiene una Marca de agua blanda de solo lectura de 10 GB. En cuanto cada volumen tiene menos de 10 GB de espacio libre, el nodo de almacenamiento pasa al modo de solo lectura suave.

¿Qué es la Marca de agua dura de sólo lectura?

- Marca de agua de sólo lectura dura de volumen de almacenamiento* es la siguiente Marca de agua para indicar que el espacio utilizable de un nodo para los datos de objeto se está llenando.

Si el espacio libre en un volumen es menor que la Marca de agua de sólo lectura de ese volumen, las escrituras en el volumen fallarán. Sin embargo, las escrituras en otros volúmenes pueden continuar hasta que el espacio libre en esos volúmenes sea menor que sus marcas de agua de sólo lectura.

Por ejemplo, supongamos que cada volumen de un nodo de almacenamiento tiene una Marca de agua de solo lectura rígida de 5 GB. En cuanto cada volumen tenga menos de 5 GB de espacio libre, el nodo de almacenamiento ya no aceptará ninguna solicitud de escritura.

La Marca de agua dura de sólo lectura es siempre inferior a la Marca de agua blanda de sólo lectura.

¿Qué es la Marca de agua de lectura y escritura?

Marca de agua de lectura y escritura de volumen de almacenamiento sólo se aplica a los nodos de almacenamiento que hayan pasado al modo de sólo lectura. Determina cuándo el nodo puede volver a ser de lectura y escritura. Cuando el espacio libre de un volumen de almacenamiento en un nodo de almacenamiento es mayor que la Marca de agua de lectura y escritura de ese volumen, el nodo cambia automáticamente al estado de lectura y escritura.

Por ejemplo, supongamos que el nodo de almacenamiento ha pasado al modo de solo lectura. Supongamos también que cada volumen tiene una Marca de agua de lectura y escritura de 30 GB. En cuanto el espacio libre de cualquier volumen aumente a 30 GB, el nodo volverá a ser de lectura y escritura.

La Marca de agua de lectura y escritura es siempre mayor que la Marca de agua de sólo lectura suave y la Marca de agua de sólo lectura dura.

Ver marcas de agua de volumen de almacenamiento

Puede ver los ajustes de Marca de agua actuales y los valores optimizados para el sistema. Si no se utilizan marcas de agua optimizadas, puede determinar si puede o debe ajustar la configuración.

Antes de empezar

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

Ver la configuración actual de la Marca de agua

Puede ver la configuración actual de la Marca de agua de almacenamiento en el Administrador de grid.

Pasos

1. Selecciona **SUPPORT** > **Other** > **Marcas de agua de almacenamiento**.
2. En la página Marcas de agua de almacenamiento, consulte la casilla de verificación Utilizar valores optimizados.
   - Si se selecciona la casilla de comprobación, las tres marcas de agua se optimizan para cada volumen de almacenamiento en cada nodo de almacenamiento, según el tamaño del nodo de almacenamiento y la capacidad relativa del volumen.

     Esta es la configuración predeterminada y recomendada. No actualice estos valores. Opcionalmente, puede hacerlo Vea las marcas de agua de almacenamiento optimizadas.

   - Si la casilla de verificación Utilizar valores optimizados no está seleccionada, se están utilizando marcas de agua personalizadas (no optimizadas). No se recomienda utilizar la configuración de Marca de agua personalizada. Utilice las instrucciones para "Solución de problemas de alertas de anulación de Marca de agua de sólo lectura baja" para determinar si puede o debe ajustar la configuración.

     Al especificar la configuración de marca de agua personalizada, debe introducir valores mayores que

0.

Ver marcas de agua de almacenamiento optimizadas

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

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

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

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

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

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

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

Gestione el almacenamiento de metadatos de objetos

La capacidad de metadatos de objetos de un sistema StorageGRID controla la cantidad máxima de objetos que se pueden almacenar en ese sistema. Para garantizar que el sistema StorageGRID tenga espacio suficiente para almacenar objetos nuevos, debe comprender dónde y cómo StorageGRID almacena los metadatos de objetos.

¿Qué son los metadatos de objetos?

Los metadatos de objetos son cualquier información que describa un objeto. StorageGRID utiliza metadatos de objetos para realizar un seguimiento de las ubicaciones de todos los objetos en el grid y gestionar el ciclo de vida de cada objeto a lo largo del tiempo.

Para un objeto en StorageGRID, los metadatos de objeto incluyen los siguientes tipos de información:

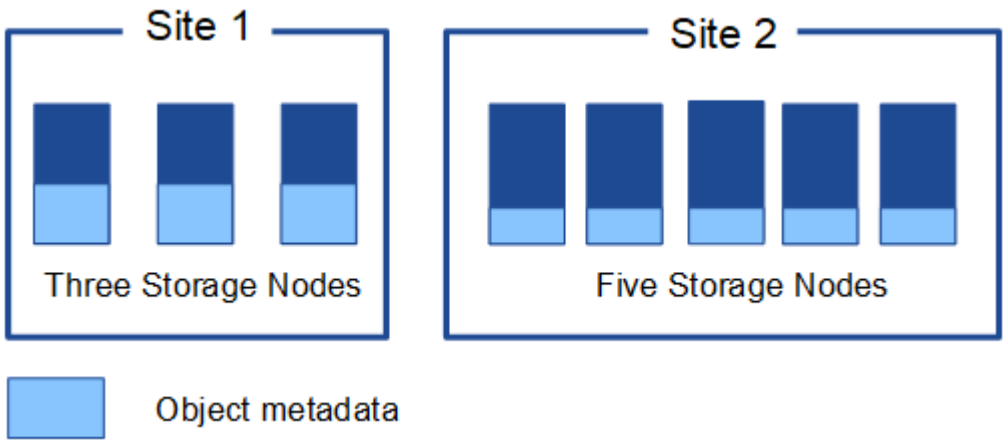
- Metadatos del sistema, incluidos un ID único para cada objeto (UUID), el nombre del objeto, el nombre del bloque de S3 o el contenedor Swift, el nombre o el ID de la cuenta de inquilino, el tamaño lógico del objeto, la fecha y la hora en que se creó el objeto por primera vez, y la fecha y hora en que 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, identificadores de segmentos y tamaños de datos.

¿Cómo se almacenan los metadatos de objetos?

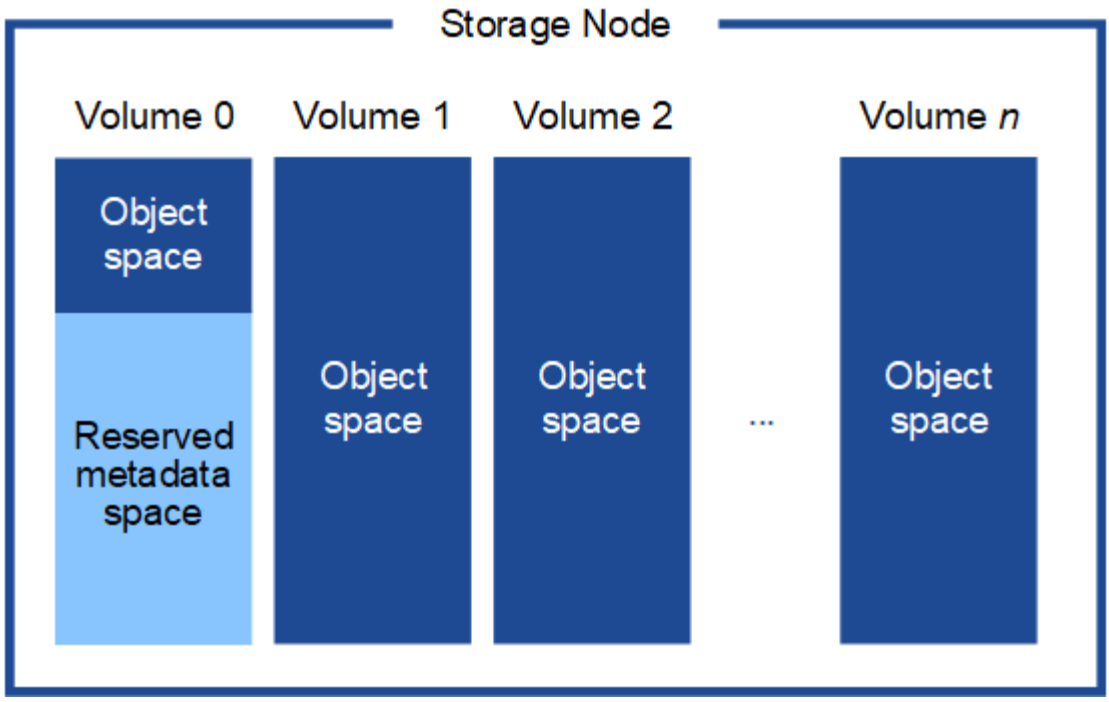
StorageGRID mantiene los metadatos de objetos en una base de datos de Cassandra, que se almacena independientemente de los datos de objetos. Para proporcionar redundancia y proteger los metadatos de objetos de la pérdida, StorageGRID almacena tres copias de los metadatos para todos los objetos del sistema en cada sitio.

Esta figura representa los nodos de almacenamiento de dos sitios. Cada sitio tiene la misma cantidad de metadatos de objeto y los metadatos de cada sitio se subdividen entre todos los nodos de almacenamiento de ese sitio.



¿Dónde se almacenan los metadatos de objetos?

En esta figura, se representan los volúmenes de almacenamiento para un único nodo de almacenamiento.



Como se muestra en la figura, StorageGRID reserva espacio para los metadatos del objeto en el volumen de almacenamiento 0 de cada nodo de almacenamiento. Utiliza el espacio reservado para almacenar metadatos de objetos y realizar operaciones esenciales de la base de datos. Cualquier espacio restante en el volumen de almacenamiento 0 y todos los demás volúmenes de almacenamiento del nodo de almacenamiento se utilizan exclusivamente para los datos de objetos (copias replicadas y fragmentos codificados de borrado).

La cantidad de espacio reservado para los metadatos de objeto en un nodo de almacenamiento en particular depende de varios factores, que se describen a continuación.

Valor de espacio reservado de metadatos

El *Metadata reserved space* es un valor para todo el sistema que representa la cantidad de espacio que se reservará para los metadatos en el volumen 0 de cada nodo de almacenamiento. Como se muestra en la tabla, el valor predeterminado de esta configuración se basa en:

- La versión de software que estaba utilizando cuando instaló inicialmente StorageGRID.
- La cantidad de RAM en cada nodo de almacenamiento.

Versión utilizada para la instalación inicial de StorageGRID	Cantidad de RAM en los nodos de almacenamiento	Valor predeterminado de espacio reservado de metadatos
11,5 a 11,8	128 GB o más en cada nodo de almacenamiento del grid	8 TB (8,000 GB)
	Debe haber menos de 128 GB en cualquier nodo de almacenamiento del grid	3 TB (3.000 GB)
11,1 a 11,4	128 GB o más en cada nodo de almacenamiento en un sitio	4 TB (4.000 GB)

Versión utilizada para la instalación inicial de StorageGRID	Cantidad de RAM en los nodos de almacenamiento	Valor predeterminado de espacio reservado de metadatos
	Menos de 128 GB en cualquier nodo de almacenamiento de cada sitio	3 TB (3.000 GB)
11,0 o anterior	Cualquier cantidad	2 TB (2.000 GB)

Ver valor de espacio reservado de metadatos

Siga estos pasos para ver la configuración de espacio reservado de metadatos para el sistema StorageGRID.

Pasos

1. Selecciona **CONFIGURACIÓN** > **Sistema** > **Ajustes de almacenamiento**.
2. En la página Configuración de almacenamiento, expanda la sección **Espacio reservado de metadatos**.

Para StorageGRID 11,8 o superior, el valor del espacio reservado de metadatos debe ser de al menos 100 GB y no más de 1 PB.

La configuración predeterminada para una nueva instalación de StorageGRID 11,6 o superior en la que cada nodo de almacenamiento tiene 128 GB o más de RAM es 8.000 GB (8 TB).

Espacio reservado real para los metadatos

En contraste con la configuración de espacio reservado de metadatos del sistema, el *espacio reservado real* para los metadatos del objeto se determina para cada nodo de almacenamiento. Para cualquier nodo de almacenamiento determinado, el espacio reservado real para los metadatos depende del tamaño del volumen 0 para el nodo y de la configuración de espacio reservado de metadatos en todo el sistema.

El tamaño del volumen 0 para el nodo	Espacio reservado real para los metadatos
Menos de 500 GB (uso fuera de producción)	10% del volumen 0
500 GB o más o Nodos de almacenamiento solo de metadatos	El menor de estos valores: • Volumen 0 • Valor de espacio reservado de metadatos **Nota**: Solo se requiere un rangedb para los nodos de almacenamiento solo de metadatos.

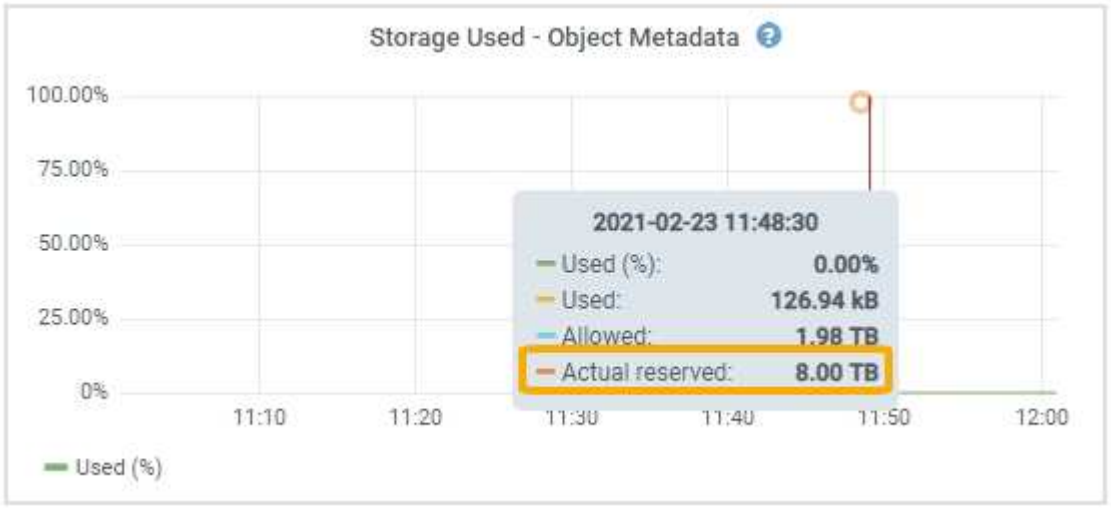
Ver el espacio reservado real para metadatos

Siga estos pasos para ver el espacio reservado real para metadatos en un nodo de almacenamiento en particular.

Pasos

1. En Grid Manager, seleccione **NODES** > ***Storage Node***.

2. Seleccione la ficha **almacenamiento**.
3. Coloque el cursor sobre el gráfico Almacenamiento usado - Metadatos de objetos y localice el valor **Real reserved**.



En la captura de pantalla, el valor **Real reservado** es 8 TB. Esta captura de pantalla es para un nodo de almacenamiento grande en una nueva instalación de StorageGRID 11.6. Debido a que el valor de espacio reservado de metadatos del sistema es menor que el volumen 0 para este nodo de almacenamiento, el espacio reservado real para este nodo es igual al valor de espacio reservado de metadatos.

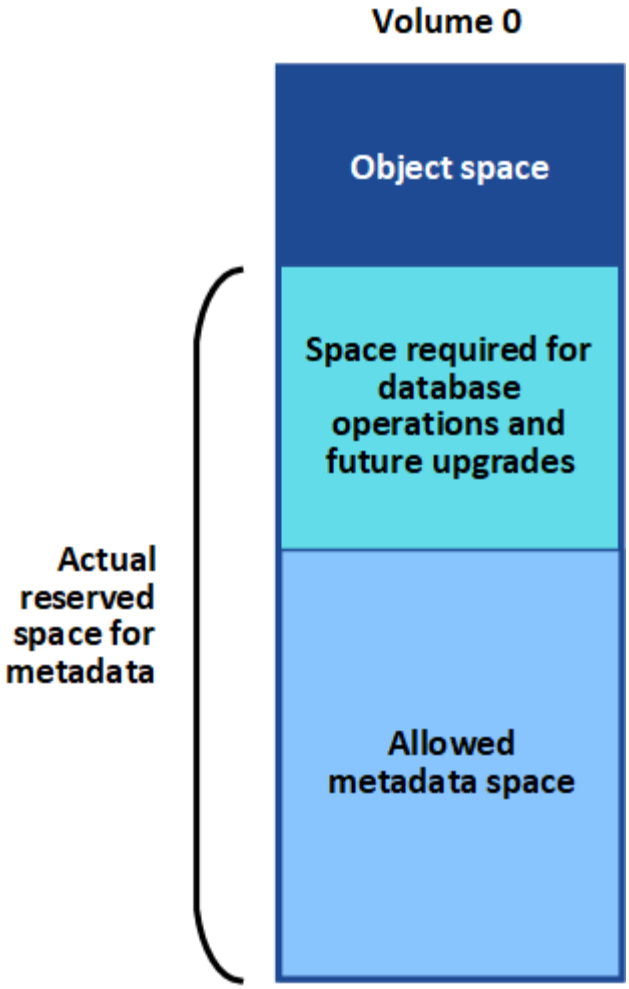
Ejemplo de espacio de metadatos reservado real

Suponga que instala un nuevo sistema StorageGRID mediante la versión 11,7 o posterior. Para este ejemplo, supongamos que cada nodo de almacenamiento tiene más de 128 GB de RAM y que el volumen 0 del nodo de almacenamiento 1 (SN1) es de 6 TB. Según estos valores:

- El espacio reservado **Metadatos** para todo el sistema se establece en 8 TB. (Este es el valor predeterminado para una nueva instalación de StorageGRID 11,6 o superior si cada nodo de almacenamiento tiene más de 128 GB de RAM).
- El espacio reservado real para los metadatos de SN1 es de 6 TB. (Todo el volumen está reservado porque el volumen 0 es más pequeño que el ajuste **Metadatos de espacio reservado**).

Espacio de metadatos permitido

El espacio reservado real de cada nodo de almacenamiento para metadatos se subdivide en el espacio disponible para los metadatos del objeto (el *espacio de metadatos permitido*) y el espacio necesario para las operaciones esenciales de la base de datos (como compactación y reparación) y las futuras actualizaciones de hardware y software. El espacio de metadatos permitido rige la capacidad general del objeto.



En la tabla siguiente se muestra cómo StorageGRID calcula el **espacio de metadatos permitido** para diferentes nodos de almacenamiento, en función de la cantidad de memoria del nodo y del espacio reservado real para los metadatos.

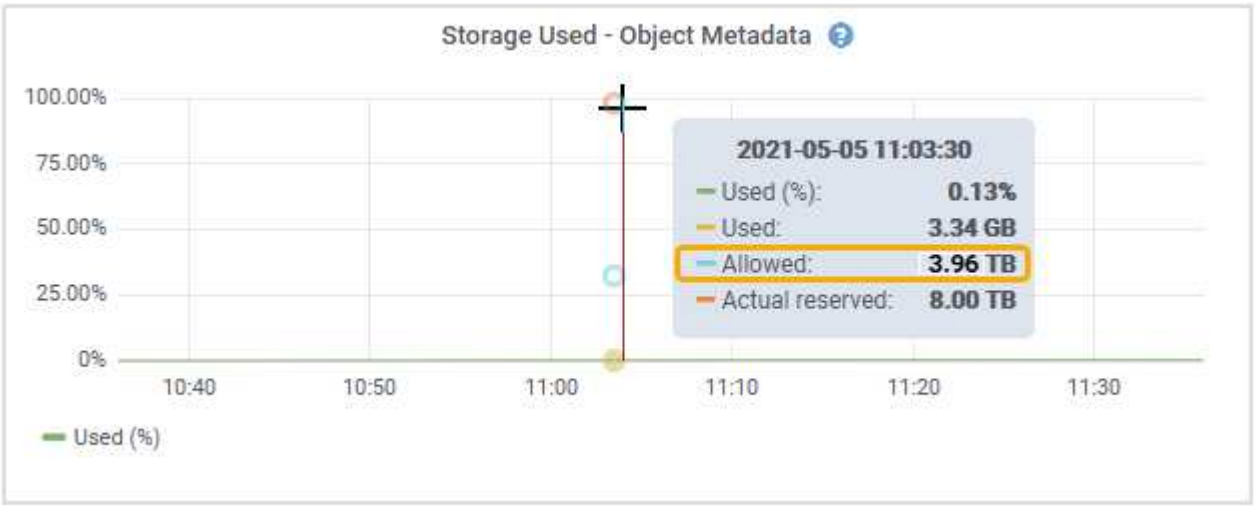
		Cantidad de memoria en el nodo de almacenamiento	
	< 128 GB	>= 128 GB	**Espacio reservado real para metadatos**
⇐ 4 TB	60 % del espacio reservado real para metadatos, hasta un máximo de 1.32 TB	60 % del espacio reservado real para metadatos, hasta un máximo de 1,98 TB	4 TB

Ver el espacio de metadatos permitido

Siga estos pasos para ver el espacio de metadatos permitido para un nodo de almacenamiento.

Pasos

1. En Grid Manager, seleccione **NODES**.
2. Seleccione el nodo de almacenamiento.
3. Seleccione la ficha **almacenamiento**.
4. Coloque el cursor sobre el gráfico de metadatos de objetos Storage Used y localice el valor **Allowed**.



En la captura de pantalla, el valor **Permitido** es 3,96 TB, que es el valor máximo para un nodo de almacenamiento cuyo espacio reservado real para metadatos es superior a 4 TB.

El valor **permitido** corresponde a esta métrica Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Ejemplo de espacio de metadatos permitido

Supongamos que instala un sistema StorageGRID mediante la versión 11.6. Para este ejemplo, supongamos que cada nodo de almacenamiento tiene más de 128 GB de RAM y que el volumen 0 del nodo de almacenamiento 1 (SN1) es de 6 TB. Según estos valores:

- El espacio reservado **Metadatos** para todo el sistema se establece en 8 TB. (Este es el valor predeterminado para StorageGRID 11,6 o superior cuando cada nodo de almacenamiento tiene más de 128 GB de RAM.)
- El espacio reservado real para los metadatos de SN1 es de 6 TB. (Todo el volumen está reservado porque el volumen 0 es más pequeño que el ajuste **Metadatos de espacio reservado**).
- El espacio permitido para los metadatos en SN1 es de 3 TB, según el cálculo mostrado en la tabla para el espacio permitido para los metadatos: (Espacio reservado real para metadatos − 1 TB) × 60%, hasta un máximo de 3.96 TB.

Cómo afectan los nodos de almacenamiento de diferentes tamaños a la capacidad de objetos

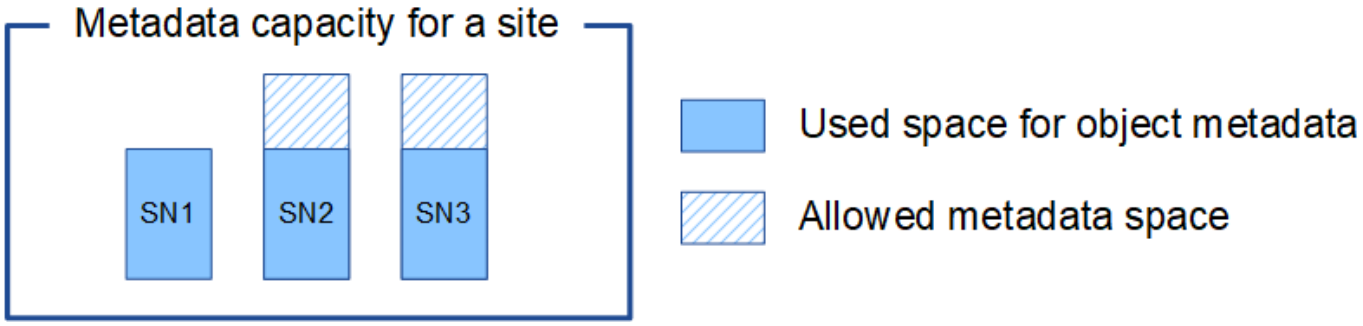
Como se ha descrito anteriormente, StorageGRID distribuye uniformemente los metadatos de objetos de los nodos de almacenamiento de cada sitio. Por este motivo, si un sitio contiene nodos de almacenamiento de distintos tamaños, el nodo más pequeño del sitio determina la capacidad de metadatos del sitio.

Observe el siguiente ejemplo:

- Hay una cuadrícula de un solo sitio que contiene tres nodos de almacenamiento de distintos tamaños.
- La configuración de espacio reservado **Metadatos** es de 4 TB.
- Los nodos de almacenamiento tienen los siguientes valores para el espacio de metadatos reservado real y el espacio de metadatos permitido.

Nodo de almacenamiento	Tamaño del volumen 0	Espacio real de metadatos reservado	Espacio de metadatos permitido
SN1	2,2 TB	2,2 TB	1,32 TB
SN2	5 TB	4 TB	1,98 TB
SN3	6 TB	4 TB	1,98 TB

Como los metadatos de objetos se distribuyen uniformemente por los nodos de almacenamiento de un sitio, cada nodo de este ejemplo solo puede contener 1.32 TB de metadatos. No se pueden utilizar los 0,66 TB adicionales de espacio permitido para SN2 y SN3.



De igual modo, como StorageGRID mantiene todos los metadatos de objetos para un sistema StorageGRID en cada sitio, la capacidad general de metadatos de un sistema StorageGRID viene determinada por la capacidad de metadatos de objetos del sitio más pequeño.

Además, dado que la capacidad de metadatos de los objetos controla el recuento máximo de objetos, cuando un nodo se queda sin capacidad de metadatos, el grid está lleno de eficacia.

Información relacionada

- Para obtener más información sobre cómo supervisar la capacidad de metadatos del objeto para cada nodo de almacenamiento, consulte las instrucciones para "Supervisión de StorageGRID".
- Para aumentar la capacidad de metadatos de objetos del sistema, "expanda una cuadrícula" Añadiendo nuevos nodos de almacenamiento.

Aumentar el espacio reservado de metadatos

Es posible que pueda aumentar la configuración del sistema de espacio reservado de metadatos si los nodos de almacenamiento cumplen con los requisitos específicos de RAM y espacio disponible.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".

- Usted tiene la "Permiso de acceso raíz o configuración de página de topología de cuadrícula y otros permisos de configuración de cuadrícula".

Acerca de esta tarea

Es posible que pueda aumentar manualmente la configuración del espacio reservado de metadatos en todo el sistema hasta 8 TB.

Sólo puede aumentar el valor de la configuración espacio reservado de metadatos para todo el sistema si ambas sentencias son verdaderas:

- Los nodos de almacenamiento de cualquier sitio del sistema tienen 128 GB o más de RAM.
- Los nodos de almacenamiento de cualquier sitio del sistema tienen suficiente espacio disponible en el volumen de almacenamiento 0.

Tenga en cuenta que, si aumenta esta configuración, reducirá al mismo tiempo el espacio disponible para el almacenamiento de objetos en el volumen de almacenamiento 0 de todos los nodos de almacenamiento. Por este motivo, es posible que prefiera establecer el espacio reservado de metadatos en un valor inferior a 8 TB, según sus requisitos esperados de metadatos de objetos.

> En general, es mejor utilizar un valor más alto en lugar de uno más bajo. Si la configuración espacio reservado de metadatos es demasiado grande, puede disminuirla más adelante. Por el contrario, si aumenta el valor más adelante, es posible que el sistema necesite mover datos de objetos para liberar espacio.

Para obtener una explicación detallada de cómo el valor de Espacio Reservado de Metadatos afecta al espacio permitido para el almacenamiento de metadatos de objetos en un nodo de almacenamiento en particular, consulte "Gestione el almacenamiento de metadatos de objetos".

Pasos

1. Determine la configuración actual del espacio reservado de metadatos.
   a. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de almacenamiento**.
   b. En la sección Marcas de agua de almacenamiento, anote el valor de **espacio reservado de metadatos**.
2. Asegúrese de tener suficiente espacio disponible en el volumen de almacenamiento 0 de cada nodo de almacenamiento para aumentar este valor.
   a. Selecciona **NODOS**.
   b. Seleccione el primer nodo de almacenamiento de la cuadrícula.
   c. Seleccione la pestaña almacenamiento.
   d. En la sección de volúmenes, localice la entrada **/var/local/rangedb/0**.
   e. Confirme que el valor disponible es igual o mayor que la diferencia entre el nuevo valor que desea utilizar y el valor espacio reservado de metadatos actual.

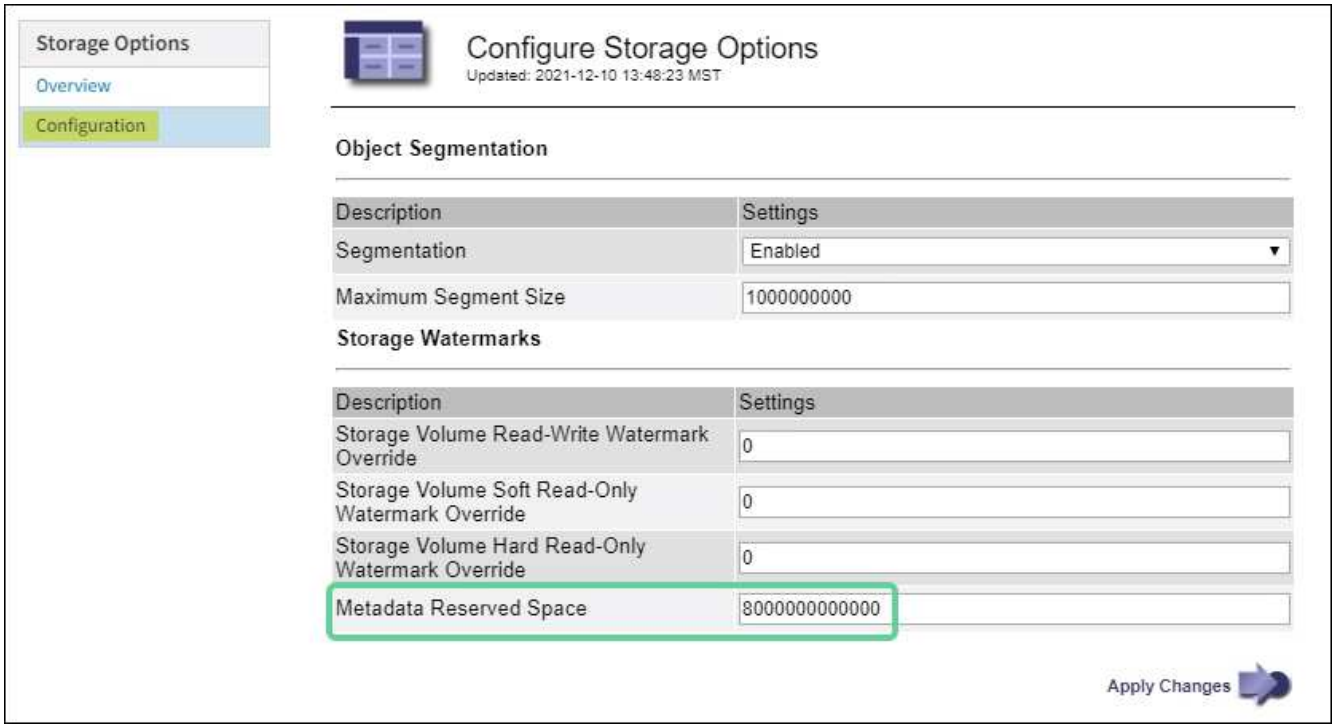
      Por ejemplo, si la configuración de espacio reservado de metadatos es actualmente 4 TB y desea aumentarla a 6 TB, el valor disponible debe ser 2 TB o superior.

   f. Repita estos pasos para todos los nodos de almacenamiento.
      - Si uno o más nodos de almacenamiento no tienen suficiente espacio disponible, no se puede aumentar el valor del espacio reservado de metadatos. No continúe con este procedimiento.

- Si cada nodo de almacenamiento tiene suficiente espacio disponible en el volumen 0, vaya al paso siguiente.

3. Asegúrese de tener al menos 128 GB de RAM en cada nodo de almacenamiento.
   a. Selecciona **NODOS**.
   b. Seleccione el primer nodo de almacenamiento de la cuadrícula.
   c. Seleccione la ficha **hardware**.
   d. Pase el cursor sobre el gráfico uso de memoria. Asegúrese de que **memoria total** es de al menos 128 GB.
   e. Repita estos pasos para todos los nodos de almacenamiento.
      - Si uno o más nodos de almacenamiento no tienen suficiente memoria total disponible, no es posible aumentar el valor del espacio reservado de metadatos. No continúe con este procedimiento.
      - Si cada nodo de almacenamiento tiene al menos 128 GB de memoria total, vaya al siguiente paso.
4. Actualice la configuración espacio reservado de metadatos.
   a. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de almacenamiento**.
   b. Seleccione la ficha Configuración.
   c. En la sección Marcas de agua de almacenamiento, seleccione **espacio reservado de metadatos**.
   d. Introduzca el nuevo valor.

      Por ejemplo, para introducir 8 TB, que es el valor máximo admitido, introduzca **8000000000000** (8, seguido de 12 ceros)



   a. Seleccione **aplicar cambios**.

Comprimir objetos almacenados

Es posible habilitar la compresión de objetos para reducir el tamaño de los objetos almacenados en StorageGRID, de modo que los objetos consuman menos almacenamiento.

Antes de empezar

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

Acerca de esta tarea

De forma predeterminada, la compresión de objetos está deshabilitada. Si habilita la compresión, StorageGRID intenta comprimir cada objeto al guardarlo, utilizando la compresión sin pérdidas.

> Si cambia este ajuste, el nuevo ajuste tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para el rendimiento y el escalado.

Antes de habilitar la compresión de objetos, tenga en cuenta lo siguiente:

- No debe seleccionar **Comprimir objetos almacenados** a menos que sepa que los datos almacenados son comprimibles.
- Las aplicaciones que guardan objetos en StorageGRID pueden comprimir objetos antes de guardarlos. Si una aplicación cliente ya ha comprimido un objeto antes de guardarlo en StorageGRID, al seleccionar esta opción no se reducirá aún más el tamaño de un objeto.
- No seleccione **Comprimir objetos almacenados** si utiliza NetApp FabricPool con StorageGRID.
- Si se selecciona **Comprimir objetos almacenados**, las aplicaciones cliente S3 y Swift deben evitar realizar operaciones GetObject que especifiquen un rango de bytes. Estas operaciones de «lectura de rango» son ineficientes, puesto que StorageGRID debe descomprimir los objetos de forma efectiva para acceder a los bytes solicitados. Las operaciones GetObject que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, no es eficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

  Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden tener un tiempo de espera.

  > Si necesita comprimir objetos y su aplicación cliente debe utilizar lecturas de rango, aumente el tiempo de espera de lectura de la aplicación.

Pasos

1. Selecciona **CONFIGURACIÓN** > **Sistema** > **Ajustes de almacenamiento** > **Compresión de objetos**.
2. Seleccione la casilla de verificación **Comprimir objetos almacenados**.
3. Seleccione **Guardar**.

Opciones de configuración del nodo de almacenamiento

Cada nodo de almacenamiento utiliza varias opciones de configuración y contadores. Puede que necesite ver los ajustes actuales o restablecer contadores para borrar alarmas (sistema heredado).

Excepto cuando se le indique específicamente en la documentación, debe consultar con el soporte técnico antes de modificar los ajustes de configuración de nodos de almacenamiento. Según sea necesario, puede restablecer los contadores de eventos para borrar las alarmas heredadas.

Siga estos pasos para acceder a la configuración y los contadores de un nodo de almacenamiento.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > ***Storage Node***.
3. Expanda el nodo de almacenamiento y seleccione el servicio o el componente.
4. Seleccione la ficha **Configuración**.

Las siguientes tablas resumen los ajustes de configuración de nodos de almacenamiento.

LDR

Nombre de atributo	Codificación	Descripción
Estado HTTP	HSTE	El estado actual de HTTP para S3, Swift y otro tráfico StorageGRID interno: • Sin conexión: No se permiten operaciones y cualquier aplicación cliente que intente abrir una sesión HTTP al servicio LDR recibe un mensaje de error. Las sesiones activas se cierran correctamente. • En línea: El funcionamiento continúa con normalidad
HTTP de inicio automático	HTA	• Si se selecciona, el estado del sistema al reiniciar depende del estado del componente **LDR** > **almacenamiento**. Si el componente **LDR** > **almacenamiento** es de sólo lectura al reiniciar, la interfaz HTTP también es de sólo lectura. Si el componente **LDR** > **almacenamiento** está en línea, HTTP también está en línea. De lo contrario, la interfaz HTTP permanece en estado sin conexión. • Si no se selecciona, la interfaz HTTP permanece sin conexión hasta que se habilita explícitamente.

LDR > almacén de datos

Nombre de atributo	Codificación	Descripción
Restablecer recuento de objetos perdidos	RCOR	Restablezca el contador del número de objetos perdidos en este servicio.

LDR > almacenamiento

Nombre de atributo	Codificación	Descripción
Estado de almacenamiento — deseado	SSD	Una configuración que puede configurar el usuario para el estado deseado del componente de almacenamiento. El servicio LDR lee este valor e intenta hacer coincidir el estado indicado por este atributo. El valor se mantiene de un reinicio a otro. Por ejemplo, puede usar esta configuración para forzar a que el almacenamiento pase a ser de solo lectura, incluso si hay un gran espacio de almacenamiento disponible. Esto puede ser útil para la solución de problemas. El atributo puede tomar uno de los siguientes valores: • Sin conexión: Cuando el estado deseado es sin conexión, el servicio LDR desconecta el componente **LDR** > **almacenamiento**. • Solo lectura: Cuando el estado deseado es de solo lectura, el servicio LDR mueve el estado de almacenamiento a Sólo lectura y deja de aceptar nuevo contenido. Sin embargo, el servicio LDR sigue aceptando solicitudes de depuración y eliminación basadas en S3 o ILM. Tenga en cuenta que el contenido puede seguir guardado en el nodo de almacenamiento durante un breve periodo hasta que se cierran las sesiones abiertas. • En línea: Deje el valor en línea durante el funcionamiento normal del sistema. Estado del almacenamiento: El servicio establecerá de forma dinámica la corriente del componente de almacenamiento en función del estado del servicio LDR, como la cantidad de espacio de almacenamiento de objetos disponible. Si el espacio es bajo, el componente se convierte en de solo lectura.
Tiempo de espera de comprobación del estado	HCT	El límite de tiempo en segundos en el que debe completarse una prueba de comprobación del estado para que un volumen de almacenamiento se considere correcto. Cambie este valor solo cuando lo indique el equipo de soporte de.

LDR > verificación

Nombre de atributo	Codificación	Descripción
Restablecer recuento de objetos que faltan	VCMI	Restablece el recuento de objetos que faltan detectados (OMIS). Utilice sólo una vez completada la comprobación de la existencia del objeto. El sistema StorageGRID restaura automáticamente los datos de objetos replicados que faltan.
Tasa de verificación	VPRI	Establecer la velocidad a la que se realiza la verificación en segundo plano. Consulte la información sobre la configuración de la tasa de verificación en segundo plano.
Restablecer recuento de objetos dañados	VCCR	Restablece el contador para los datos de objetos replicados dañados que se han encontrado durante la verificación en segundo plano. Esta opción se puede utilizar para borrar la condición de alarma objetos dañados detectados (OCOR).
Eliminar objetos en cuarentena	OQRT	Eliminar objetos dañados del directorio de cuarentena, restablecer el recuento de objetos en cuarentena a cero y borrar la alarma objetos en cuarentena detectados (OQRT). Esta opción se utiliza después de que el sistema StorageGRID restaura automáticamente los objetos dañados. Si se activa una alarma objetos perdidos, es posible que el soporte técnico desee acceder a los objetos en cuarentena. En algunos casos, los objetos en cuarentena podrían ser útiles para la recuperación de datos o para depurar los problemas subyacentes que causaron las copias de objetos dañadas.

LDR > codificación de borrado

Nombre de atributo	Codificación	Descripción
Restablecer el número de errores de escritura	RSWF	Restablezca el contador para obtener errores de escritura de los datos de objetos codificados con borrado al nodo de almacenamiento.
Recuento de errores de restablecimiento de lecturas	RSRF	Restablezca el contador para ver los errores de lectura de los datos de objetos codificados con borrado desde el nodo de almacenamiento.
Restablecer recuento de errores de eliminación	RSDF	Restablezca el contador para eliminar errores de datos de objetos codificados con borrado desde el nodo de almacenamiento.

Nombre de atributo	Codificación	Descripción
Restablecer el número de copias dañadas detectadas	RSCC	Restablezca el contador del número de copias dañadas de datos de objetos codificados con borrado en el nodo de almacenamiento.
Restablecer recuento de fragmentos dañados detectados	RSCD	Restablezca el contador para fragmentos dañados de datos de objetos codificados con borrado en el nodo de almacenamiento.
Restablecer recuento de fragmentos perdidos detectados	RSMD	Restablezca el contador para ver los fragmentos faltantes de datos de objetos codificados con borrado en el nodo de almacenamiento. Utilice sólo una vez completada la comprobación de la existencia del objeto.

LDR > replicación

Nombre de atributo	Codificación	Descripción
Restablecer recuento de fallos de replicación entrante	RICR	Restablezca el contador de fallos de replicación de entrada. Esto se puede utilizar para borrar la alarma RIRF (replicación entrante — fallida).
Restablecer recuento de fallos de replicación de salida	RCR	Restablezca el contador para fallos de replicación saliente. Esto se puede utilizar para borrar la alarma RORF (réplicas de salida — fallida).
Desactivar la replicación entrante	DSIR	Seleccione esta opción para desactivar la replicación entrante como parte de un procedimiento de mantenimiento o prueba. Deje sin marcar durante el funcionamiento normal. Cuando la replicación entrante está desactivada, los objetos se pueden recuperar del nodo de almacenamiento para copiarlos en otras ubicaciones del sistema StorageGRID, pero los objetos no se pueden copiar en este nodo de almacenamiento desde otras ubicaciones: El servicio LDR es de solo lectura.

Nombre de atributo	Codificación	Descripción
Desactive la replicación saliente	DSOR	Seleccione esta opción para deshabilitar la replicación saliente (incluidas las solicitudes de contenido para las recuperaciones HTTP) como parte de un procedimiento de mantenimiento o de prueba. Deje sin marcar durante el funcionamiento normal. Cuando la replicación saliente está desactivada, los objetos se pueden copiar en este nodo de almacenamiento, pero los objetos no se pueden recuperar del nodo de almacenamiento para copiarlos en otras ubicaciones del sistema StorageGRID. El servicio LDR es de sólo escritura.

Gestione nodos de almacenamiento completos

A medida que los nodos de almacenamiento alcancen la capacidad, debe ampliar el sistema StorageGRID añadiendo almacenamiento nuevo. Hay tres opciones disponibles: Añadir volúmenes de almacenamiento, añadir bandejas de ampliación de almacenamiento y añadir nodos de almacenamiento.

Añadir volúmenes de almacenamiento

Cada nodo de almacenamiento es compatible con un número máximo de volúmenes de almacenamiento. El máximo definido varía según la plataforma. Si un nodo de almacenamiento contiene menos de la cantidad máxima de volúmenes de almacenamiento, es posible añadir volúmenes para aumentar su capacidad. Consulte las instrucciones para "Expandir un sistema StorageGRID".

Añada bandejas de ampliación del almacenamiento

Algunos nodos de almacenamiento de dispositivos StorageGRID, como el SG6060, pueden admitir bandejas de almacenamiento adicionales. Si tiene dispositivos StorageGRID con funcionalidades de expansión que todavía no se han expandido hasta la máxima capacidad, se pueden añadir bandejas de almacenamiento para aumentar la capacidad. Consulte las instrucciones para "Expandir un sistema StorageGRID".

Añada nodos de almacenamiento

Puede aumentar la capacidad de almacenamiento con la adición de nodos de almacenamiento. Al añadir almacenamiento, deben tenerse en cuenta las reglas de ILM activas y los requisitos de capacidad. Consulte las instrucciones para "Expandir un sistema StorageGRID".

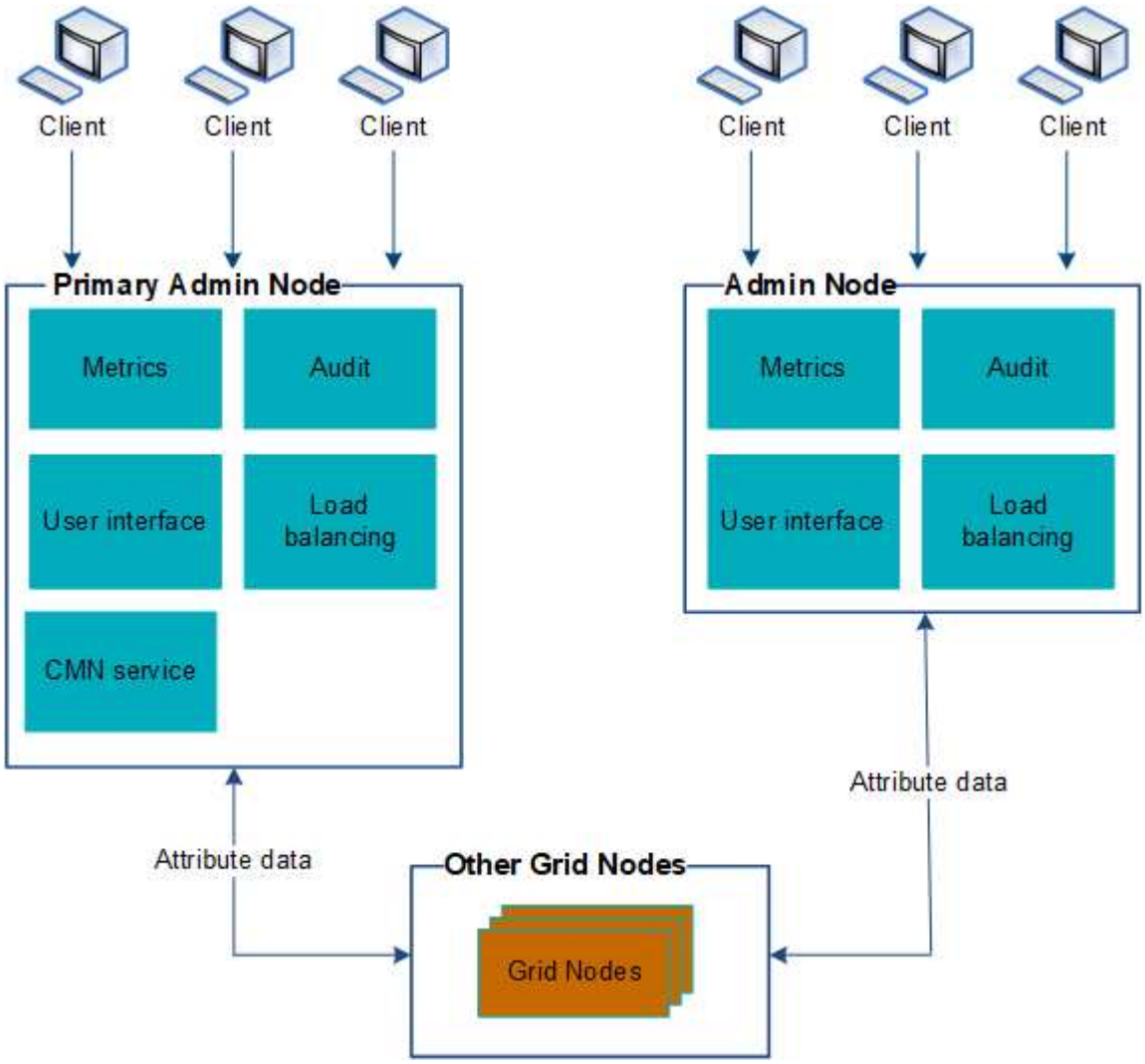
Gestione los nodos de administrador

Use varios nodos de administrador

Un sistema StorageGRID puede incluir varios nodos de administrador para permitir supervisar y configurar continuamente el sistema StorageGRID incluso si falla un nodo de administración.

Si un nodo de administración deja de estar disponible, el procesamiento de atributos continúa, las alertas y las alarmas (sistema heredado) siguen activándose y las notificaciones por correo electrónico y los paquetes de

AutoSupport aún se envían. Sin embargo, tener varios nodos de administración no ofrece protección de conmutación al nodo de respaldo, excepto notificaciones y paquetes de AutoSupport. En particular, las confirmaciones de alarma realizadas desde un nodo de administración no se copian en otros nodos de administración.



Si falla un nodo de administración, existen dos opciones para ver y configurar el sistema StorageGRID:

- Los clientes web pueden volver a conectarse a cualquier otro nodo de administrador disponible.
- Si un administrador del sistema ha configurado un grupo de nodos de administración de alta disponibilidad, los clientes web pueden seguir accediendo a Grid Manager o al Gestor de inquilinos mediante la dirección IP virtual del grupo de alta disponibilidad. Consulte "Gestión de grupos de alta disponibilidad".

> Al utilizar un grupo de alta disponibilidad, el acceso se interrumpe si el nodo de administración activo falla. Los usuarios deben volver a iniciar sesión después de que la dirección IP virtual del grupo ha conmute a otro nodo de administración del grupo.

Algunas tareas de mantenimiento solo se pueden realizar con el nodo de administrador principal. Si el nodo de administración principal falla, debe recuperarse antes de que el sistema StorageGRID vuelva a funcionar completamente.

Identifique el nodo de administración principal

El nodo de administración principal aloja el servicio CMN. Algunos procedimientos de mantenimiento solo se pueden realizar mediante el nodo de administrador principal.

Antes de empezar

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

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > **Admin Node** y, a continuación, seleccione ➕ Para expandir el árbol de topología y mostrar los servicios alojados en este nodo de administración.

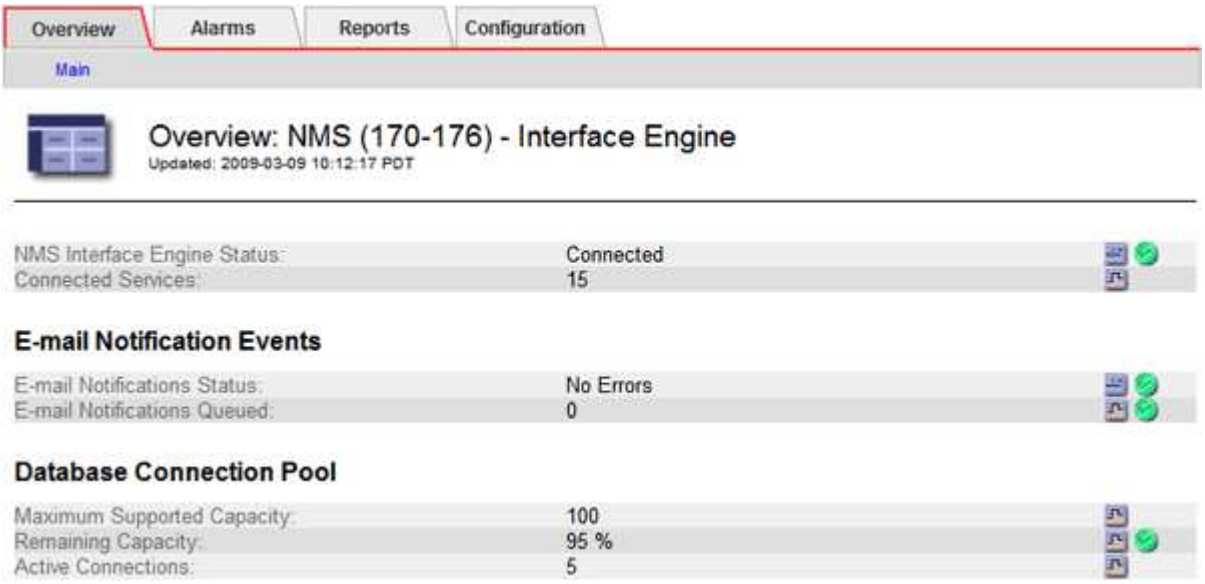
   El nodo de administración principal aloja el servicio CMN.

3. Si este nodo de administrador no aloja el servicio CMN, compruebe los demás nodos de administración.

Ver el estado de notificación y las colas

El servicio del sistema de administración de redes (NMS) en los nodos de administración envía notificaciones al servidor de correo. Puede ver el estado actual del servicio NMS y el tamaño de su cola de notificaciones en la página Motor de interfaz.

Para acceder a la página Motor de interfaz, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. Por último, seleccione ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.



Las notificaciones se procesan a través de la cola de notificaciones de correo electrónico y se envían al servidor de correo una tras otra en el orden en que se activan. Si hay un problema (por ejemplo, un error de conexión de red) y el servidor de correo no está disponible cuando se intenta enviar la notificación, un intento de mayor esfuerzo de reenviar la notificación al servidor de correo continúa durante un período de 60 segundos. Si la notificación no se envía al servidor de correo después de 60 segundos, la notificación se descarta de la cola de notificaciones y se realiza un intento de enviar la siguiente notificación de la cola.

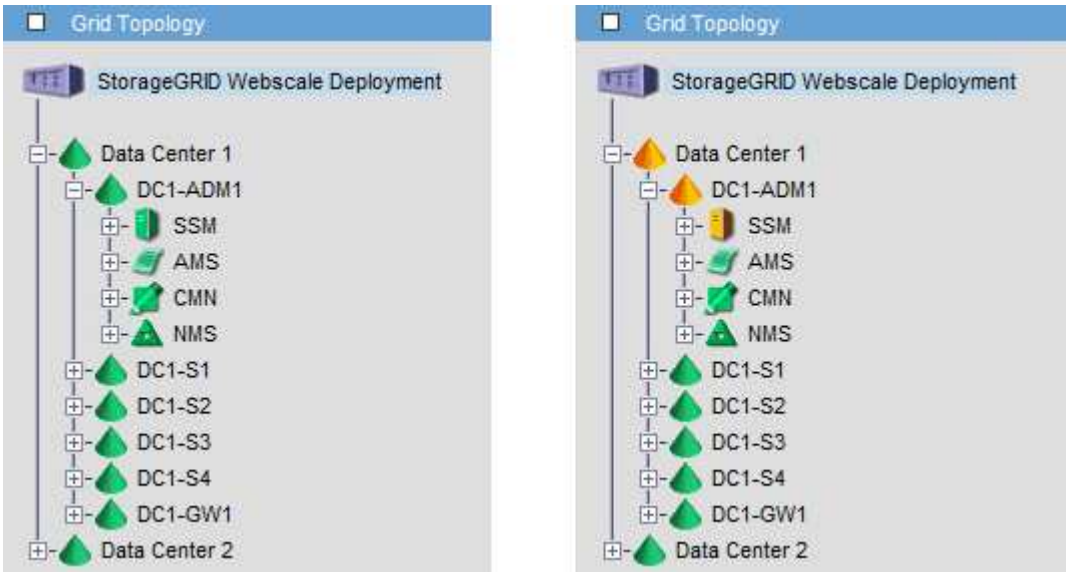
Puesto que las notificaciones se pueden borrar de la cola de notificaciones sin enviarse, es posible que se

active una alarma sin que se envíe una notificación. Si se elimina una notificación de la cola sin que se envíe, se activa la alarma secundaria MINS (Estado de notificación de correo electrónico).

Cómo muestran los nodos de administración alarmas confirmadas (sistema heredado)

Cuando reconoce una alarma en un nodo de administración, la alarma confirmada no se copia en ningún otro nodo de administración. Puesto que las confirmaciones no se copian en otros nodos de administración, el árbol de topología de cuadrícula puede no tener el mismo aspecto para cada nodo de administración.

Esta diferencia puede ser útil al conectar clientes Web. Los clientes web pueden tener diferentes vistas del sistema StorageGRID de acuerdo con las necesidades del administrador.



Tenga en cuenta que las notificaciones se envían desde el nodo de administración donde se produce la confirmación.

Configure el acceso de los clientes de auditoría

Configure el acceso del cliente de auditoría para NFS

El nodo Admin, a través del servicio sistema de administración de auditorías (AMS), registra todos los eventos del sistema auditados en un archivo de registro disponible a través del recurso compartido de auditoría, que se agrega a cada nodo Admin en la instalación. El recurso compartido de auditoría se habilita automáticamente como recurso compartido de solo lectura.

> La compatibilidad con NFS ha quedado obsoleta y se eliminará en una futura versión.

Para acceder a los registros de auditoría, puede configurar el acceso de clientes a recursos compartidos de auditoría para NFS. O bien, puede hacerlo "usar un servidor de syslog externo".

El sistema StorageGRID utiliza un reconocimiento positivo para evitar la pérdida de mensajes de auditoría antes de que se escriban en el archivo de registro. Un mensaje permanece en cola en un servicio hasta que el servicio AMS o un servicio intermedio de retransmisión de auditoría ha reconocido el control de él. Para obtener más información, consulte "Revisar los registros de auditoría".

Antes de empezar

- Usted tiene la `Passwords.txt` archivo con la contraseña root/admin.
- Usted tiene la `Configuration.txt` Archivo (disponible en el paquete de recuperación).
- El cliente de auditoría utiliza NFS versión 3 (NFSv3).

Acerca de esta tarea

Realice este procedimiento para cada nodo de administrador en una implementación de StorageGRID desde la que desea recuperar mensajes de auditoría.

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Confirme que todos los servicios tienen el estado en ejecución o verificado. Introduzca: `storagegrid-status`

   Si alguno de los servicios no aparece como en ejecución o verificado, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos. Pulse **Ctrl**+**C**.
4. Inicie la utilidad de configuración NFS. Introduzca: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

5. Agregue el cliente de auditoría: `add-audit-share`
   a. Cuando se le solicite, introduzca la dirección IP o el rango de direcciones IP del cliente de auditoría para el recurso compartido de auditoría: `client_IP_address`
   b. Cuando se le solicite, pulse **Intro**.
6. Si se permite que más de un cliente de auditoría acceda al recurso compartido de auditoría, agregue la dirección IP del usuario adicional: `add-ip-to-share`
   a. Introduzca el número del recurso compartido de auditoría: *`audit_share_number`*

b. Cuando se le solicite, introduzca la dirección IP o el rango de direcciones IP del cliente de auditoría para el recurso compartido de auditoría: *client_IP_address*

c. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de NFS.

d. Repita estos mismos pasos para cada cliente de auditoría adicional que tenga acceso al recurso compartido de auditoría.

7. De manera opcional, compruebe su configuración.

   a. Introduzca lo siguiente: `validate-config`

      Los servicios se comprueban y visualizan.

   b. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de NFS.

   c. Cierre la utilidad de configuración NFS: `exit`

8. Determine si debe habilitar los recursos compartidos de auditoría en otros sitios.

   - Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.
   - Si la implementación de StorageGRID incluye nodos de administración en otros sitios, habilite estos recursos compartidos de auditoría según sea necesario:

     i. Inicie sesión de forma remota en el nodo de administración del sitio:

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

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

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

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

     ii. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración adicional.

     iii. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota. Introduzca: `exit`

9. Cierre la sesión del shell de comandos: `exit`

   A los clientes de auditoría de NFS se les concede acceso a un recurso compartido de auditoría en función de su dirección IP. Conceda acceso al recurso compartido de auditoría a un nuevo cliente de auditoría de NFS añadiendo su dirección IP al recurso compartido o elimine un cliente de auditoría existente eliminando su dirección IP.

Agregar un cliente de auditoría NFS a un recurso compartido de auditoría

A los clientes de auditoría de NFS se les concede acceso a un recurso compartido de auditoría en función de su dirección IP. Conceda acceso al recurso compartido de auditoría a un nuevo cliente de auditoría de NFS añadiendo su dirección IP al recurso compartido de auditoría.

La compatibilidad con NFS ha quedado obsoleta y se eliminará en una futura versión.

Antes de empezar

- Usted tiene la `Passwords.txt` archivo con la contraseña de la cuenta root/admin.
- Tiene el `Configuration.txt` Archivo (disponible en el paquete de recuperación).
- El cliente de auditoría utiliza NFS versión 3 (NFSv3).

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Inicie la utilidad de configuración NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Introduzca: `add-ip-to-share`

   Se muestra una lista de los recursos compartidos de auditoría de NFS habilitados en el nodo de administración. El recurso compartido de auditoría aparece como: `/var/local/log`

4. Introduzca el número del recurso compartido de auditoría: *`audit_share_number`*
5. Cuando se le solicite, introduzca la dirección IP o el rango de direcciones IP del cliente de auditoría para el recurso compartido de auditoría: *`client_IP_address`*

   El cliente de auditoría se agrega al recurso compartido de auditoría.

6. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de NFS.

7. Repita los pasos para cada cliente de auditoría que se debe agregar al recurso compartido de auditoría.
8. Si lo desea, compruebe la configuración: `validate-config`

Los servicios se comprueban y visualizan.

a. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de NFS.

9. Cierre la utilidad de configuración NFS: `exit`
10. Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.

    De lo contrario, si la implementación de StorageGRID incluye nodos de administración en otros sitios, opcionalmente podrá habilitar estos recursos compartidos de auditoría según sea necesario:

    a. Inicie sesión de forma remota en el nodo de administración de un sitio:
       i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
       ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
       iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
       iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
    b. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración.
    c. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota: `exit`
11. Cierre la sesión del shell de comandos: `exit`

Comprobar la integración de auditoría de NFS

Después de configurar un recurso compartido de auditoría y agregar un cliente de auditoría NFS, puede montar el recurso compartido del cliente de auditoría y comprobar que los archivos estén disponibles en el recurso compartido de auditoría.

> La compatibilidad con NFS ha quedado obsoleta y se eliminará en una futura versión.

Pasos

1. Verifique la conectividad (o variante para el sistema cliente) usando la dirección IP del cliente del nodo de administración que aloja el servicio AMS. Introduzca: `ping IP_address`

   Verifique que el servidor responde, indicando conectividad.

2. Monte el recurso compartido de sólo lectura de auditoría usando un comando apropiado para el sistema operativo cliente. Un ejemplo de comando de Linux es (introduzca en una línea):

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/log myAudit`

   Utilice la dirección IP del nodo de administración que aloja el servicio AMS y el nombre de recurso compartido predefinido para el sistema de auditoría. El punto de montaje puede ser cualquier nombre seleccionado por el cliente (por ejemplo, *`myAudit`* en el comando anterior).

3. Verifique que los archivos estén disponibles en el recurso compartido de auditoría. Introduzca: `ls myAudit /*`

donde *myAudit* es el punto de montaje del recurso compartido de auditoría. Debe haber al menos un archivo de registro en la lista.

Eliminar un cliente de auditoría NFS del recurso compartido de auditoría

A los clientes de auditoría de NFS se les concede acceso a un recurso compartido de auditoría en función de su dirección IP. Puede eliminar un cliente de auditoría existente eliminando su dirección IP.

Antes de empezar

- Usted tiene la `Passwords.txt` archivo con la contraseña de la cuenta root/admin.
- Usted tiene la `Configuration.txt` Archivo (disponible en el paquete de recuperación).

Acerca de esta tarea

No puede eliminar la última dirección IP permitida para acceder al recurso compartido de auditoría.

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Inicie la utilidad de configuración NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Elimine la dirección IP del recurso compartido de auditoría: `remove-ip-from-share`

   Se muestra una lista numerada de recursos compartidos de auditoría configurados en el servidor. El recurso compartido de auditoría aparece como: `/var/local/log`

4. Introduzca el número correspondiente al recurso compartido de auditoría: *audit_share_number*

   Se muestra una lista numerada de direcciones IP permitidas para acceder al recurso compartido de auditoría.

5. Introduzca el número correspondiente a la dirección IP que desea eliminar.

   El recurso compartido de auditoría se actualiza y ya no se permite el acceso desde ningún cliente de auditoría con esta dirección IP.

6. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de NFS.

7. Cierre la utilidad de configuración NFS: `exit`
8. Si la implementación de StorageGRID es una puesta en marcha de varios sitios de centro de datos con nodos de administración adicionales en otros sitios, deshabilite estos recursos compartidos de auditoría según sea necesario:
   a. Inicie sesión de forma remota en el nodo de administración de cada sitio:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   b. Repita estos pasos para configurar los recursos compartidos de auditoría de cada nodo de administración adicional.
   c. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota: `exit`
9. Cierre la sesión del shell de comandos: `exit`

Cambiar la dirección IP de un cliente de auditoría de NFS

Complete estos pasos si necesita cambiar la dirección IP de un cliente de auditoría de NFS.

Pasos

1. Agregue una nueva dirección IP a un recurso compartido de auditoría NFS existente.
2. Elimine la dirección IP original.

Información relacionada

- "Agregar un cliente de auditoría NFS a un recurso compartido de auditoría"
- "Eliminar un cliente de auditoría NFS del recurso compartido de auditoría"

Gestione los nodos de archivado

Archivado en el cloud mediante la API de S3

Puede configurar un nodo de archivado para conectarse directamente a Amazon Web Services (AWS) o a cualquier otro sistema que pueda conectarse al sistema StorageGRID a través de la API de S3.

La compatibilidad con los nodos de archivo está obsoleta y se eliminará en una versión futura. El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades.

La opción Cloud Tiering - Simple Storage Service (S3) también queda obsoleta. Si está utilizando un nodo de archivado con esta opción, "Migre sus objetos a un pool de almacenamiento en la nube" en su lugar.

Además, debe eliminar los nodos de archivado de la política de gestión de la vida útil de la información activa en StorageGRID 11,7 o versiones anteriores. La eliminación de datos de objetos almacenados en nodos de archivado simplificará las actualizaciones futuras. Consulte "Trabajar con reglas de ILM y políticas de ILM".

Configure los ajustes de conexión para la API de S3

Si se conecta a un nodo de archivado con la interfaz de S3, debe configurar los ajustes de conexión para la API de S3. Hasta que se hayan configurado estos ajustes, el servicio ARC permanecerá en un estado de alarma principal, ya que no puede comunicarse con el sistema de almacenamiento de archivos externo.

La compatibilidad con los nodos de archivo está obsoleta y se eliminará en una versión futura. El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades.

La opción Cloud Tiering - Simple Storage Service (S3) también queda obsoleta. Si está utilizando un nodo de archivado con esta opción, "Migre sus objetos a un pool de almacenamiento en la nube" en su lugar.

Además, debe eliminar los nodos de archivado de la política de gestión de la vida útil de la información activa en StorageGRID 11,7 o versiones anteriores. La eliminación de datos de objetos almacenados en nodos de archivado simplificará las actualizaciones futuras. Consulte "Trabajar con reglas de ILM y políticas de ILM".

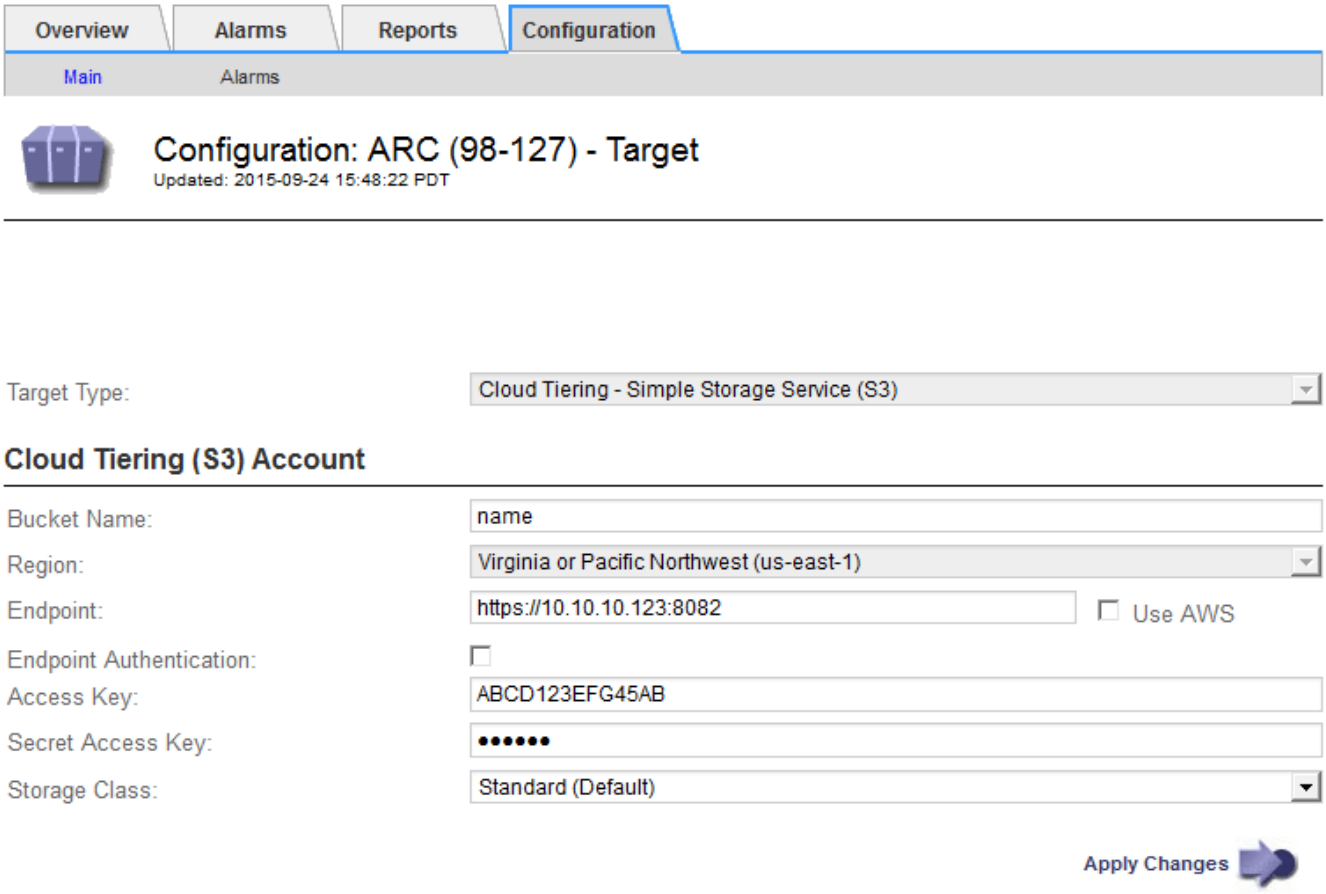
Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Ha creado un bucket en el sistema de almacenamiento de archivado de destino:
  - El bloque está dedicado a un único nodo de archivado. No puede ser utilizado por otros nodos de archivo u otras aplicaciones.
  - El cucharón tiene la región adecuada seleccionada para su ubicación.
  - El bloque debe configurarse con el control de versiones suspendido.
- La segmentación de objetos está activada y el tamaño máximo de segmento es menor o igual a 4.5 GIB (4,831,838,208 bytes). Las solicitudes de API S3 que superen este valor fallarán si se usa S3 como sistema de almacenamiento de archivado externo.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.

2. Seleccione **nodo de archivo** > **ARC** > **objetivo**.
3. Seleccione **Configuración** > **Principal**.



4. Seleccione **Cloud Tiering - simple Storage Service (S3)** en la lista desplegable Target Type.

> Los ajustes de configuración no estarán disponibles hasta que seleccione un tipo de destino.

5. Configure la cuenta de organización en niveles de cloud (S3) a través de la cual el nodo de archivado se conectará al sistema de almacenamiento de archivado externo compatible con S3 de destino.

   La mayoría de los campos en esta página son claros y explicativos. A continuación, se describen los campos que podrían presentar dificultades.

   - **Región**: Sólo está disponible si se selecciona **usar AWS**. La región que seleccione debe coincidir con la región del bloque.
   - **Endpoint** y **Use AWS**: Para Amazon Web Services (AWS), seleccione **usar AWS**. **Endpoint** se rellena automáticamente con una dirección URL de extremo basada en los atributos Nombre de bloque y Región. Por ejemplo:

     ```
     https://bucket.region.amazonaws.com
     ```

     En el caso de un destino que no sea AWS, introduzca la URL del sistema que aloja el bloque, incluido el número de puerto. Por ejemplo:

```
https://system.com:1080
```

- **Autenticación de punto final**: Activada de forma predeterminada. Si la red al sistema de almacenamiento de archivado externo es de confianza, puede desactivar la casilla de verificación para desactivar el certificado SSL de punto final y la verificación de nombre de host para el sistema de almacenamiento de archivado externo de destino. Si otra instancia de un sistema StorageGRID es el dispositivo de almacenamiento de archivado de destino y el sistema está configurado con certificados firmados públicamente, puede mantener la casilla de verificación seleccionada.
- **Clase de almacenamiento**: Seleccione **Estándar (predeterminado)** para almacenamiento normal. Seleccione **redundancia reducida** sólo para objetos que se puedan volver a crear fácilmente. **Redundancia reducida** proporciona almacenamiento de menor costo con menos confiabilidad. Si el sistema de almacenamiento de archivado objetivo es otra instancia del sistema StorageGRID, **clase de almacenamiento** controla cuántas copias provisionales del objeto se realizan durante el procesamiento en el sistema de destino, si se utiliza el COMMIT doble cuando se ingieren objetos allí.

6. Seleccione **aplicar cambios**.

   Los ajustes de configuración especificados se validan y se aplican al sistema StorageGRID. Después de aplicar la configuración, el destino no se puede cambiar.

Modifique la configuración de conexión para la API de S3

Una vez que se configura el nodo de archivado para conectarse a un sistema de almacenamiento de archivado externo a través de la API S3, puede modificar algunos ajustes si cambia la conexión.

Antes de empezar

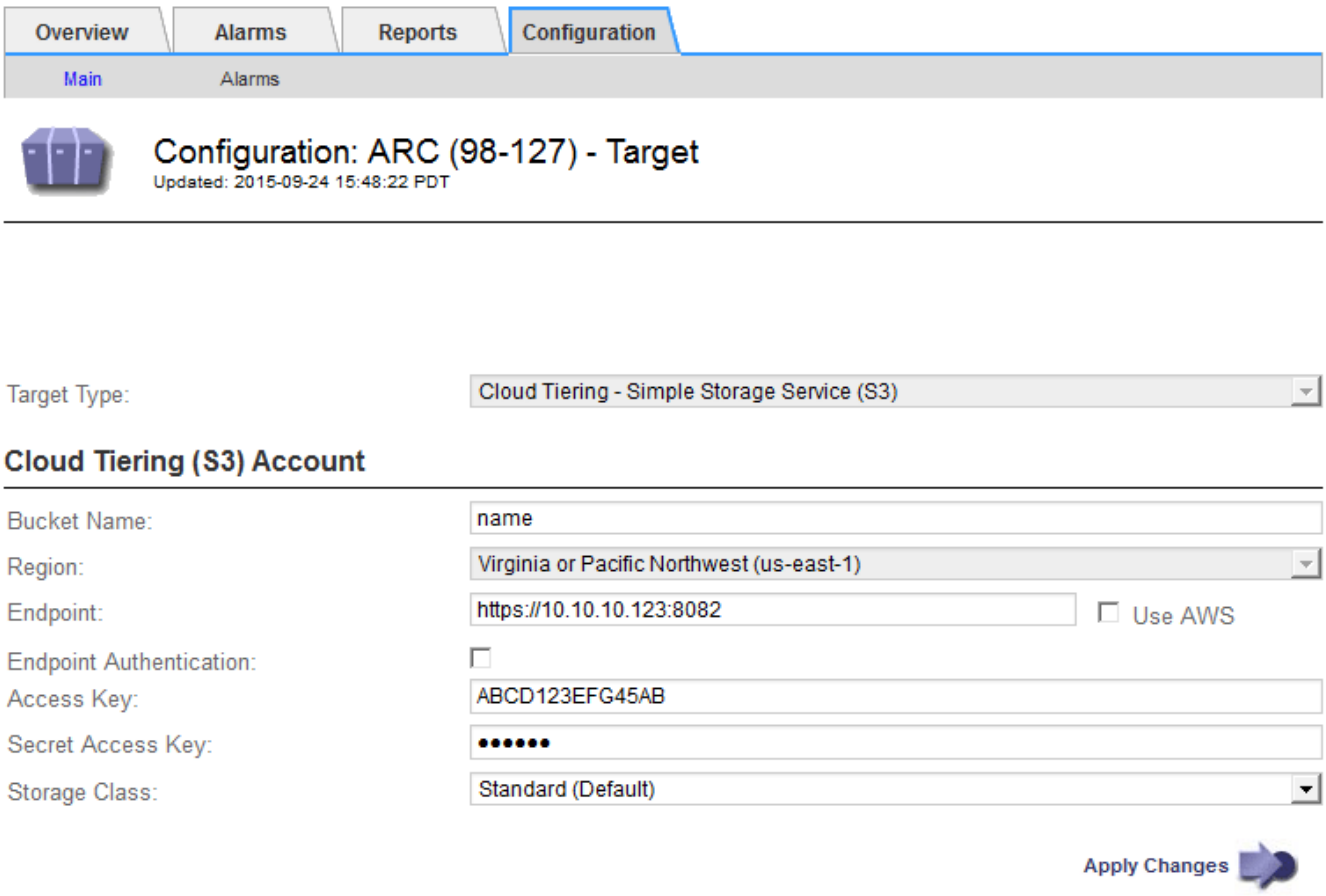
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".

Acerca de esta tarea

Si cambia la cuenta de Cloud Tiering (S3), debe asegurarse de que las credenciales de acceso del usuario tengan acceso de lectura/escritura al bloque, incluidos todos los objetos que el nodo de archivado había ingerido previamente en el bloque.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Target**.
3. Seleccione **Configuración** > **Principal**.



4. Modifique la información de la cuenta, según sea necesario.

   Si cambia la clase de almacenamiento, se almacenan datos de objeto nuevos con la nueva clase de almacenamiento. El objeto existente continúa almacenado en la clase de almacenamiento definida cuando se procesa.

   Nombre de bloque, región y punto final, utilice valores de AWS y no se puede cambiar.

5. Seleccione **aplicar cambios**.

Modifique el estado del servicio de organización en niveles del cloud

Puede controlar la capacidad de lectura y escritura del nodo de archivado en el sistema de almacenamiento de archivado externo objetivo que se conecta a través de la API de S3 cambiando el estado del servicio de organización en niveles de cloud.

Antes de empezar

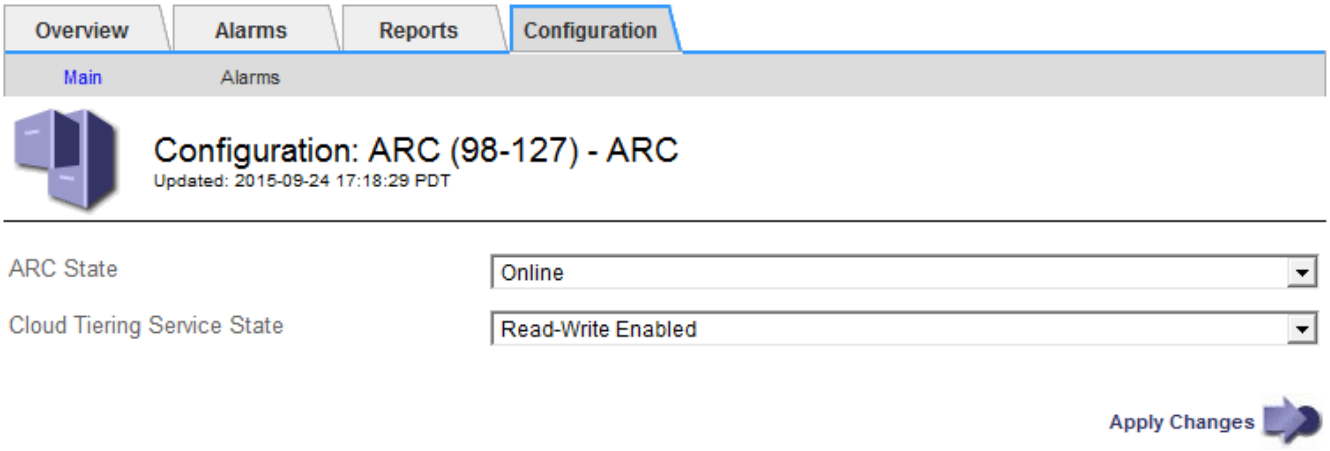
- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Debe configurarse el nodo de archivado.

Acerca de esta tarea

Puede desconectar el nodo de archivado de forma efectiva cambiando el estado del servicio de organización en niveles en la nube a **Read-Write Disabled**.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC**.
3. Seleccione **Configuración** > **Principal**.



4. Seleccione un **Estado del servicio de organización en niveles de la nube**.
5. Seleccione **aplicar cambios**.

Restablezca el número de errores de almacén para la conexión API de S3

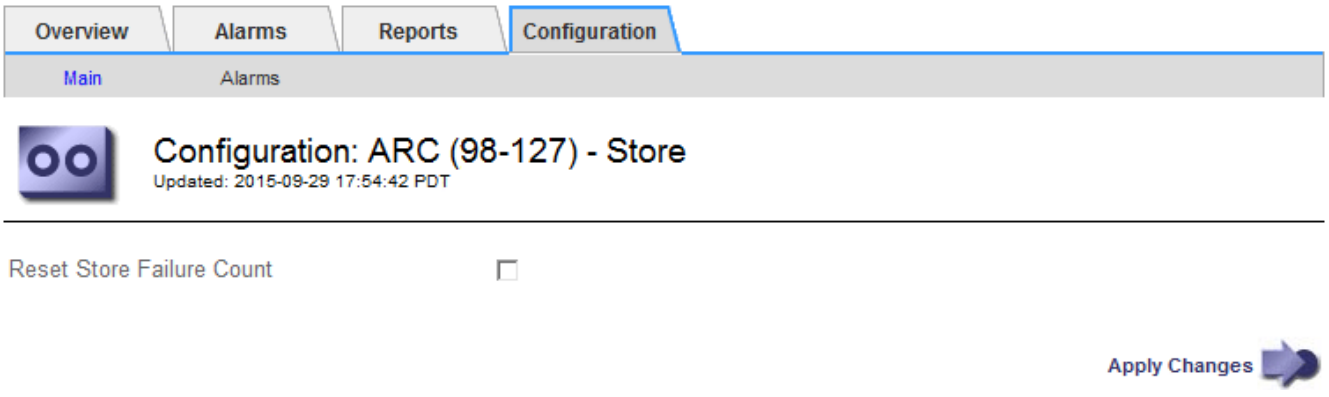
Si el nodo de archivado se conecta a un sistema de almacenamiento de archivado a través de la API de S3, puede restablecer el recuento de fallos de almacenamiento, que se puede utilizar para borrar la alarma de ARVF (fallos de almacenamiento).

Antes de empezar

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

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Store**.
3. Seleccione **Configuración** > **Principal**.



4. Seleccione **Restablecer recuento de fallos de tienda**.

5. Seleccione **aplicar cambios**.

   El atributo fallos de almacén se restablece a cero.

Migrar objetos desde organización en niveles en el cloud: S3 a un pool de almacenamiento en el cloud

Si actualmente está utilizando la función **Cloud Tiering - Simple Storage Service (S3)** para organizar en niveles los datos de objetos en un bucket S3, debe migrar sus objetos a un Cloud Storage Pool en su lugar. Los pools de almacenamiento en cloud proporcionan un método escalable que aprovecha todos los nodos de almacenamiento del sistema StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Ya ha almacenado objetos en el bloque de S3 configurado para la organización en niveles del cloud.

> Antes de migrar datos de objetos, póngase en contacto con su representante de cuenta de NetApp para comprender y gestionar cualquier coste asociado.

Acerca de esta tarea

Desde el punto de vista de la gestión del ciclo de vida de la información, un pool de almacenamiento en cloud es similar al de un pool de almacenamiento. Sin embargo, si bien los pools de almacenamiento constan de nodos de almacenamiento o nodos de archivado dentro del sistema StorageGRID, un pool de almacenamiento en cloud consta de un bloque S3 externo.

Antes de migrar objetos desde Cloud Tiering: S3 a un pool de almacenamiento en cloud, primero debe crear un bucket de S3 y, a continuación, crear el Cloud Storage Pool en StorageGRID. A continuación, se puede crear una nueva política de ILM y reemplazar la regla de ILM utilizada para almacenar objetos en el bloque de niveles de cloud con una regla de ILM clonada que almacena los mismos objetos en el Cloud Storage Pool.

> Cuando los objetos se almacenan en un pool de almacenamiento en cloud, las copias de esos objetos no se pueden almacenar también en StorageGRID. Si la regla de ILM que está usando actualmente para la organización en niveles del cloud está configurada para almacenar objetos en varias ubicaciones a la vez, considere si desea realizar esta migración opcional porque perderá esa funcionalidad. Si continúa con esta migración, debe crear nuevas reglas en lugar de clonar las existentes.

Pasos

1. Cree un pool de almacenamiento en el cloud.

   Utilice un nuevo bloque de S3 para el Cloud Storage Pool a fin de garantizar que solo contenga los datos gestionados por el Cloud Storage Pool.

2. Localiza todas las reglas de ILM en las políticas de ILM activas que provocan que los objetos se almacenen en el depósito de Cloud Tiering.
3. Clonar cada una de estas reglas.
4. En las reglas clonadas, cambie la ubicación de ubicación a la nueva agrupación de almacenamiento en cloud.

5. Guarde las reglas clonadas.
6. Cree una nueva directiva que utilice las nuevas reglas.
7. Simular y activar la nueva directiva.

   Cuando se activa la nueva política y se realiza la evaluación de ILM, los objetos se mueven desde el bloque de S3 configurado para Cloud Tiering al bloque de S3 configurado para Cloud Storage Pool. El espacio utilizable de la cuadrícula no se ve afectado. Una vez que los objetos se mueven al Cloud Storage Pool, se eliminan del bloque de almacenamiento en niveles del cloud.

Información relacionada

"Gestión de objetos con ILM"

Archivado en cinta mediante TSM Middleware

Puede configurar un nodo de archivado para que se destine a un servidor de Tivoli Storage Manager (TSM) que proporcione una interfaz lógica para almacenar y recuperar datos de objetos en dispositivos de almacenamiento de acceso aleatorio o secuencial, incluidas bibliotecas de cintas.

El servicio ARC del nodo de archivado actúa como cliente al servidor TSM, usando Tivoli Storage Manager como middleware para comunicarse con el sistema de almacenamiento de archivado.

> La compatibilidad con los nodos de archivo está obsoleta y se eliminará en una versión futura. El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades.
>
> La opción Cloud Tiering - Simple Storage Service (S3) también queda obsoleta. Si está utilizando un nodo de archivado con esta opción, "Migre sus objetos a un pool de almacenamiento en la nube" en su lugar.
>
> Además, debe eliminar los nodos de archivado de la política de gestión de la vida útil de la información activa en StorageGRID 11,7 o versiones anteriores. La eliminación de datos de objetos almacenados en nodos de archivado simplificará las actualizaciones futuras. Consulte "Trabajar con reglas de ILM y políticas de ILM".

Clases de gestión de TSM

Las clases de gestión definidas por el middleware TSM describen cómo funcionan las operaciones de copia de seguridad y archivado de TSM's y se pueden utilizar para especificar reglas para el contenido que aplica el servidor TSM. Estas reglas funcionan de manera independiente con la política de ILM del sistema StorageGRID, y deben ser coherentes con la necesidad del sistema StorageGRID de que los objetos se almacenen de forma permanente y que siempre estén disponibles para su recuperación en el nodo de archivado. Una vez que el nodo de archivado envía los datos de objeto a un servidor TSM, se aplican las reglas de ciclo de vida y retención de TSM mientras los datos del objeto se almacenan en cinta gestionada por el servidor TSM.

El servidor TSM utiliza la clase de gestión TSM para aplicar reglas para la ubicación de los datos o la retención después de que el nodo de archivado envía los objetos al servidor TSM. Por ejemplo, los objetos identificados como backups de base de datos (contenido temporal que puede sobrescribirse con datos más nuevos) se pueden tratar de forma diferente a los datos de la aplicación (contenido fijo que debe conservarse indefinidamente).

Para que el nodo de archivado pueda comunicarse con el middleware Tivoli Storage Manager (TSM), debe configurar varios valores.

Antes de empezar

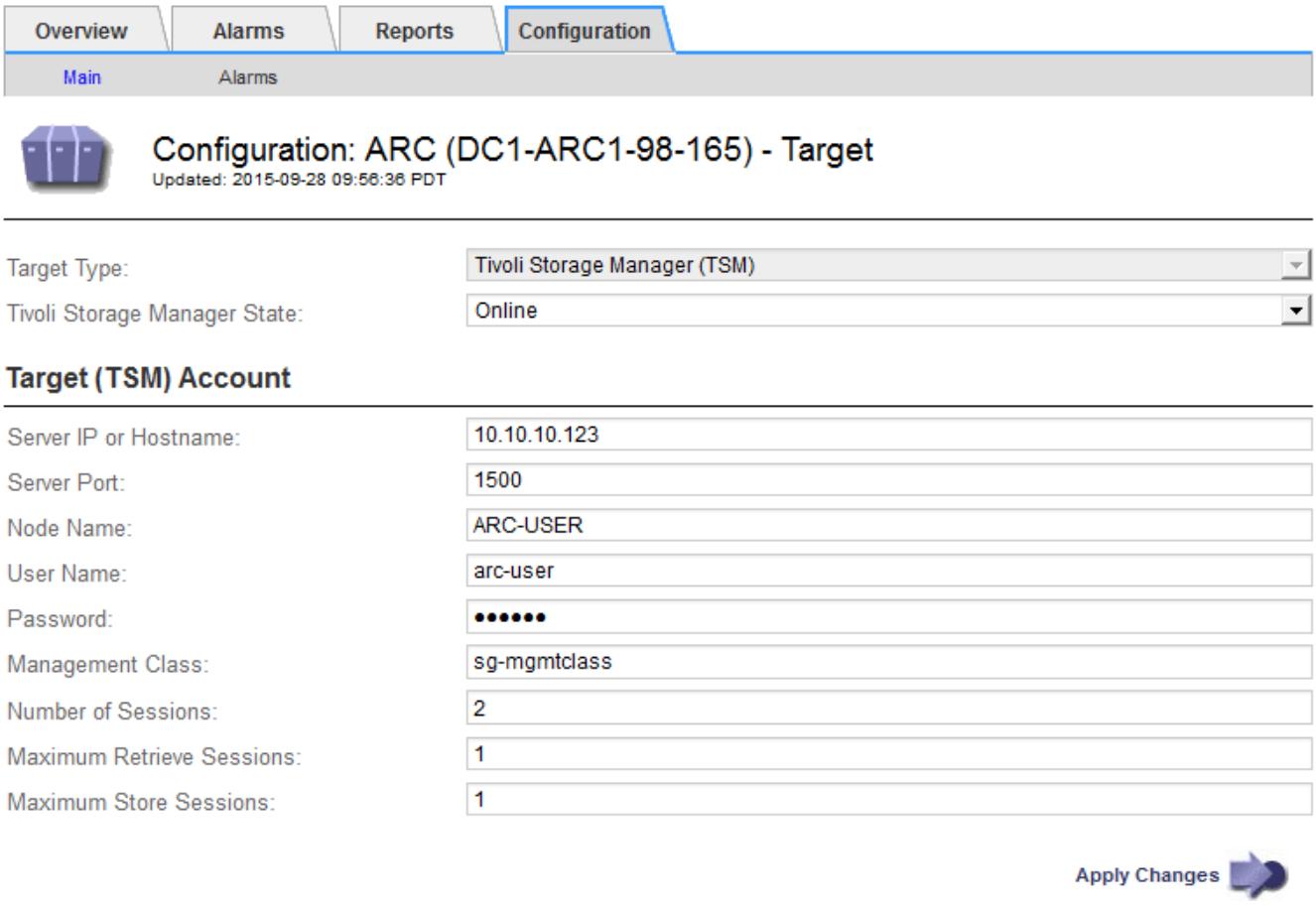
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".

Acerca de esta tarea

Hasta que se hayan configurado estos ajustes, el servicio ARC permanecerá en un estado de alarma principal, ya que no puede comunicarse con Tivoli Storage Manager.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Target**.
3. Seleccione **Configuración** > **Principal**.



4. En la lista desplegable **Tipo de destino**, seleccione **Tivoli Storage Manager (TSM)**.
5. En **Tivoli Storage Manager State**, seleccione **Offline** para evitar las recuperaciones desde el servidor de middleware TSM.

   De forma predeterminada, el estado de Tivoli Storage Manager se establece en línea, lo que significa que el nodo de archivado puede recuperar datos de objeto del servidor de middleware TSM.

6. Complete la siguiente información:

   - **IP del servidor o nombre de host**: Especifique la dirección IP o el nombre de dominio completo del servidor de middleware TSM utilizado por el servicio ARC. La dirección IP predeterminada es 127.0.0.1.
   - **Puerto del servidor**: Especifique el número de puerto en el servidor de middleware TSM al que se conectará el servicio ARC. El valor predeterminado es 1500.
   - **Nombre de nodo**: Especifique el nombre del nodo de archivado. Debe introducir el nombre (Arc-user) que ha registrado en el servidor de middleware TSM.
   - **Nombre de usuario**: Especifique el nombre de usuario que el servicio ARC utiliza para iniciar sesión en el servidor TSM. Introduzca el nombre de usuario predeterminado (Arc-user) o el usuario administrativo que ha especificado para el nodo de archivado.
   - **Contraseña**: Especifique la contraseña utilizada por el servicio ARC para iniciar sesión en el servidor TSM.
   - **Clase de administración**: Especifique la clase de administración predeterminada que se va a utilizar si no se especifica una clase de administración cuando el objeto se está guardando en el sistema StorageGRID, o la clase de administración especificada no está definida en el servidor de middleware TSM.
   - **Número de sesiones**: Especifique el número de unidades de cinta en el servidor de middleware TSM dedicadas al nodo de archivado. El nodo de archivado crea simultáneamente un máximo de una sesión por punto de montaje más un pequeño número de sesiones adicionales (menos de cinco).

     Debe cambiar este valor para que sea igual al valor establecido para MAXNUMMP (número máximo de puntos de montaje) cuando se registró o actualizó el nodo de archivado. (En el comando register, el valor predeterminado de MAXNUMMP utilizado es 1, si no se establece ningún valor.)

   También debe cambiar el valor de MAXSESSIONS para el servidor TSM a un número que sea al menos tan grande como el número de sesiones establecido para el servicio ARC. El valor predeterminado de MAXSESSIONS en el servidor TSM es 25.

   - **Sesiones de recuperación máximas**: Especifique el número máximo de sesiones que el servicio ARC puede abrir al servidor de middleware TSM para las operaciones de recuperación. En la mayoría de los casos, el valor apropiado es el número de sesiones menos el número máximo de sesiones de almacén. Si necesita compartir una unidad de cinta para su almacenamiento y recuperación, especifique un valor igual al número de sesiones.
   - **Sesiones de almacenamiento máximas**: Especifique el número máximo de sesiones simultáneas que el servicio ARC puede abrir al servidor de middleware TSM para operaciones de archivado.

     Este valor se debería establecer en uno excepto cuando el sistema de almacenamiento de archivado destino está lleno y solo se pueden llevar a cabo recuperaciones. Establezca este valor en cero para utilizar todas las sesiones para las recuperaciones.

7. Seleccione **aplicar cambios**.

Optimice un nodo de archivado para sesiones de middleware de TSM

Puede optimizar el rendimiento de un nodo de archivado que se conecta a Tivoli Server Manager (TSM) configurando las sesiones del nodo de archivado.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".

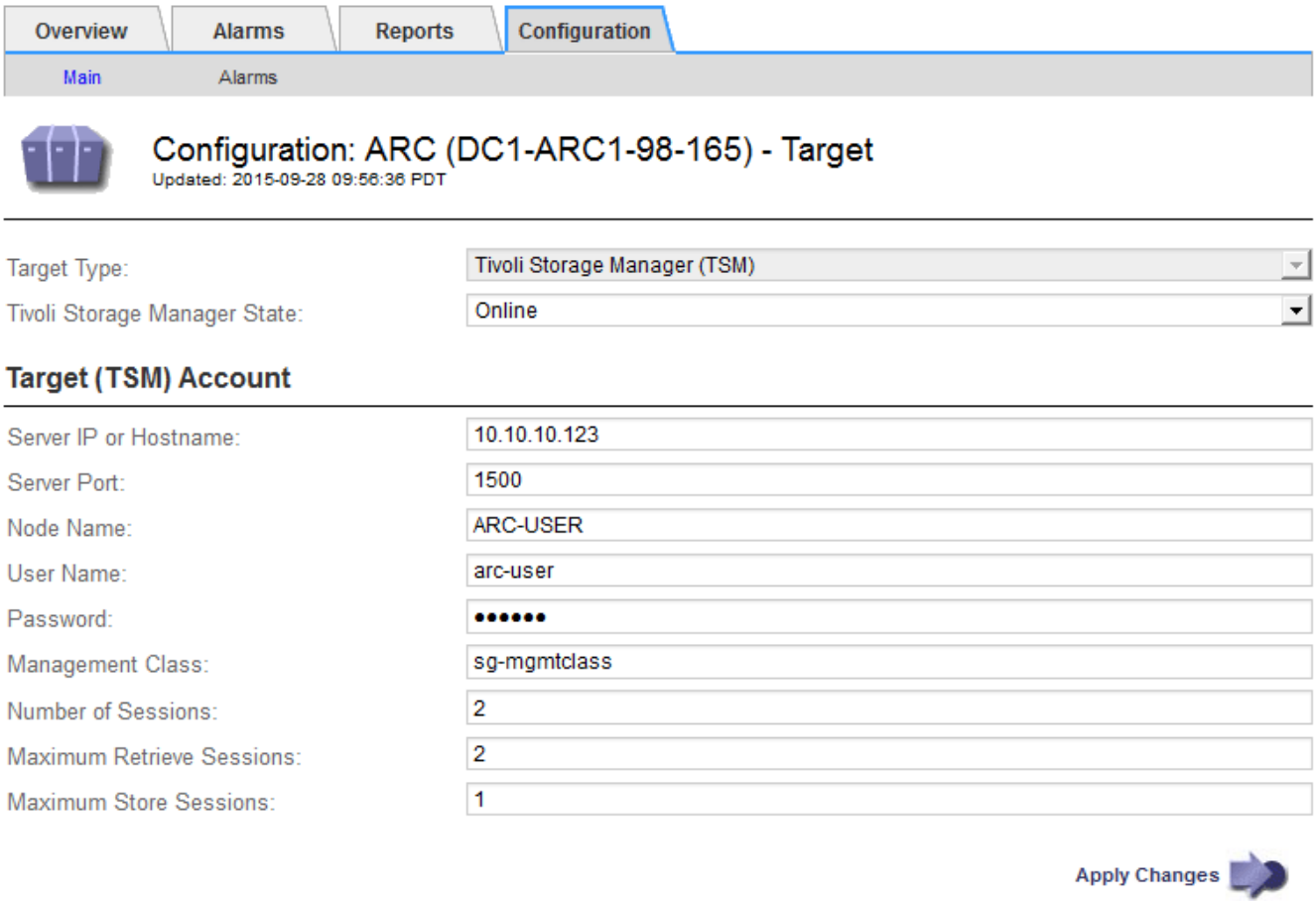
- Ya tienes "permisos de acceso específicos".

Acerca de esta tarea

Normalmente, el número de sesiones simultáneas que el nodo de archivado ha abierto al servidor de middleware TSM se establece en el número de unidades de cinta que el servidor TSM ha dedicado al nodo de archivado. Se asigna una unidad de cinta para el almacenamiento mientras el resto se asigna para la recuperación. Sin embargo, en situaciones en las que un nodo de almacenamiento se está reconstruyendo desde copias de nodo de archivado o el nodo de archivado está funcionando en modo de sólo lectura, puede optimizar el rendimiento del servidor TSM estableciendo el número máximo de sesiones de recuperación para que sea el mismo que el número de sesiones simultáneas. El resultado es que todas las unidades pueden utilizarse al mismo tiempo para la recuperación; como máximo, una de estas unidades también puede utilizarse para el almacenamiento, si corresponde.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Target**.
3. Seleccione **Configuración** > **Principal**.
4. Cambiar **máximo de sesiones de recuperación** para que sea igual que **número de sesiones**.



5. Seleccione **aplicar cambios**.

Configure el estado del archivo y los contadores para TSM

Si el nodo de archivado se conecta a un servidor de middleware TSM, puede configurar el estado del almacén de archivos de un nodo de archivado en línea o sin conexión.

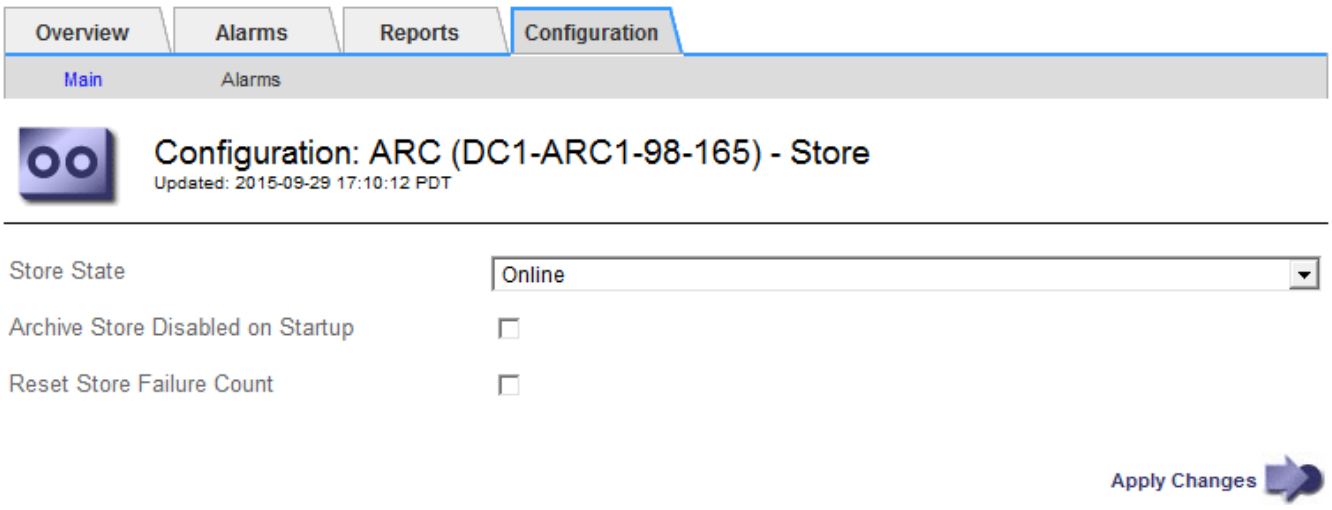
También puede desactivar el almacén de archivos cuando se inicie el nodo de archivado por primera vez o restablecer el recuento de fallos que se va a realizar el seguimiento de la alarma asociada.

Antes de empezar

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

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Store**.
3. Seleccione **Configuración** > **Principal**.



4. Modifique los siguientes ajustes, según sea necesario:
   - Estado del almacén: Establezca el estado del componente en:
     - Online: El nodo de archivado está disponible para procesar datos de objetos para el almacenamiento del sistema de almacenamiento de archivado.
     - Offline: El nodo de archivado no está disponible para procesar datos de objetos para el almacenamiento del sistema de almacenamiento de archivado.
   - Almacén de archivos desactivado al inicio: Cuando se selecciona, el componente almacén de archivos permanece en el estado de sólo lectura cuando se reinicia. Se usa para deshabilitar de forma persistente el almacenamiento en el sistema de almacenamiento de archivado dirigido. Útil cuando el sistema de almacenamiento de archivado dirigido no puede aceptar contenido.
   - Restablecer recuento de fallos de almacén: Restablezca el contador para fallos de almacén. Se puede utilizar para borrar la alarma ARVF (fallo de almacén).
5. Seleccione **aplicar cambios**.

Información relacionada

"Gestione un nodo de archivado cuando el servidor TSM alcance la capacidad"

Gestione un nodo de archivado cuando el servidor TSM alcance la capacidad

El servidor TSM no tiene forma de notificar al nodo de archivado cuando la base de

datos TSM o el almacenamiento multimedia de archivado gestionado por el servidor TSM está cerca de su capacidad. Esta situación se puede evitar gracias a la supervisión proactiva del servidor TSM.

Antes de empezar

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

Acerca de esta tarea

El nodo de archivado continúa aceptando datos de objetos para su transferencia al servidor TSM una vez que el servidor TSM deja de aceptar contenido nuevo. Este contenido no se puede escribir en medios gestionados por el servidor TSM. Si esto ocurre, se activa una alarma.

Impedir que el servicio ARC envíe contenido al servidor TSM

Para evitar que el servicio ARC envíe más contenido al servidor TSM, puede desconectar el nodo de archivado si desconecta el componente **ARC** > **Store**. Este procedimiento también puede ser útil para evitar alarmas cuando el servidor TSM no está disponible para tareas de mantenimiento.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Store**.
3. Seleccione **Configuración** > **Principal**.

4. Cambiar **Estado de tienda** a `Offline`.
5. Seleccione **almacén de archivos desactivado al inicio**.
6. Seleccione **aplicar cambios**.

Configure el nodo de archivado como de solo lectura si el middleware TSM alcanza la capacidad

Si el servidor de middleware TSM objetivo alcanza la capacidad, el nodo de archivado se puede optimizar para realizar únicamente recuperaciones.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Target**.

3. Seleccione **Configuración** > **Principal**.
4. Cambie el número máximo de sesiones de recuperación para que sea el mismo que el número de sesiones simultáneas enumeradas en el número de sesiones.
5. Cambie el número máximo de sesiones de almacenamiento a 0.

> No es necesario cambiar el número máximo de sesiones de almacén a 0 si el nodo de archivado es de sólo lectura. No se crearán sesiones de almacenamiento.

6. Seleccione **aplicar cambios**.

Configure los ajustes de recuperación del nodo de archivado

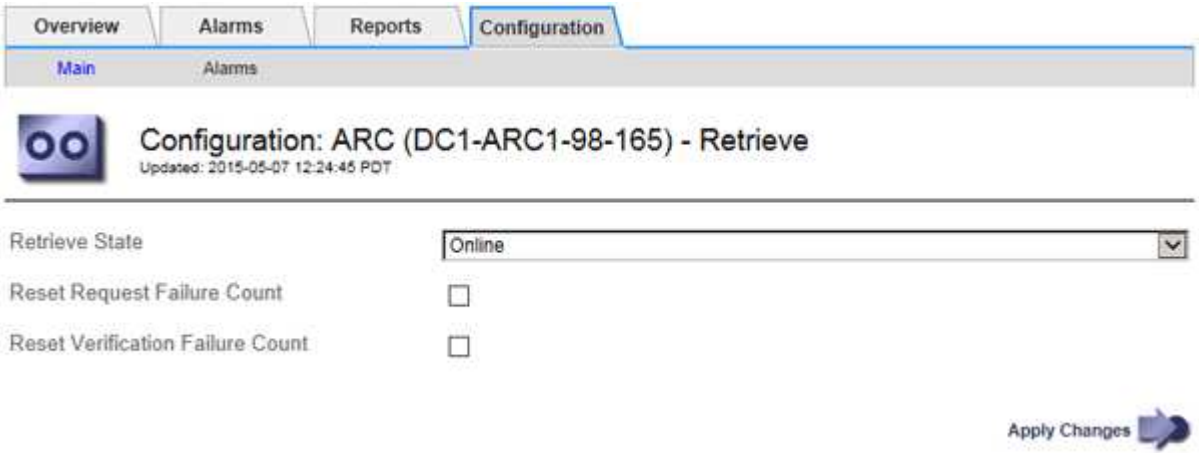
Puede configurar los ajustes de recuperación de un nodo de archivado para establecer el estado en línea o sin conexión, o restablecer los recuentos de fallos que se van a realizar el seguimiento de las alarmas asociadas.

Antes de empezar

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

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione **nodo de archivo** > **ARC** > **recuperar**.
3. Seleccione **Configuración** > **Principal**.



4. Modifique los siguientes ajustes, según sea necesario:
   - **Estado de recuperación**: Establezca el estado del componente en:
     - En línea: El nodo de cuadrícula está disponible para recuperar datos de objeto del dispositivo multimedia de archivado.
     - Offline: El nodo de grid no está disponible para recuperar los datos del objeto.
   - Restablecer Recuento de Fallos de Solicitud: Seleccione la casilla de control para restablecer el contador de fallos de solicitud. Esto se puede utilizar para borrar la alarma ARRF (fallos de solicitud).
   - Restablecer recuento de fallos de verificación: Seleccione la casilla de verificación para restablecer el contador de fallos de verificación en los datos de objetos recuperados. Esto se puede utilizar para

borrar la alarma ARRV (fallos de verificación).

5. Seleccione **aplicar cambios**.

Configure la replicación del nodo de archivado

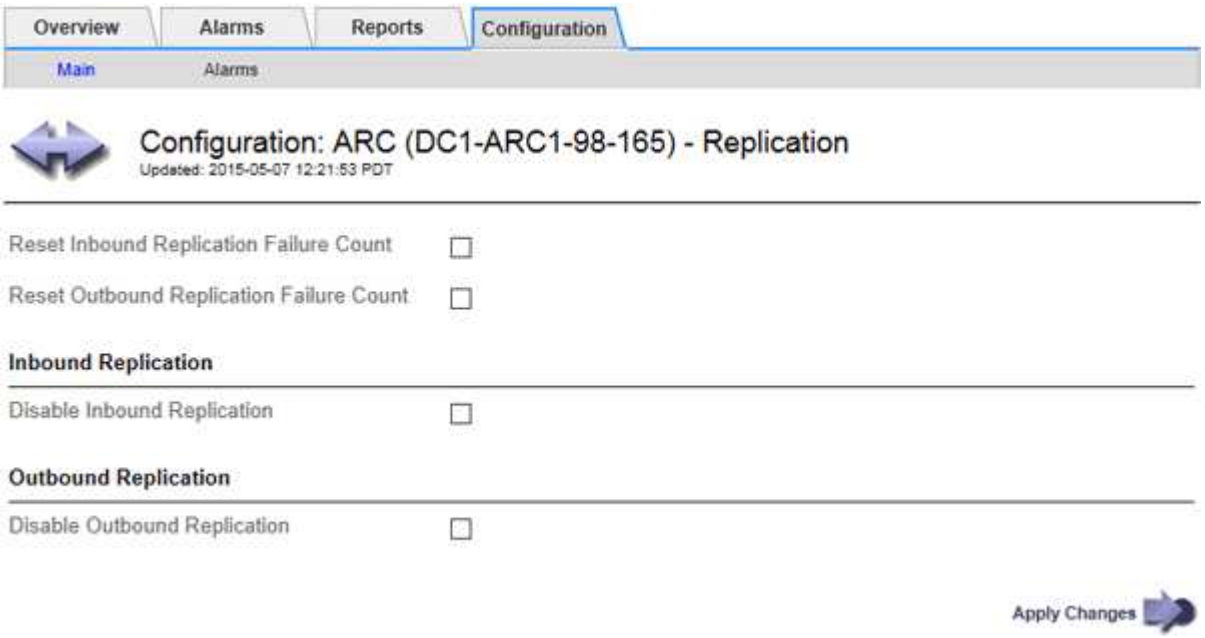
Puede configurar la configuración de replicación para un nodo de archivado y desactivar la replicación entrante y saliente, o restablecer los recuentos de fallos que se van a realizar el seguimiento de las alarmas asociadas.

Antes de empezar

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

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC** > **Replication**.
3. Seleccione **Configuración** > **Principal**.



4. Modifique los siguientes ajustes, según sea necesario:
   - **Restablecer recuento de fallos de replicación entrante**: Seleccione para restablecer el contador en caso de fallos de replicación entrante. Esto se puede utilizar para borrar la alarma RIRF (replicaciones entrantes — fallidas).
   - **Reset Outbound Replication Failure Count**: Seleccione para restablecer el contador de fallos de replicación saliente. Esto se puede utilizar para borrar la alarma RORF (réplicas de salida — fallida).
   - **Desactivar replicación entrante**: Seleccione esta opción para desactivar la replicación entrante como parte de un procedimiento de mantenimiento o prueba. Dejar borrado durante el funcionamiento normal.

     Cuando la replicación entrante está desactivada, los datos de objeto se pueden recuperar del servicio ARC para la replicación en otras ubicaciones del sistema StorageGRID, pero los objetos no se pueden replicar en este servicio ARC desde otras ubicaciones del sistema. El servicio ARC es de sólo lectura-.

- **Deshabilitar la replicación saliente**: Seleccione la casilla de verificación para desactivar la replicación saliente (incluidas las solicitudes de contenido para recuperaciones HTTP) como parte de un procedimiento de mantenimiento o prueba. Deje sin marcar durante el funcionamiento normal.

  Cuando la replicación saliente está desactivada, los datos de objeto se pueden copiar en este servicio ARC para cumplir con las reglas de ILM, pero los datos de objeto no se pueden recuperar del servicio ARC para copiarlos en otras ubicaciones del sistema StorageGRID. El servicio ARC es de sólo escritura-.

5. Seleccione **aplicar cambios**.

Establezca alarmas personalizadas para el nodo de archivado

Debe establecer alarmas personalizadas para los atributos ARQL y ARRL que se utilizan para supervisar la velocidad y la eficacia de la recuperación de datos de objetos del sistema de almacenamiento de archivado por parte del nodo de archivado.

- ARQL: Longitud media de la cola. El tiempo medio, en microsegundos, que los datos de objetos se encuentran en cola para la recuperación del sistema de almacenamiento de archivado.
- ARRL: Promedio de latencia de solicitud. El tiempo medio, en microsegundos, que necesita el nodo de archivado para recuperar los datos de objetos del sistema de almacenamiento de archivado.

Los valores aceptables para estos atributos dependen de la configuración y el uso del sistema de almacenamiento de ficheros. (Vaya a **ARC** > **Retrieve** > **Overview** > **Main**.) Los valores establecidos para los tiempos de espera de las solicitudes y el número de sesiones disponibles para las solicitudes de recuperación tienen una influencia especial.

Una vez finalizada la integración, supervise las recuperaciones de datos de objetos del nodo de archivado para establecer valores para los tiempos de recuperación y las longitudes de cola normales. A continuación, cree alarmas personalizadas para ARQL y ARRL que se activarán si surge una condición de funcionamiento anormal. Consulte las instrucciones para "gestión de alarmas (sistema heredado)".

Integrar Tivoli Storage Manager

Configuración y funcionamiento del nodo de archivado

Su sistema StorageGRID gestiona el nodo de archivado como una ubicación en la que los objetos se almacenan de forma indefinida y siempre son accesibles.

Cuando se procesa un objeto, se realizan copias en todas las ubicaciones necesarias, incluidos los nodos de archivado, según las reglas de gestión del ciclo de vida de la información (ILM) definidas en el sistema StorageGRID. El nodo de archivado actúa como cliente de un servidor TSM y las bibliotecas del cliente TSM se instalan en el nodo de archivado mediante el proceso de instalación del software StorageGRID. Los datos de objeto dirigidos al nodo de archivado para el almacenamiento se guardan directamente en el servidor TSM a medida que se reciben. El nodo de archivado no guarda los datos de objetos antes de guardarlos en el servidor TSM ni realiza la agregación de objetos. Sin embargo, el nodo de archivado puede enviar varias copias al servidor TSM en una única transacción cuando las tasas de datos lo garantizan.

Una vez que el nodo de archivado guarda los datos de objeto en el servidor TSM, el servidor TSM administra los datos de objeto con sus políticas de ciclo de vida/retención. Estas políticas de retención deben definirse para que sean compatibles con la operación del nodo de archivado. Es decir, los datos de objeto guardados por el nodo de archivado deben almacenarse indefinidamente y siempre deben ser accesibles desde el nodo de archivado, a menos que el nodo de archivado los elimine.

No hay conexión entre las reglas de ILM del sistema StorageGRID y las políticas de retención/ciclo de vida del servidor TSM. Cada uno de ellos funciona de forma independiente; sin embargo, a medida que se ingiere cada objeto en el sistema StorageGRID, puede asignarle una clase de gestión de TSM. Esta clase de gestión se pasa al servidor TSM junto con los datos de objetos. La asignación de diferentes clases de gestión a diferentes tipos de objetos permite configurar el servidor TSM para colocar los datos de objetos en distintos pools de almacenamiento o aplicar distintas políticas de migración o retención según sea necesario. Por ejemplo, los objetos identificados como backups de base de datos (contenido temporal que puede sobrescribirse con datos más nuevos) pueden tratarse de forma diferente a los datos de la aplicación (contenido fijo que debe conservarse indefinidamente).

El nodo de archivado se puede integrar con un servidor TSM nuevo o existente; no requiere un servidor TSM dedicado. Los servidores TSM se pueden compartir con otros clientes, siempre que el tamaño del servidor TSM se ajusta de forma adecuada a la carga máxima esperada. TSM debe instalarse en un servidor o máquina virtual independiente del nodo de archivado.

Es posible configurar más de un nodo de archivado para escribir en el mismo servidor TSM; sin embargo, esta configuración sólo se recomienda si los nodos de archivado escriben diferentes conjuntos de datos en el servidor TSM. No se recomienda configurar más de un nodo de archivado para escribir en el mismo servidor TSM cuando cada nodo de archivado escribe copias de los mismos datos de objeto en el archivo. En este último caso, ambas copias están sujetas a un único punto de error (el servidor TSM) para las copias redundantes de datos de objetos.

Los nodos de archivado no utilizan el componente de gestión de almacenamiento jerárquico (HSM) de TSM.

Prácticas recomendadas de configuración

Cuando esté dimensionando y configurando su servidor TSM, debería aplicar las prácticas recomendadas para optimizar su funcionamiento con el nodo de archivado.

Al cambiar el tamaño y configurar el servidor TSM, debe tener en cuenta los siguientes factores:

- Como el nodo de archivado no agrega objetos antes de guardarlos en el servidor TSM, se debe ajustar el tamaño de la base de datos TSM para que contenga referencias a todos los objetos que se escribirán en el nodo de archivado.
- El software Archive Node no puede tolerar la latencia involucrada en la escritura de objetos directamente en cinta u otros medios extraíbles. Por lo tanto, el servidor TSM debe configurarse con un pool de almacenamiento en disco para el almacenamiento inicial de datos guardados por el nodo de archivado siempre que se utilice un medio extraíble.
- Debe configurar las políticas de retención de TSM para utilizar la retención basada en eventos-. El nodo de archivado no admite las políticas de retención de TSM basadas en la creación. Utilice los siguientes valores recomendados de retmin=0 y retver=0 en la directiva de retención (que indica que la retención comienza cuando el nodo de archivado activa un evento de retención y se conserva durante 0 días después de ese). Sin embargo, estos valores para retmin y retver son opcionales.

El pool de discos debe estar configurado para migrar datos al pool de cintas (es decir, el pool de cintas debe ser NXTSTGPOOL del pool de discos). El pool de cintas no debe configurarse como un pool de copias del pool de discos con escritura simultánea en ambos pools (es decir, el pool de cintas no puede ser un COPYSTGPOOL para el pool de discos). Para crear copias sin conexión de las cintas que contienen datos del nodo de archivado, configure el servidor TSM con un segundo grupo de cintas que sea un grupo de copias del grupo de cintas utilizado para los datos del nodo de archivado.

Complete la configuración del nodo de archivado

El nodo de archivado no funciona después de completar el proceso de instalación. Antes de que el sistema StorageGRID pueda guardar objetos en el nodo de archivado de TSM, debe completar la instalación y configuración del servidor TSM y configurar el nodo de archivado para que se comunique con el servidor TSM.

Consulte la siguiente documentación de IBM, según sea necesario, cuando prepare el servidor TSM para la integración con el nodo de archivado en un sistema StorageGRID:

- "Guía del usuario e instalación de los controladores de dispositivos de cinta de IBM"
- "Referencia de programación de controladores de dispositivo de cinta IBM"

Instale un nuevo servidor TSM

Puede integrar el nodo de archivado con un servidor TSM nuevo o existente. Si va a instalar un nuevo servidor TSM, siga las instrucciones de la documentación de TSM para completar la instalación.

Un nodo de archivado no se puede alojar conjuntamente con un servidor TSM.

Configure el servidor TSM

Esta sección incluye instrucciones de ejemplo para preparar un servidor TSM siguiendo las mejores prácticas de TSM.

Las siguientes instrucciones le guían en el proceso de:

- Definición de un pool de almacenamiento en disco y un pool de almacenamiento en cinta (si es necesario) en el servidor TSM
- Definición de una directiva de dominio que utiliza la clase de administración TSM para los datos guardados desde el nodo de archivado y registro de un nodo para utilizar esta directiva de dominio

Estas instrucciones se proporcionan solo para su guía; no están destinadas a reemplazar la documentación de TSM, ni para proporcionar instrucciones completas y adecuadas para todas las configuraciones. Un administrador de TSM debe proporcionar instrucciones específicas para la implementación que esté familiarizado con sus requisitos detallados y con el conjunto completo de documentación de TSM Server.

Definir los pools de almacenamiento en disco y cinta de TSM

El nodo de archivado escribe en un pool de almacenamiento en disco. Para archivar el contenido en cinta, debe configurar el grupo de almacenamiento en disco para mover el contenido a un grupo de almacenamiento en cinta.

Acerca de esta tarea

Para un servidor TSM, debe definir un pool de almacenamiento en cinta y un pool de almacenamiento en disco en Tivoli Storage Manager. Después de definir el pool de discos, cree un volumen de discos y asígnelo al pool de discos. -pool de cintas no es necesario si el servidor TSM utiliza únicamente el almacenamiento en disco.

Debe realizar varios pasos en el servidor TSM antes de poder crear un grupo de almacenamiento de cinta.

(Cree una biblioteca de cintas y al menos una unidad en la biblioteca de cintas. Defina una ruta de acceso desde el servidor a la biblioteca y desde el servidor a las unidades y, a continuación, defina una clase de dispositivo para las unidades.) Los detalles de estos pasos pueden variar en función de la configuración de hardware y los requisitos de almacenamiento del sitio. Para obtener más información, consulte la documentación de TSM.

El siguiente conjunto de instrucciones ilustra el proceso. Debe tener en cuenta que los requisitos de su sitio pueden variar en función de los requisitos de la implementación. Para obtener detalles de configuración e instrucciones, consulte la documentación de TSM.

Debe iniciar sesión en el servidor con privilegios administrativos y utilizar la herramienta dsmadmc para ejecutar los siguientes comandos.

Pasos

1. Cree una biblioteca de cintas.

   `define library` *`tapelibrary`* `libtype=`*`scsi`*

   Donde *`tapelibrary`* es un nombre arbitrario elegido para la biblioteca de cintas y el valor de `libtype` pueden variar en función del tipo de biblioteca de cintas.

2. Defina una ruta de acceso desde el servidor a la biblioteca de cintas.

   `define path` *`servername`* *`tapelibrary`* `srctype=server desttype=library device=`*`lib-devicename`*

   - *`servername`* Es el nombre del servidor TSM
   - *`tapelibrary`* es el nombre de la biblioteca de cintas que ha definido
   - *`lib-devicename`* es el nombre del dispositivo de la biblioteca de cintas

3. Defina una unidad para la biblioteca.

   `define drive` *`tapelibrary drivename`*

   - *`drivename`* es el nombre que desea especificar para la unidad
   - *`tapelibrary`* es el nombre de la biblioteca de cintas que ha definido

     Se recomienda configurar una unidad o unidades adicionales, según la configuración de hardware. (Por ejemplo, si el servidor TSM está conectado a un switch Fibre Channel que tiene dos entradas de una biblioteca de cintas, quizás desee definir una unidad para cada entrada).

4. Defina una ruta desde el servidor hasta la unidad definida.

   `define path` *`servername`* `drivename srctype=server desttype=drive library=`*`tapelibrary`* `device=`*`drive-dname`*

   - *`drive-dname`* es el nombre del dispositivo de la unidad
   - *`tapelibrary`* es el nombre de la biblioteca de cintas que ha definido

     Repita el procedimiento para cada unidad que haya definido para la biblioteca de cintas, utilizando una unidad aparte *`drivename`* y.. *`drive-dname`* para cada unidad.

5. Defina una clase de dispositivo para las unidades.

   ```
   define devclass DeviceClassName devtype=lto library=tapelibrary
   format=tapetype
   ```

   - *DeviceClassName* es el nombre de la clase de dispositivo
   - *lto* es el tipo de unidad conectada al servidor
   - *tapelibrary* es el nombre de la biblioteca de cintas que ha definido
   - *tapetype* es el tipo de cinta; por ejemplo, triunter3
6. Agregue volúmenes de cinta al inventario de la biblioteca.

   ```
   checkin libvolume tapelibrary
   ```

   tapelibrary es el nombre de la biblioteca de cintas que ha definido.
7. Cree la agrupación de almacenamiento de cinta principal.

   ```
   define stgpool SGWSTapePool DeviceClassName description=description
   collocate=filespace maxscratch=XX
   ```

   - *SGWSTapePool* Es el nombre del pool de almacenamiento de cinta del nodo de archivado. Puede seleccionar cualquier nombre para la agrupación de almacenamiento de cinta (siempre que el nombre utilice las convenciones de sintaxis esperadas por el servidor TSM).
   - *DeviceClassName* es el nombre de la clase de dispositivo para la biblioteca de cintas.
   - *description* Es una descripción del grupo de almacenamiento que se puede mostrar en el servidor TSM mediante `query stgpool` comando. Por ejemplo, «pool de almacenamiento en cinta para el nodo de archivado».
   - *collocate=filespace* Especifica que el servidor TSM debe escribir objetos del mismo espacio en una única cinta.
   - `XX` es uno de los siguientes:
     - El número de cintas vacías de la biblioteca de cintas (en el caso de que el nodo de archivado sea la única aplicación que utiliza la biblioteca).
     - El número de cintas asignadas para su uso por el sistema StorageGRID (en aquellos casos en los que se comparte la biblioteca de cintas).
8. En un servidor TSM, cree un pool de almacenamiento en disco. En la consola administrativa del servidor TSM, introduzca

   ```
   define stgpool SGWSDiskPool disk description=description
   maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
   lowmig=percent_low
   ```

   - *SGWSDiskPool* Es el nombre del pool de discos del nodo de archivado. Es posible seleccionar cualquier nombre para el pool de almacenamiento de discos (siempre que el nombre utilice las convenciones de sintaxis que espera el TSM).
   - *description* Es una descripción del grupo de almacenamiento que se puede mostrar en el servidor TSM mediante `query stgpool` comando. Por ejemplo, «Pool de almacenamiento en disco para el nodo de archivado».

- *maximum_file_size* fuerza a que los objetos de mayor tamaño se escriban directamente en la cinta, en lugar de en la caché del pool de discos. Se recomienda establecer *maximum_file_size* A 10 GB.
- *nextstgpool=SGWSTapePool* Hace referencia al pool de almacenamiento de disco al pool de almacenamiento de cinta definido para el nodo de archivado.
- *percent_high* establece el valor en el que el pool de discos comienza a migrar su contenido al grupo de cintas. Se recomienda establecer *percent_high* 0 para que la migración de datos comience inmediatamente
- *percent_low* establece el valor en el que se detiene la migración al pool de cintas. Se recomienda establecer *percent_low* 0 para borrar el pool de discos.

9. En un servidor TSM, cree un volumen de disco (o volúmenes) y asígnelo al pool de discos.

   `define volume SGWSDiskPool volume_name formatsize=size`

   - *SGWSDiskPool* es el nombre del pool de discos.
   - *volume_name* es la ruta completa a la ubicación del volumen (por ejemplo, `/var/local/arc/stage6.dsm`) En el servidor TSM en el que escribe el contenido del pool de discos como preparación para la transferencia a cinta.
   - *size* Es el tamaño, en MB, del volumen de disco.

     Por ejemplo, para crear un único volumen de disco de forma que el contenido de un pool de discos llene una única cinta, configure el valor del tamaño en 200000 cuando el volumen de cinta tenga una capacidad de 200 GB.

     Sin embargo, es posible que sea conveniente crear varios volúmenes de disco de un tamaño menor, ya que el servidor TSM puede escribir en cada volumen del pool de discos. Por ejemplo, si el tamaño de la cinta es 250 GB, cree 25 volúmenes de disco con un tamaño de 10 GB (10000) cada uno.

   El servidor TSM preasigna espacio en el directorio para el volumen de disco. Esto puede tardar algún tiempo en completarse (más de tres horas para un volumen de disco de 200 GB).

Defina una directiva de dominio y registre un nodo

Debe definir una directiva de dominio que utilice la clase de administración TSM para los datos guardados desde el nodo de archivado y, a continuación, registrar un nodo para utilizar esta directiva de dominio.

> Los procesos de nodo de archivado pueden perder memoria si caduca la contraseña de cliente para el nodo de archivado en Tivoli Storage Manager (TSM). Asegúrese de que el servidor TSM esté configurado para que el nombre de usuario/contraseña del cliente para el nodo de archivado no caduque nunca.

Al registrar un nodo en el servidor TSM para el uso del nodo de archivado (o actualizar un nodo existente), debe especificar el número de puntos de montaje que el nodo puede utilizar para las operaciones de escritura especificando el parámetro MAXNUMMP en el comando REGISTER NODE. La cantidad de puntos de montaje suele ser equivalente al número de cabezales de unidad de cinta asignados al nodo de archivado. El número especificado para MAXNUMMP en el servidor TSM debe ser al menos tan grande como el valor establecido para **ARC** > **Target** > **Configuration** > **Main** > **Maximum Store Sessions** para el nodo de archivado, Que se define en un valor de 0 o 1, ya que las sesiones de almacén simultáneas no son

compatibles con el nodo de archivado.

El valor de MAXSESSIONS establecido para el servidor TSM controla el número máximo de sesiones que todas las aplicaciones cliente pueden abrir al servidor TSM. El valor de MAXSESSIONS especificado en el TSM debe ser al menos tan grande como el valor especificado para **ARC** > **Target** > **Configuration** > **Main** > **Number of Sessions** en el Grid Manager para el nodo de archivado. El nodo de archivado crea simultáneamente al menos una sesión por punto de montaje más un pequeño número (< 5) de sesiones adicionales.

El nodo TSM asignado al nodo de archivado utiliza una directiva de dominio personalizada `tsm-domain`. La `tsm-domain` La política de dominio es una versión modificada de la política de dominio «estándar», configurada para escribir en cinta y con el destino de archivado establecido para ser el pool de almacenamiento del sistema StorageGRID (*`SGWSDiskPool`*).

> Debe iniciar sesión en el servidor TSM con privilegios administrativos y utilizar la herramienta dsmadmc para crear y activar la directiva de dominio.

Crear y activar la directiva de dominio

Debe crear una directiva de dominio y, a continuación, activarla para configurar el servidor TSM a fin de guardar los datos enviados desde el nodo de archivado.

Pasos

1. Crear una política de dominio.

   ```
   copy domain standard tsm-domain
   ```

2. Si no utiliza una clase de gestión existente, introduzca una de las siguientes opciones:

   ```
   define policyset tsm-domain standard
   ```

   ```
   define mgmtclass tsm-domain standard default
   ```

   `default` es la clase de administración predeterminada para la implementación.

3. Cree un copygroup en el pool de almacenamiento apropiado. Introducir (en una línea):

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

   `default` Es la clase de administración predeterminada para el nodo de archivado. Los valores de `retinit`, `retmin`, y. `retver` Se han elegido para reflejar el comportamiento de retención utilizado actualmente por el nodo de archivado

   > No configurar `retinit` para `retinit=create`. Ajuste `retinit=create` Bloquea el nodo de archivado para que no elimine contenido, ya que los eventos de retención se utilizan para eliminar contenido del servidor TSM.

4. Asigne la clase de administración para que sea la predeterminada.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Establezca el nuevo conjunto de directivas como activo.

   ```
   activate policyset tsm-domain standard
   ```

   Ignore la advertencia que aparece cuando introduce el comando activate.

6. Registre un nodo para utilizar el nuevo conjunto de directivas en el servidor TSM. En el servidor TSM, introduzca (en una línea):

   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```

   Arc-user y Arc-password son el mismo nombre de nodo de cliente y contraseña que se define en Archive Node, y el valor de MAXNUMMP se establece en el número de unidades de cinta reservadas para las sesiones de almacén de nodo de archivado.

   > De forma predeterminada, al registrar un nodo se crea un ID de usuario administrativo con la autoridad del propietario del cliente, con la contraseña definida para el nodo.

Migrar datos a StorageGRID

Puede migrar grandes cantidades de datos al sistema StorageGRID a la vez que utiliza el sistema StorageGRID para realizar operaciones diarias.

Utilice esta guía cuando planifique una migración de grandes cantidades de datos al sistema StorageGRID. No es una guía general sobre la migración de datos y no incluye pasos detallados para realizar una migración. Siga las directrices y las instrucciones de esta sección para asegurarse de que la migración de datos al sistema StorageGRID se realice de forma eficiente sin interferir en las operaciones del día a día y de que el sistema StorageGRID gestione los datos migrados de forma adecuada.

Confirmar la capacidad del sistema StorageGRID

Antes de migrar grandes cantidades de datos al sistema StorageGRID, confirme que el sistema StorageGRID tiene la capacidad de disco necesaria para gestionar el volumen previsto.

Si el sistema StorageGRID incluye un nodo de archivado y se ha guardado una copia de los objetos migrados en un almacenamiento near-line (como la cinta), asegúrese de que el almacenamiento del nodo de archivado tenga suficiente capacidad para el volumen previsto de datos migrados.

Como parte de la evaluación de la capacidad, observe el perfil de datos de los objetos que tiene pensado migrar y calcule la cantidad de capacidad de disco necesaria. Para obtener información detallada sobre cómo supervisar la capacidad del disco del sistema StorageGRID, consulte "Gestione nodos de almacenamiento" y las instrucciones para "Supervisión de StorageGRID".

Determine la política de ILM para los datos migrados

La política de ILM del sistema StorageGRID determina cuántas copias se realizan, las ubicaciones a las que se almacenan las copias y durante el tiempo que se conservan estas copias. Una política de ILM consta de un conjunto de reglas de ILM que describen cómo filtrar objetos y gestionar datos de objetos a lo largo del tiempo.

En función del uso que se haga de los datos migrados y de los requisitos relativos a los datos migrados, es posible que desee definir reglas de ILM únicas para los datos migrados que difieren de las reglas de ILM que

se usan para las operaciones cotidianas. Por ejemplo, si hay requisitos normativos diferentes para la gestión diaria de los datos que para los datos que se incluyen en la migración, es posible que desee usar un número distinto de copias de los datos migrados en un grado de almacenamiento diferente.

Puede configurar reglas que se apliquen exclusivamente a los datos migrados si es posible distinguir de forma única entre los datos migrados y los datos de objetos guardados de las operaciones diarias.

Si puede distinguir de forma fiable entre los tipos de datos mediante uno de los criterios de metadatos, puede usar estos criterios para definir una regla de ILM que solo se aplica a los datos migrados.

Antes de iniciar la migración de datos, asegúrese de comprender la política de gestión del ciclo de vida de la información del sistema StorageGRID y cómo se aplicará a los datos migrados, y de haber realizado y probado cualquier cambio en la política de ILM. Consulte "Gestión de objetos con ILM".

> Una política de ILM que se haya especificado incorrectamente puede provocar una pérdida de datos irrecuperable. Revise detenidamente todos los cambios realizados en una política de ILM antes de activarla para asegurarse de que la política funcione como se desee.

Evaluar el impacto de la migración en las operaciones

Un sistema StorageGRID está diseñado para proporcionar un funcionamiento eficiente para el almacenamiento y la recuperación de objetos, y proporcionar una protección excelente frente a la pérdida de datos mediante la creación sin problemas de copias redundantes de datos de objetos y metadatos.

Sin embargo, la migración de datos debe gestionarse cuidadosamente de acuerdo con las instrucciones de esta guía para evitar repercutir en las operaciones diarias del sistema o, en casos extremos, colocando los datos en riesgo de pérdida en caso de fallo en el sistema StorageGRID.

Migración de grandes cantidades de datos coloca una carga adicional en el sistema. Cuando el sistema StorageGRID está cargado en gran medida, responde más lentamente a las solicitudes de almacenamiento y recuperación de objetos. Esto puede interferir con las solicitudes de almacenamiento y recuperación que son integrales a las operaciones diarias. La migración también puede ocasionar otros problemas operativos. Por ejemplo, cuando un nodo de almacenamiento se está agotando la capacidad, la carga intermitente pesada debido a la ingesta en lote puede provocar que el nodo de almacenamiento se cicle entre las notificaciones de solo lectura y de lectura y escritura.

Si la carga pesada persiste, se pueden desarrollar colas para diversas operaciones que el sistema StorageGRID debe realizar para garantizar la redundancia total de los datos de objetos y los metadatos.

La migración de datos debe gestionarse con cuidado según las directrices que se indican en este documento para garantizar el funcionamiento seguro y eficiente del sistema StorageGRID durante la migración. Al migrar datos, procese objetos en lotes o acelerador continuamente del procesamiento. A continuación, supervise continuamente el sistema StorageGRID para asegurarse de que no se excedan los distintos valores de atributos.

Programe y supervise la migración de datos

La migración de datos debe programarse y supervisarse según sea necesario para garantizar que los datos se coloquen según la política de ILM en el plazo estipulado.

Programar la migración de datos

Evite migrar datos durante las horas operativas del núcleo. Limite la migración de datos a noches, fines de semana y otras veces cuando el uso del sistema sea bajo.

Si es posible, no programe la migración de datos durante períodos de actividad alta. Sin embargo, si no es práctico evitar completamente el período de alta actividad, es seguro continuar siempre que usted supervise de cerca los atributos relevantes y tome medidas si exceden los valores aceptables.

Supervisar la migración de datos

En esta tabla, se enumeran los atributos que debe supervisar durante la migración de datos y los problemas que representan.

Si utiliza directivas de clasificación de tráfico con límites de tasa para acelerar el procesamiento, puede supervisar la tasa observada junto con las estadísticas descritas en la siguiente tabla y reducir los límites si es necesario.

Supervisar	Descripción
Número de objetos que están a la espera de la evaluación de ILM	1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. 2. Seleccione ***deployment*** > **Descripción general** > **Principal**. 3. En la sección ILM Activity, supervise el número de objetos que se muestran para los siguientes atributos: ◦ **Esperando - todos (XQUZ)**: El número total de objetos que esperan la evaluación de ILM. ◦ **Esperando - Cliente (XCQZ)**: El número total de objetos que esperan la evaluación de ILM de las operaciones cliente (por ejemplo, ingesta). 4. Si el número de objetos mostrado para cualquiera de estos atributos supera 100,000, acelere la tasa de procesamiento de objetos para reducir la carga en el sistema StorageGRID.
Capacidad de almacenamiento específica del sistema de archivado	Si la normativa de gestión del ciclo de vida de la información guarda una copia de los datos migrados a un sistema de almacenamiento de archivado dirigido (cinta o cloud), supervise la capacidad del sistema de almacenamiento de archivado dirigido para garantizar que los datos migrados disponen de capacidad suficiente.
Nodo de archivo > **ARC** > **Tienda**	Si se activa una alarma para el atributo **fallos de almacenamiento (ARVF)**, es posible que el sistema de almacenamiento de archivado dirigido haya alcanzado la capacidad. Compruebe el sistema de almacenamiento de archivos de destino y resuelva cualquier problema que haya activado una alarma.

Gestión de objetos con ILM

Gestión de objetos con ILM

Las reglas de gestión de la vida útil de la información (ILM) en una política de ILM indican a StorageGRID cómo crear y distribuir copias de datos de objetos y cómo gestionar esas copias con el tiempo.

Acerca de estas instrucciones

Diseñar e implementar reglas y políticas de ILM requiere una planificación cuidadosa. Debe comprender los requisitos operativos, la topología del sistema StorageGRID, las necesidades de protección de objetos y los tipos de almacenamiento disponibles. A continuación, debe determinar cómo desea copiar, distribuir y almacenar diferentes tipos de objetos.

Utilice estas instrucciones para:

- Conozca más detalles sobre gestión de la vida útil de la información de StorageGRID "Funcionamiento de ILM a lo largo de la vida de un objeto".
- Aprenda a configurar "pools de almacenamiento", "Pools de almacenamiento en cloud", y. "Reglas de ILM".
- Aprenda cómo "Cree, simule y active una política de ILM" que protegerá los datos de objetos en uno o más sitios.
- Aprenda cómo "Gestionar objetos con S3 Object Lock", Que ayuda a garantizar que los objetos en cubos específicos de S3 no se borren o sobrescriban durante un período de tiempo específico.

Leer más

Para obtener más información, consulte estos vídeos:

- "Vídeo: Reglas de gestión del ciclo de vida de la información en StorageGRID 11,8".

- "Vídeo: Políticas de gestión del ciclo de vida de la información en StorageGRID 11,8"

ILM y ciclo de vida de los objetos

Cómo funciona ILM a lo largo de la vida de un objeto

Comprender cómo utiliza StorageGRID ILM para gestionar objetos durante cada fase de su vida útil puede ayudarle a diseñar una política más eficaz.

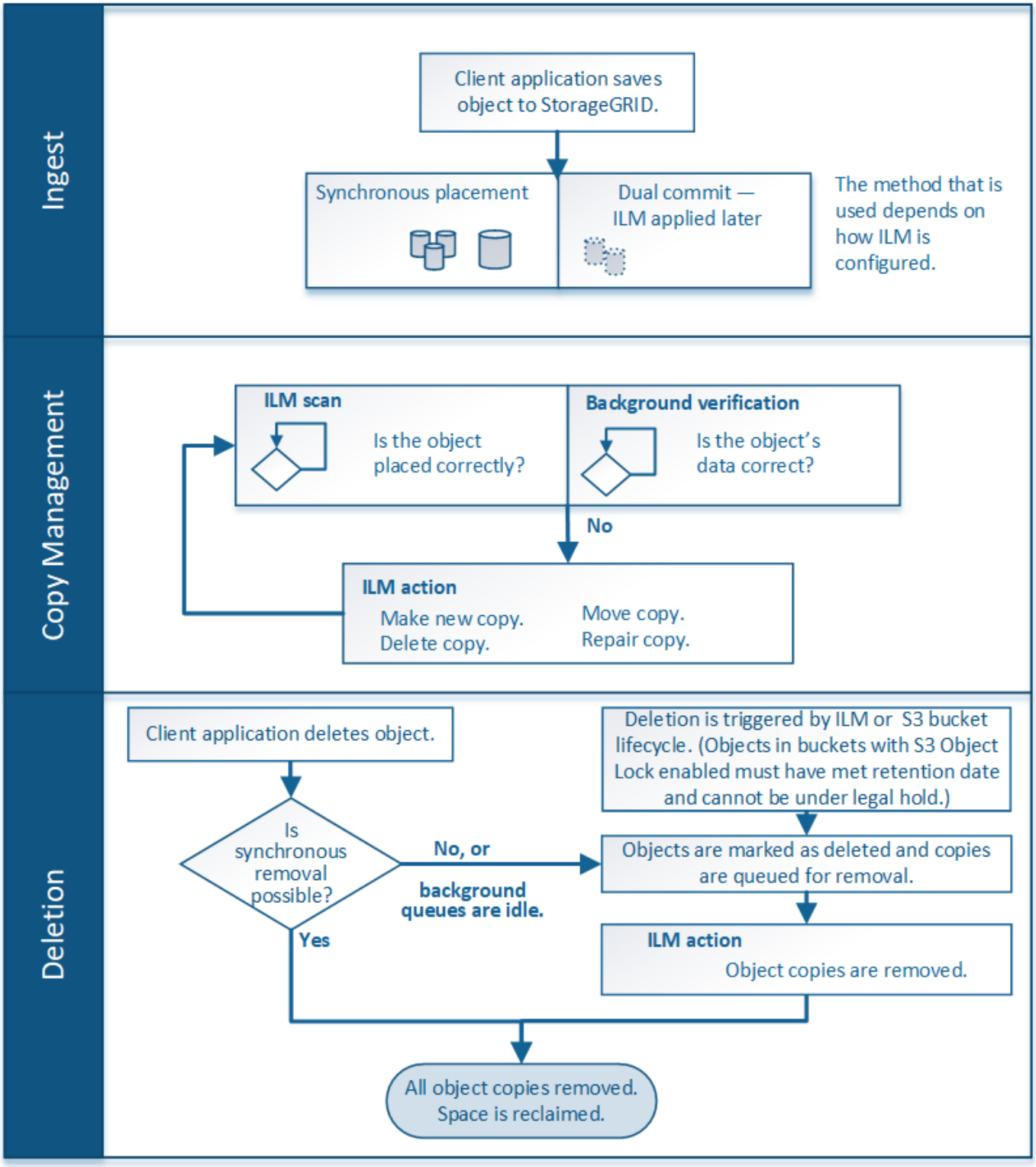
- **Ingreso**: La ingesta comienza cuando una aplicación cliente S3 o Swift establece una conexión para guardar un objeto en el sistema StorageGRID, y se completa cuando StorageGRID devuelve un mensaje de “Ingreso correcto” al cliente. Los datos de objetos se protegen durante la ingesta aplicando instrucciones de ILM inmediatamente (ubicación síncrona) o creando copias provisionales y aplicando ILM más tarde (registro doble), según cómo se especifiquen los requisitos de ILM.
- **Administración de copias**: Después de crear el número y el tipo de copias de objetos que se especifican en las instrucciones de colocación de ILM, StorageGRID administra las ubicaciones de objetos y protege los objetos contra pérdidas.
  - * Análisis y evaluación de ILM*: StorageGRID analiza continuamente la lista de objetos almacenados en la cuadrícula y comprueba si las copias actuales cumplen con los requisitos de ILM. Cuando se requieren diferentes tipos, números o ubicaciones de copias de objetos, StorageGRID crea, elimina o mueve copias según sea necesario.
  - **Verificación de antecedentes**: StorageGRID realiza continuamente la verificación de fondo para verificar la integridad de los datos de los objetos. Si se encuentra un problema, StorageGRID crea automáticamente una copia de objeto nueva o un fragmento de objeto con código de borrado de reemplazo en una ubicación que cumple los requisitos actuales de ILM. Consulte "Verifique la

integridad del objeto".

- **Eliminación de objetos**: La gestión de un objeto finaliza cuando se eliminan todas las copias del sistema StorageGRID. Los objetos se pueden eliminar como resultado de una solicitud de eliminación por parte de un cliente, o bien como resultado de la eliminación por ILM o la eliminación provocada por el vencimiento del ciclo de vida de un bloque de S3.

> Los objetos de un depósito que tiene S3 Object Lock activado no se pueden eliminar si están en una retención legal o si se ha especificado una fecha de retención hasta que no se cumple.

El diagrama resume el funcionamiento de ILM a lo largo del ciclo de vida de un objeto.



Cómo se ingieren los objetos

Opciones de procesamiento

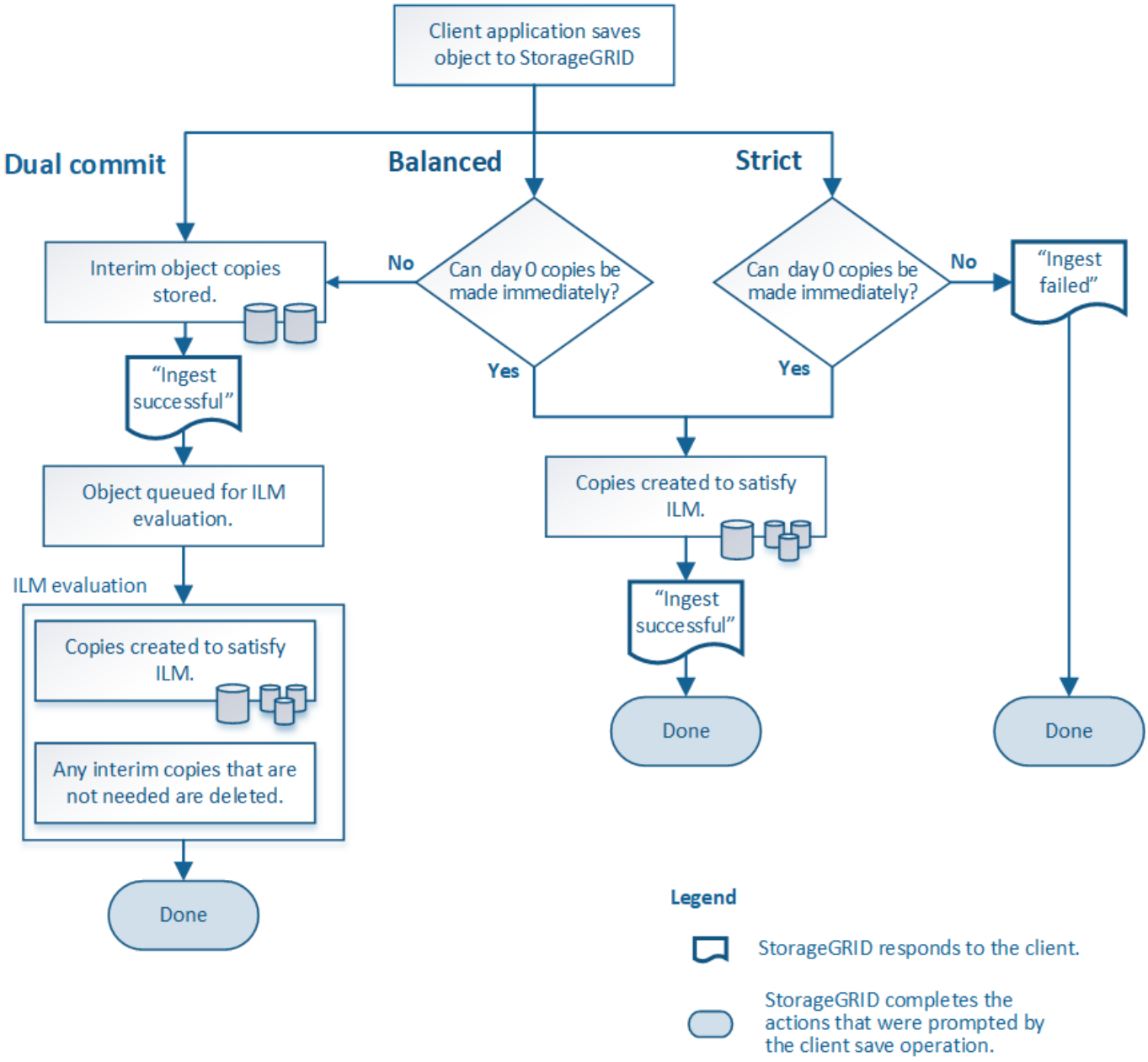
Al crear una regla de ILM, se deben especificar una de estas tres opciones para proteger los objetos durante la ingesta: Dual commit, strict o balanced.

Según elija, StorageGRID realiza copias provisionales y pone en cola los objetos para la evaluación de ILM

más tarde, o utiliza una ubicación síncrona y realiza copias inmediatamente para cumplir los requisitos de ILM.

Diagrama de flujo de opciones de ingesta

El diagrama de flujo muestra lo que ocurre cuando una regla de ILM se equipara con objetos que utiliza cada una de las tres opciones de ingesta.



Registro doble

Cuando selecciona la opción Confirmación doble, StorageGRID realiza de forma inmediata copias de objetos provisionales en dos nodos de almacenamiento diferentes y devuelve un mensaje de procesamiento correcto al cliente. El objeto se pone en cola para la evaluación de ILM, y se realicen copias que cumplan con las instrucciones de ubicación de la regla más adelante. Si la política de ILM no puede procesarse inmediatamente después de la confirmación doble, la protección contra pérdida de sitio podría tardar tiempo en lograrse.

Utilice la opción Dual Commit en uno de los siguientes casos:

- Está usando reglas de la ILM de varios sitios y la latencia de procesamiento de clientes es su principal consideración. Al utilizar la confirmación doble, debe asegurarse de que el grid pueda realizar el trabajo adicional de creación y eliminación de las copias de registro doble si no cumplen con el ciclo de vida de la información. Específicamente:
  - La carga en la cuadrícula debe ser lo suficientemente baja para evitar que se produzca una acumulación de ILM.
  - El grid debe tener un exceso de recursos de hardware (IOPS, CPU, memoria, ancho de banda de red, etc.).
- Utiliza reglas de ILM de varios sitios y la conexión WAN entre los sitios suele tener una alta latencia o un ancho de banda limitado. En este escenario, el uso de la opción Dual commit puede ayudar a evitar los tiempos de espera de los clientes. Antes de elegir la opción Dual commit, debe probar la aplicación cliente con cargas de trabajo realistas.

Equilibrada (predeterminado)

Cuando selecciona la opción equilibrada, StorageGRID también utiliza la ubicación síncrona durante la ingesta y hace inmediatamente todas las copias especificadas en las instrucciones de ubicación de la regla. En contraste con la opción estricta, si StorageGRID no puede hacer todas las copias de inmediato, utiliza Confirmación doble en su lugar. Si la política de ILM utiliza ubicaciones en varios sitios y no se puede lograr la protección inmediata contra la pérdida de sitio, se activa la alerta **ILM ubicación inalcanzable**.

Utilice la opción equilibrada para lograr la mejor combinación de protección de datos, rendimiento de grid y éxito de procesamiento. Equilibrada es la opción predeterminada del asistente Create ILM Rule.

Estricto

Al seleccionar la opción estricta, StorageGRID utiliza una ubicación síncrona al procesar y crea inmediatamente todas las copias de los objetos especificadas en las instrucciones de ubicación de la regla. La ingesta genera un error si StorageGRID no puede crear todas las copias, por ejemplo, porque no está disponible en estos momentos una ubicación de almacenamiento necesaria. El cliente debe volver a intentar la operación.

Utilice la opción estricta si tiene un requisito operativo y de normativa para almacenar inmediatamente objetos solo en las ubicaciones descritas en la regla de ILM. Por ejemplo, para satisfacer un requisito normativo, es posible que necesite utilizar la opción estricta y un filtro avanzado de restricción de ubicación para garantizar que los objetos nunca se almacenen en determinados centros de datos.

Consulte "Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto".

Ventajas, desventajas y limitaciones de las opciones de ingesta

Comprender las ventajas y las desventajas de cada una de las tres opciones de protección de datos en el procesamiento (confirmación equilibrada, estricta o doble) puede ayudarle a decidir cuál seleccionar para una regla de ILM.

Para obtener una descripción general de las opciones de ingesta, consulte "Opciones de procesamiento".

Ventajas de las opciones equilibradas y estrictas

En comparación con el registro doble, que crea copias provisionales durante la ingesta, las dos opciones de colocación sincrónica pueden proporcionar las siguientes ventajas:

- **Mejor seguridad de datos**: Los datos de objeto están protegidos inmediatamente como se especifica en las instrucciones de colocación de la regla ILM, que se pueden configurar para proteger contra una amplia variedad de condiciones de fallo, incluyendo la falla de más de una ubicación de almacenamiento. La confirmación doble solo puede protegerse contra la pérdida de una única copia local.
- **Funcionamiento de red más eficiente**: Cada objeto se procesa una sola vez, ya que se ingiere. Dado que el sistema StorageGRID no necesita realizar un seguimiento o eliminar copias provisionales, hay menos carga de procesamiento y se consume menos espacio de la base de datos.
- **(equilibrado) recomendado**: La opción equilibrada proporciona una eficiencia óptima de ILM. Se recomienda utilizar la opción Balanced a menos que se requiera un comportamiento de ingesta estricto o que el grid cumpla todos los criterios para utilizar Dual commit.
- **(estricta) certeza acerca de las ubicaciones de objetos**: La opción estricta garantiza que los objetos se almacenen inmediatamente de acuerdo con las instrucciones de colocación en la regla ILM.

Desventajas de las opciones equilibradas y estrictas

En comparación con la confirmación doble, las opciones equilibradas y estrictas tienen algunas desventajas:

- **Procesamiento de clientes más largos**: Las latencias de procesamiento de clientes pueden ser más largas. Cuando utiliza las opciones equilibradas o estrictas, no se devuelve al cliente un mensaje de ingesta correcta hasta que se creen y almacenen todos los fragmentos con código de borrado o las copias replicadas. Sin embargo, lo más probable es que los datos de objetos lleguen a su ubicación final mucho más rápido.
- **(Estrictas) mayores tasas de fallo de ingesta**: Con la opción estricta, la ingesta falla siempre que StorageGRID no puede hacer inmediatamente todas las copias especificadas en la regla de ILM. Es posible que observe tasas elevadas de error de procesamiento si una ubicación de almacenamiento necesaria está temporalmente sin conexión o si los problemas de red provocan retrasos en la copia de objetos entre sitios.
- * (Estricta) las ubicaciones de carga de varias partes de S3 pueden no ser las esperadas en algunas circunstancias*: Con estricta, se espera que los objetos se coloquen como se describe en la regla ILM o que falle el procesamiento. Sin embargo, con una carga de varias partes de S3 KB, se evalúa ILM para cada parte del objeto conforme se procesa, y para el objeto en su conjunto cuando se completa la carga de varias partes. En las siguientes circunstancias, esto podría dar lugar a colocaciones que son diferentes de lo esperado:
  - **Si ILM cambia mientras una carga multiparte de S3 está en curso**: Debido a que cada pieza se coloca según la regla que está activa cuando se ingiere la pieza, es posible que algunas partes del objeto no cumplan los requisitos actuales de ILM cuando se completa la carga de varias partes. En estos casos, la ingesta del objeto no falla. En su lugar, cualquier pieza que no se coloque correctamente se pone en cola para la reevaluación de ILM y posteriormente se mueve a la ubicación correcta.
  - **Cuando las reglas de ILM filtran el tamaño**: Al evaluar ILM para una pieza, StorageGRID filtra el tamaño de la pieza, no el tamaño del objeto. Esto significa que las partes de un objeto se pueden almacenar en ubicaciones que no cumplan con los requisitos de ILM para el objeto como un todo. Por ejemplo, si una regla especifica que todos los objetos de 10 GB o más se almacenan en DC1 mientras que todos los objetos más pequeños se almacenan en DC2, al ingerir cada parte de 1 GB de una carga multiparte de 10 partes se almacena en DC2. Cuando se evalúa ILM para el objeto, todas las partes del objeto se mueven a DC1.
- **(estricta) la ingesta no falla cuando las etiquetas de objeto o los metadatos se actualizan y las colocaciones recientemente requeridas no se pueden hacer**: Con estricto, se espera que los objetos se coloquen como se describe en la regla ILM o que falle el procesamiento. Sin embargo, cuando se actualizan metadatos o etiquetas de un objeto que ya está almacenado en la cuadrícula, el objeto no se vuelve a procesar. Esto significa que cualquier cambio en la ubicación del objeto que se desencadene por

la actualización no se realiza inmediatamente. Los cambios de colocación se realizan cuando la ILM se vuelve a evaluar por los procesos normales de ILM en segundo plano. Si no se pueden realizar cambios de ubicación necesarios (por ejemplo, porque no está disponible una nueva ubicación requerida), el objeto actualizado conserva su ubicación actual hasta que los cambios de ubicación sean posibles.

Limitaciones en la ubicación de objetos con las opciones equilibradas y estrictas

Las opciones equilibradas o estrictas no se pueden usar para reglas de ILM que tengan alguna de estas instrucciones de ubicación:

- Ubicación en un pool de almacenamiento en cloud desde el día 0.
- Ubicación en un nodo de archivado en el día 0.
- Colocaciones en un pool de almacenamiento en la nube o en un nodo de archivado cuando la regla tiene un tiempo de creación definido por el usuario como su tiempo de referencia.

Estas restricciones se deben a que StorageGRID no puede realizar copias de forma síncrona en un grupo de almacenamiento en la nube o en un nodo de archivado, y una hora de creación definida por el usuario podría resolverse en el presente.

Cómo interactúan las reglas de ILM y la coherencia para afectar a la protección de datos

Tanto su regla de ILM como su elección de coherencia afectan al modo en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, el comportamiento de ingesta seleccionado para una regla de ILM afecta a la ubicación inicial de las copias del objeto, mientras que la consistencia utilizada cuando se almacena un objeto afecta a la ubicación inicial de los metadatos de objetos. Dado que StorageGRID necesita acceso a los datos y metadatos de un objeto para satisfacer las solicitudes del cliente, seleccionar niveles de protección correspondientes para la consistencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas del sistema más predecibles.

A continuación encontrará un breve resumen de los valores de coherencia disponibles en StorageGRID:

- **Todos**: Todos los nodos reciben metadatos de objeto inmediatamente o la solicitud fallará.
- **Strong-global**: Los metadatos de objetos se distribuyen inmediatamente a todos los sitios. Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente en todos los sitios.
- **Strong-site**: Los metadatos de objetos se distribuyen inmediatamente a otros nodos en el sitio. Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.
- **Read-after-new-write**: Proporciona consistencia de lectura después de escritura para nuevos objetos y consistencia eventual para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
- **Disponible**: Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

> Antes de seleccionar un valor de consistencia, "lea la descripción completa de la consistencia". Debe comprender los beneficios y las limitaciones antes de cambiar el valor predeterminado.

Un ejemplo de cómo pueden interactuar las reglas de coherencia e ILM

Suponga que tiene un grid de dos sitios con la siguiente regla de ILM y la siguiente consistencia:

- **Norma ILM**: Cree dos copias de objetos, una en el sitio local y otra en un sitio remoto. Use un comportamiento de ingesta estricto.
- **Consistencia**: Fuerte-global (los metadatos de objetos se distribuyen inmediatamente a todos los sitios).

Cuando un cliente almacena un objeto en el grid, StorageGRID realiza copias de objetos y distribuye los metadatos en ambos sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra la pérdida en el momento del mensaje de procesamiento correcto. Por ejemplo, si el sitio local se pierde poco después del procesamiento, seguirán existiendo copias de los datos del objeto y los metadatos del objeto en el sitio remoto. El objeto se puede recuperar completamente.

Si, en cambio, utiliza la misma regla de ILM y la coherencia del sitio fuerte, es posible que el cliente reciba un mensaje de éxito después de replicar los datos de objetos en el sitio remoto, pero antes de que los metadatos de los objetos se distribuyan allí. En este caso, el nivel de protección de los metadatos de objetos no coincide con el nivel de protección de los datos de objetos. Si el sitio local se pierde poco después del procesamiento, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre las reglas de coherencia y de ILM puede ser compleja. Póngase en contacto con NetApp si necesita ayuda.

Información relacionada

- "Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto"

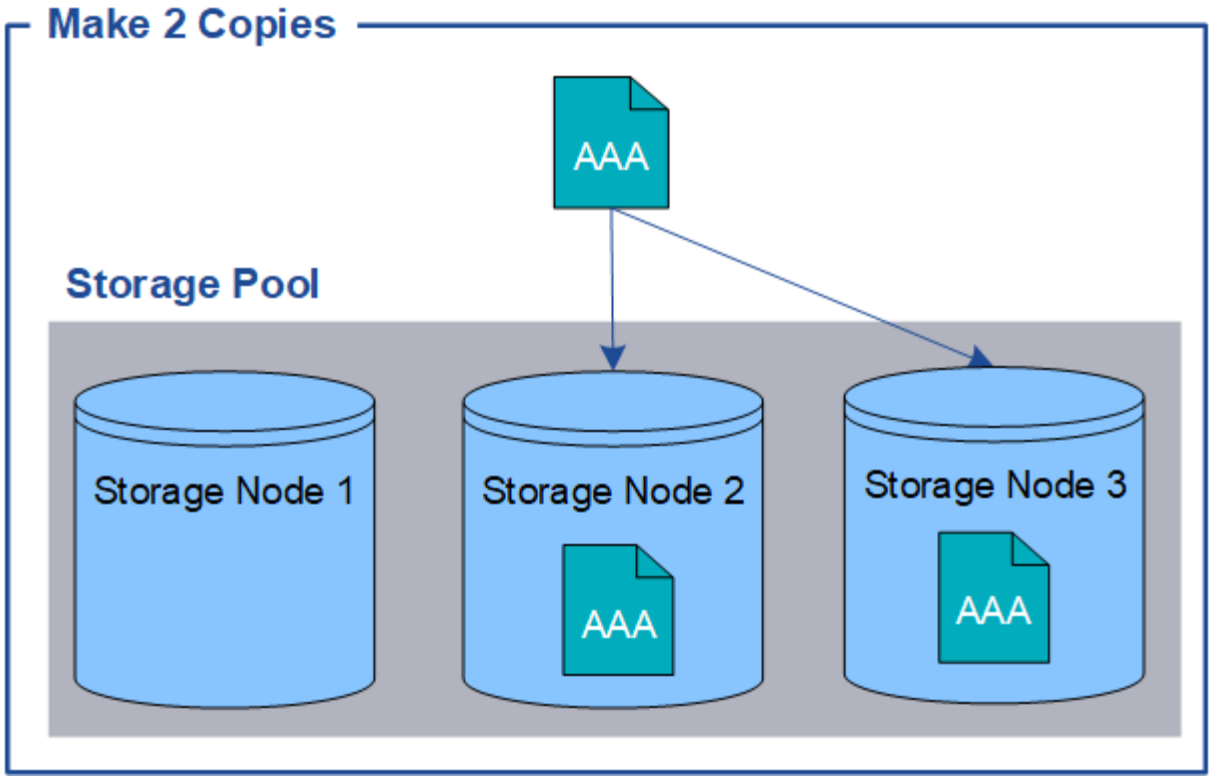
Cómo se almacenan los objetos (codificación de borrado o replicación)

¿Qué es la replicación?

La replicación es uno de los dos métodos que utiliza StorageGRID para almacenar datos de objetos. Cuando los objetos coinciden con una regla de ILM que usa la replicación, el sistema crea copias exactas de datos de objetos y almacena las copias en nodos de almacenamiento o nodos de archivado.

Cuando configura una regla de ILM para crear copias replicadas, especifica cuántas copias se deben crear, dónde deben ubicarse y cuánto tiempo deben almacenarse las copias en cada ubicación.

En el ejemplo siguiente, la regla de ILM especifica que dos copias replicadas de cada objeto se coloquen en un pool de almacenamiento que contenga tres nodos de almacenamiento.



Cuando StorageGRID coincide con los objetos de esta regla, crea dos copias del objeto, colocando cada copia en un nodo de almacenamiento diferente en el pool de almacenamiento. Las dos copias pueden colocarse en dos de los tres nodos de almacenamiento disponibles. En este caso, la regla colocó copias de objetos en los nodos de almacenamiento 2 y 3. Debido a que hay dos copias, el objeto se puede recuperar si alguno de los nodos del pool de almacenamiento falla.

> StorageGRID solo puede almacenar una copia replicada de un objeto en un nodo de almacenamiento dado. Si el grid incluye tres nodos de almacenamiento y se crea una regla de gestión del ciclo de vida de la información de 4 copias, solo se crearán tres copias: Una por cada nodo de almacenamiento. Se activa la alerta **colocación de ILM inalcanzable** para indicar que la regla ILM no se pudo aplicar completamente.

Información relacionada

- "Qué es la codificación de borrado"
- "Qué es un pool de almacenamiento"
- "Habilite la protección contra pérdida de sitios mediante replicación y código de borrado"

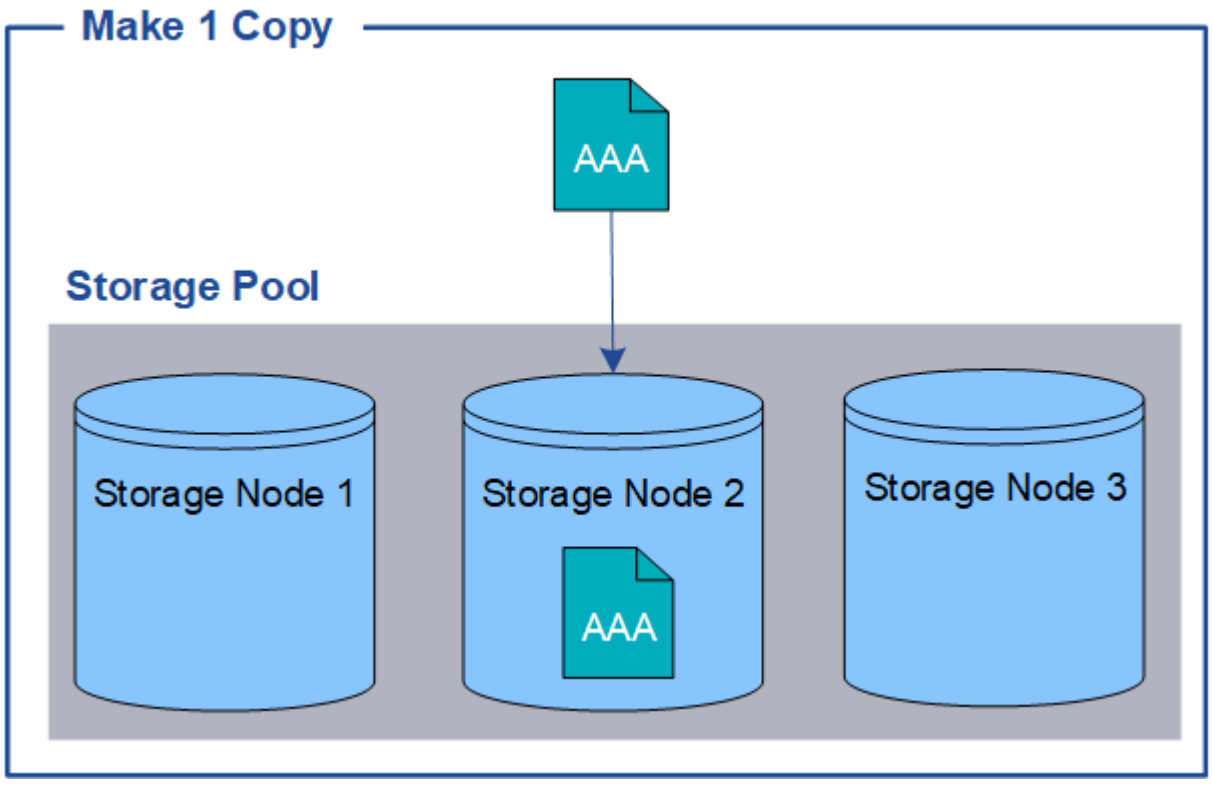
Por qué no se debe utilizar la replicación de copia única

Al crear una regla de ILM para crear copias replicadas, debe especificar siempre al menos dos copias durante cualquier periodo de tiempo en las instrucciones de ubicación.

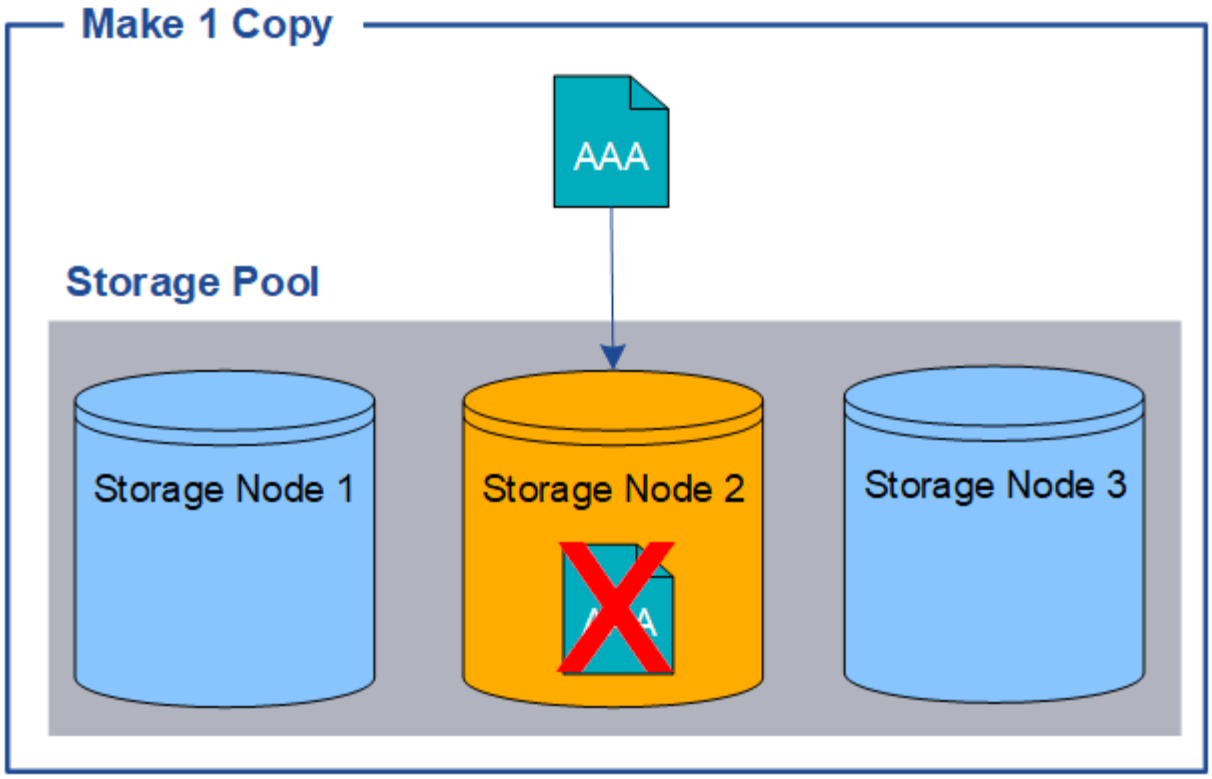
> No utilice una regla de ILM que cree solo una copia replicada durante un período de tiempo. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

En el ejemplo siguiente, la regla Make 1 Copy ILM especifica que una copia replicada de un objeto se coloca

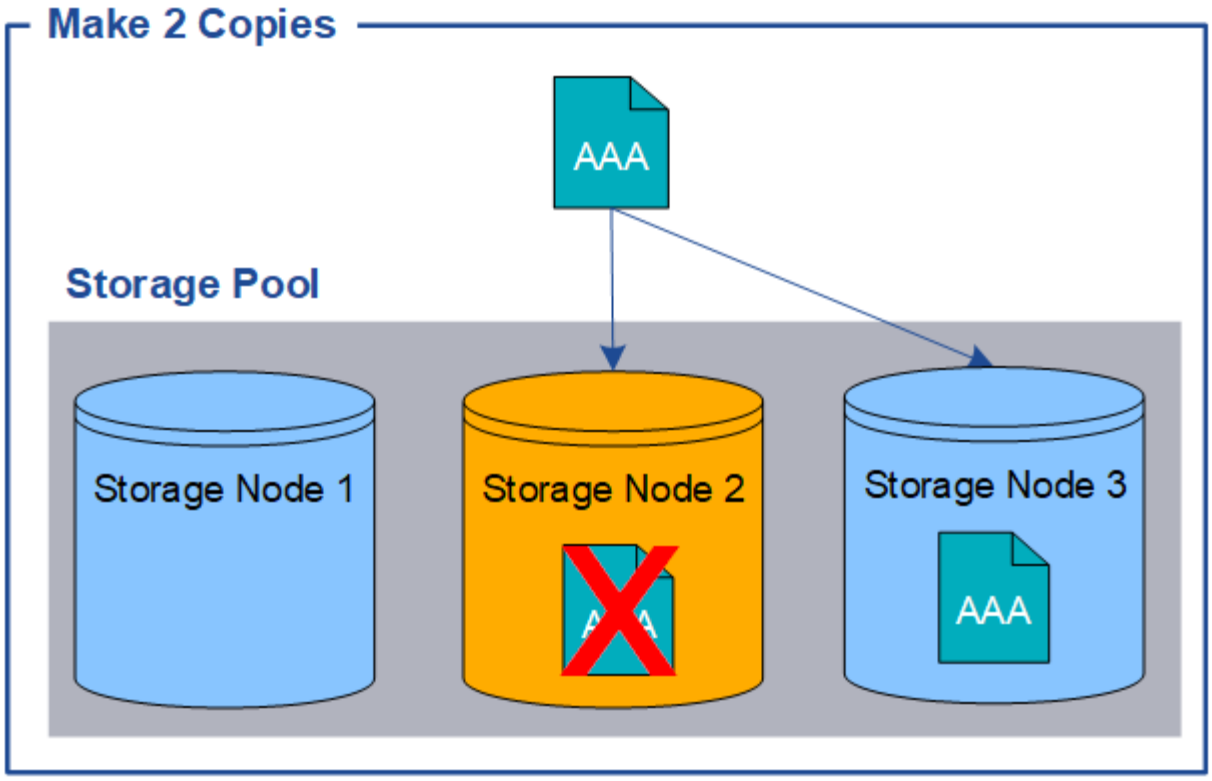
en un pool de almacenamiento que contiene tres nodos de almacenamiento. Cuando se ingiere un objeto que coincida con esta regla, StorageGRID coloca una sola copia en un solo nodo de almacenamiento.



Cuando una regla de ILM crea solo una copia replicada de un objeto, se vuelve inaccesible cuando el nodo de almacenamiento no está disponible. En este ejemplo, perderá temporalmente el acceso al objeto AAA siempre que el nodo de almacenamiento 2 esté desconectado, como durante una actualización u otro procedimiento de mantenimiento. Perderá el objeto AAA completamente si falla el nodo de almacenamiento 2.



Para evitar la pérdida de datos de objetos, siempre debe realizar al menos dos copias de todos los objetos que desee proteger con replicación. Si existen dos o más copias, puede seguir teniendo acceso al objeto si un nodo de almacenamiento falla o se desconecta.



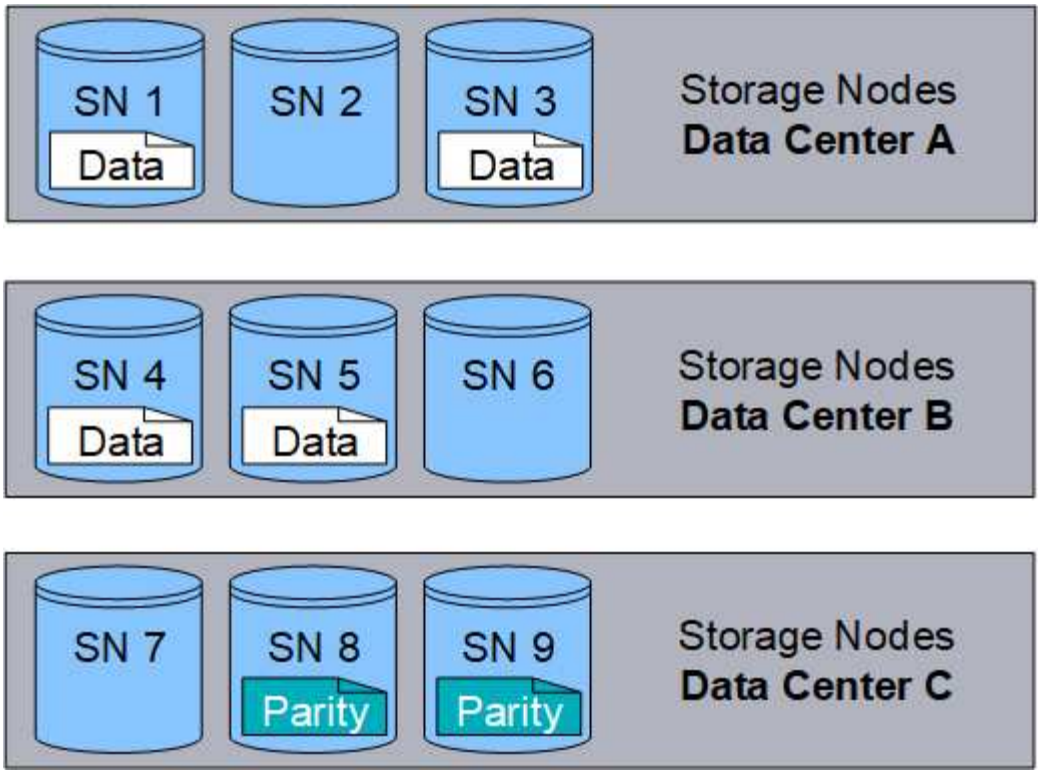
¿Qué es el código de borrado?

El código de borrado es uno de los dos métodos que utiliza StorageGRID para almacenar datos de objetos. Cuando los objetos coinciden con una regla de ILM que utiliza código de borrado, esos objetos se dividen en fragmentos de datos, se calculan fragmentos de paridad adicionales y cada fragmento se almacena en un nodo de almacenamiento diferente.

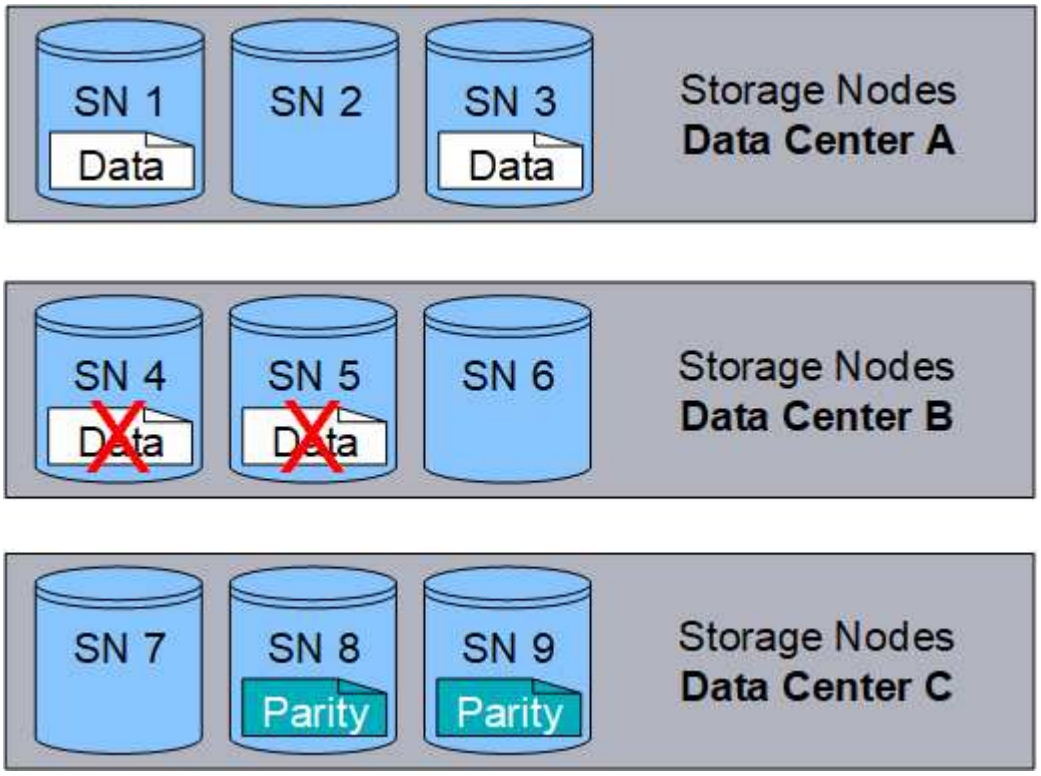
Cuando se accede a un objeto, se vuelve a ensamblar utilizando los fragmentos almacenados. Si un dato o un fragmento de paridad se corrompen o se pierden, el algoritmo de código de borrado puede recrear ese fragmento con un subconjunto de los datos restantes y los fragmentos de paridad.

Al crear reglas de ILM, StorageGRID crea perfiles de código de borrado compatibles con esas reglas. Puede ver una lista de perfiles de codificación de borrado, "cambie el nombre de un perfil de código de borrado", o. "Desactive un perfil de código de borrado si actualmente no se utiliza en ninguna regla de ILM".

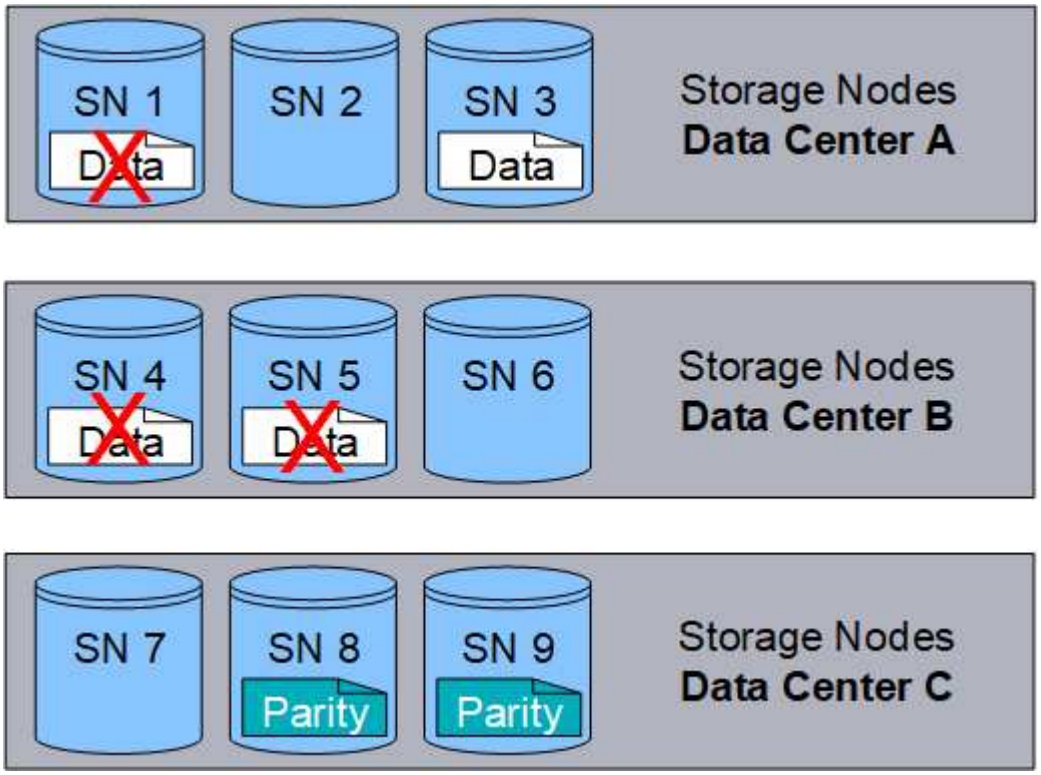
En el siguiente ejemplo, se muestra el uso de un algoritmo de codificación de borrado en los datos de un objeto. En este ejemplo, la regla ILM utiliza un esquema de codificación de borrado 4+2. Cada objeto se divide en cuatro fragmentos de datos iguales y dos fragmentos de paridad se calculan a partir de los datos del objeto. Cada uno de los seis fragmentos se almacena en un nodo diferente en tres sitios de centro de datos para proporcionar protección de datos ante fallos de nodos o pérdidas de sitios.



El esquema de codificación de borrado 4+2 se puede configurar de varias maneras. Por ejemplo, puede configurar un pool de almacenamiento de un único sitio que contenga seis nodos de almacenamiento. Para "protección contra pérdida de sitios", Puede utilizar un pool de almacenamiento que contenga tres sitios con tres nodos de almacenamiento en cada sitio. Un objeto se puede recuperar siempre que cuatro de los seis fragmentos (datos o paridad) permanezcan disponibles. Se pueden perder hasta dos fragmentos sin perder los datos del objeto. Si se pierde un sitio entero, el objeto aún puede recuperarse o repararse, siempre que se pueda acceder a todos los demás fragmentos.



Si se pierden más de dos nodos de almacenamiento, el objeto no se puede recuperar.



Información relacionada

- "Qué es la replicación"
- "Qué es un pool de almacenamiento"
- "¿Qué son los esquemas de código de borrado"
- "Cambie el nombre de un perfil de código de borrado"
- "Desactivar un perfil de código de borrado"

¿Qué son los esquemas de código de borrado?

Los esquemas de codificación de borrado controlan cuántos fragmentos de datos se crean y cuántos fragmentos de paridad se crean para cada objeto.

Cuando configura el perfil de código de borrado para una regla de ILM, debe seleccionar un esquema de código de borrado disponible en función del número de nodos de almacenamiento y sitios que componen el pool de almacenamiento que piensa usar.

El sistema StorageGRID utiliza el algoritmo de codificación de borrado Reed-Solomon. El algoritmo divide un objeto en `k` fragmentos de datos y cálculos `m` fragmentos de paridad. La `k + m = n` los fragmentos se distribuyen `n` Nodos de almacenamiento para proporcionar protección de datos. Un objeto puede soportar hasta `m` fragmentos perdidos o corruptos. Para recuperar o reparar un objeto, `k` se necesitan fragmentos.

Cuando seleccione el pool de almacenamiento que se utilizará en una regla que creará una copia con código de borrado, utilice las siguientes directrices para los pools de almacenamiento:

- El pool de almacenamiento debe incluir tres o más sitios, o exactamente un sitio.

No se puede usar código de borrado si el pool de almacenamiento incluye dos sitios.

  - Esquemas de codificación de borrado para pools de almacenamiento que contengan tres o más sitios
  - Esquemas de codificación de borrado para pools de almacenamiento in situ

- No utilice un pool de almacenamiento que incluya el sitio predeterminado, Todos los sitios.
- El pool de almacenamiento debe incluir al menos *k+m* +1 Nodos de almacenamiento que pueden almacenar datos de objetos.

  Los nodos de almacenamiento se pueden configurar durante la instalación de modo que solo contengan metadatos de objetos y no datos de objetos. Para obtener más información, consulte "Tipos de nodos de almacenamiento".

  El número mínimo necesario de nodos de almacenamiento es k+m. Sin embargo, tener al menos un nodo de almacenamiento adicional puede ayudar a evitar fallos de ingesta o errores de gestión de la vida útil si un nodo de almacenamiento necesario no está disponible temporalmente.

La sobrecarga de almacenamiento de un esquema de código de borrado se calcula dividiendo el número de fragmentos de paridad (m) por el número de fragmentos de datos (k). Puede utilizar la sobrecarga del almacenamiento para calcular cuánto espacio en disco necesita cada objeto con código de borrado:

*disk space = object size + (object size * storage overhead)*

Por ejemplo, si almacena un objeto de 10 MB mediante el esquema 4+2 (que tiene un 50% de sobrecarga de almacenamiento), el objeto consume 15 MB de almacenamiento de cuadrícula. Si almacena el mismo objeto de 10 MB con el esquema 6+2 (que tiene un 33% de sobrecarga de almacenamiento), el objeto consume aproximadamente 13.3 MB.

Seleccione el esquema de código de borrado que tenga el valor total más bajo de k+m que satisface sus necesidades. Los esquemas de código de borrado con un número menor de fragmentos por lo general son más eficientes computacionalmente, ya que se crean y distribuyen menos fragmentos (o se recuperan) por objeto, pueden ofrecer un mejor rendimiento debido al tamaño de fragmento más grande y pueden requerir que se añadan menos nodos en una expansión cuando se necesita más almacenamiento. (Para obtener información sobre cómo planificar una expansión de almacenamiento, consulte "Instrucciones para ampliar StorageGRID".)

Esquemas de codificación de borrado para pools de almacenamiento que contengan tres o más sitios

En la siguiente tabla se describen los esquemas de codificación de borrado que admite actualmente StorageGRID para pools de almacenamiento que incluyen tres o más sitios. Todos estos esquemas proporcionan protección contra pérdida de sitio. Se puede perder un sitio y el objeto seguirá siendo accesible.

Para esquemas de código de borrado que ofrecen protección contra pérdida de sitio, la cantidad recomendada de nodos de almacenamiento en el pool de almacenamiento supera *k+m* +1 Dado que cada sitio requiere un mínimo de tres nodos de almacenamiento.

Esquema de codificación de borrado (*k*+*m*)	Número mínimo de sitios implementados	Número recomendado de nodos de almacenamiento en cada sitio	Número total recomendado de nodos de almacenamiento	¿Protección contra pérdida de sitio?	Gastos generales de almacenamiento
4+2	3	3	9	Sí	50 %
6+2	4	3	12	Sí	33 %
8+2	5	3	15	Sí	25 %
6+3	3	4	12	Sí	50 %
9+3	4	4	16	Sí	33 %
2+1	3	3	9	Sí	50 %
4+1	5	3	15	Sí	25 %
6+1	7	3	21	Sí	17 %
7+5	3	5	15	Sí	71 %

StorageGRID requiere un mínimo de tres nodos de almacenamiento por sitio. Para utilizar el esquema 7+5, cada sitio requiere un mínimo de cuatro nodos de almacenamiento. Se recomienda usar cinco nodos de almacenamiento por sitio.

Al seleccionar un esquema de codificación de borrado que proporcione protección al sitio, equilibre la importancia relativa de los siguientes factores:

- **Número de fragmentos**: El rendimiento y la flexibilidad de expansión son generalmente mejores cuando el número total de fragmentos es menor.
- **Tolerancia a fallos**: La tolerancia a fallos se incrementa al tener más segmentos de paridad (es decir, cuando `m` tiene un valor más alto.)
- **Tráfico de red**: Al recuperarse de fallos, utilizando un esquema con más fragmentos (es decir, un total más alto para `k+m`) crea más tráfico de red.
- **Gastos generales de almacenamiento**: Los esquemas con mayor sobrecarga requieren más espacio de almacenamiento por objeto.

Por ejemplo, al decidir entre un esquema 4+2 y un esquema 6+3 (que ambos tienen un 50% de gastos generales de almacenamiento), seleccione el esquema 6+3 si se requiere tolerancia a fallos adicional. Seleccione el esquema 4+2 si los recursos de red están limitados. Si todos los demás factores son iguales, seleccione 4+2 porque tiene un número total menor de fragmentos.

Si no está seguro de qué esquema usar, seleccione 4+2 o 6+3, o póngase en contacto con el servicio de asistencia técnica.

Esquemas de codificación de borrado para pools de almacenamiento in situ

Un pool de almacenamiento in situ admite todos los esquemas de codificación de borrado definidos para tres o más sitios, siempre y cuando el sitio tenga suficientes nodos de almacenamiento.

El número mínimo necesario de nodos de almacenamiento es `k+m`, pero una piscina de almacenamiento con `k+m +1` Se recomiendan los nodos de almacenamiento. Por ejemplo, el esquema de codificación de borrado 2+1 requiere un pool de almacenamiento con un mínimo de tres nodos de almacenamiento, pero se recomiendan cuatro nodos de almacenamiento.

Esquema de codificación de borrado (*k+m*)	Número mínimo de nodos de almacenamiento	Número recomendado de nodos de almacenamiento	Gastos generales de almacenamiento
4+2	6	7	50 %
6+2	8	9	33 %
8+2	10	11	25 %
6+3	9	10	50 %
9+3	12	13	33 %
2+1	3	4	50 %
4+1	5	6	25 %
6+1	7	8	17 %
7+5	12	13	71 %

Ventajas, desventajas y requisitos de codificación de borrado

Antes de decidir si se debe utilizar la replicación o el código de borrado para proteger los datos de objetos frente a pérdidas, debe comprender las ventajas, las desventajas y los requisitos para la codificación de borrado.

Ventajas de la codificación de borrado

En comparación con la replicación, la codificación de borrado ofrece una mayor fiabilidad, disponibilidad y eficiencia del almacenamiento.

- **Confiabilidad**: La fiabilidad se mide en términos de tolerancia a fallos, es decir, el número de fallos simultáneos que se pueden sostener sin pérdida de datos. Con la replicación, se almacenan varias copias idénticas en diferentes nodos y entre sitios. Con el código de borrado, un objeto se codifica en fragmentos de datos y de paridad, y se distribuye entre muchos nodos y sitios. Esta dispersión proporciona protección frente a fallos del sitio y del nodo. En comparación con la replicación, la codificación de borrado proporciona una mayor fiabilidad con costes de almacenamiento comparables.

- **Disponibilidad**: La disponibilidad se puede definir como la capacidad de recuperar objetos si los nodos de almacenamiento fallan o se vuelven inaccesibles. En comparación con la replicación, la codificación de borrado proporciona una mayor disponibilidad con costes de almacenamiento comparables.
- **Eficiencia del almacenamiento**: Para niveles similares de disponibilidad y fiabilidad, los objetos protegidos mediante codificación de borrado consumen menos espacio en disco que los mismos objetos si están protegidos mediante replicación. Por ejemplo, un objeto de 10 MB que se replica en dos sitios consume 20 MB de espacio en disco (dos copias), mientras que el objeto con código de borrado en tres sitios con un esquema de código de borrado 6+3 solo consume 15 MB de espacio en disco.

> El espacio en disco para los objetos codificados de borrado se calcula como el tamaño del objeto más la sobrecarga del almacenamiento. El porcentaje de sobrecarga del almacenamiento es el número de fragmentos de paridad dividido por el número de fragmentos de datos.

Desventajas del código de borrado

En comparación con la replicación, los códigos de borrado tienen las siguientes desventajas:

- Se recomienda un mayor número de nodos de almacenamiento y sitios, en función del esquema de código de borrado. Por el contrario, si replica datos de objetos, solo necesita un nodo de almacenamiento para cada copia. Consulte "Esquemas de codificación de borrado para pools de almacenamiento que contengan tres o más sitios" y.. "Esquemas de codificación de borrado para pools de almacenamiento in situ".
- Aumento del coste y de la complejidad de las ampliaciones del almacenamiento. Para expandir una implementación que utiliza replicación, debe agregar capacidad de almacenamiento en cada ubicación donde se realicen copias de objetos. Para ampliar una puesta en marcha que utilice código de borrado, debe tener en cuenta el esquema de codificación de borrado y el grado de llenado de los nodos de almacenamiento existentes. Por ejemplo, si espera a que los nodos existentes estén llenos al 100 %, debe agregar al menos `k+m` Nodos de almacenamiento, pero si amplía cuando los nodos existentes estén llenos al 70 %, puede añadir dos nodos por sitio y seguir maximizando la capacidad de almacenamiento útil. Para obtener más información, consulte "Añada capacidad de almacenamiento para objetos codificados de borrado".
- Al utilizar códigos de borrado en ubicaciones distribuidas geográficamente, aumenta la latencia de recuperación. Los fragmentos de objetos para un objeto que se codifica para el borrado y se distribuye por sitios remotos tardan más en recuperarse a través de conexiones WAN que un objeto que se replica y está disponible localmente (el mismo sitio al que se conecta el cliente).
- Al utilizar la codificación de borrado en ubicaciones distribuidas geográficamente, se está utilizando más el tráfico de red WAN para restauraciones y reparaciones, especialmente en objetos que se recuperan con frecuencia o para reparaciones de objetos a través de conexiones de red WAN.
- Cuando se utiliza la codificación de borrado en varios sitios, el rendimiento máximo del objeto se reduce drásticamente a medida que aumenta la latencia de red entre sitios. Esta disminución se debe a la correspondiente disminución del rendimiento de la red TCP, que afecta a la rapidez con la que el sistema StorageGRID puede almacenar y recuperar fragmentos de objeto.
- Mayor uso de recursos de computación.

Cuándo se debe utilizar la codificación de borrado

El código de borrado se ajusta mejor a los siguientes requisitos:

- Los objetos tienen un tamaño superior a 1 MB.

> El código de borrado se adapta mejor a los objetos de más de 1 MB. No use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

- Almacenamiento a largo plazo o en frío para contenido que se recupera con poca frecuencia.
- Alta disponibilidad y fiabilidad de los datos.
- Protección frente a fallos completos de sitios y nodos.
- Eficiencia del almacenamiento.
- Puestas en marcha de un único sitio que requieren protección de datos eficiente con solo una copia codificada por borrado en lugar de múltiples copias replicadas.
- Puestas en marcha de varios sitios en las que la latencia entre sitios es inferior a 100 ms.

Cómo se determina la retención de objetos

StorageGRID ofrece opciones tanto para los administradores de grid como para los usuarios individuales de inquilino para especificar el tiempo que se tarda en almacenar los objetos. En general, cualquier instrucción de retención proporcionada por un usuario inquilino tiene prioridad sobre las instrucciones de retención proporcionadas por el administrador de grid.

Cómo los usuarios de inquilinos controlan la retención de objetos

Los usuarios de inquilinos tienen tres formas principales de controlar cuánto tiempo se almacenan los objetos en StorageGRID:

- Si la configuración global de Object Lock está habilitada para el grid, los usuarios inquilinos S3 pueden crear bloques con S3 Object Lock habilitado y, a continuación, utilizar la API REST de S3 para especificar la configuración de retención hasta la fecha y la conservación legal de cada versión de objeto añadida a ese bloque.
  - Una versión de objeto que está bajo una conservación legal no se puede eliminar con ningún método.
  - Antes de que se alcance la fecha de retención hasta la versión de un objeto, esa versión no se puede eliminar con ningún método.
  - Los objetos de los bloques con S3 Object Lock habilitado son conservados por ILM «para siempre». Sin embargo, cuando se alcanza su fecha de retención hasta la fecha, una solicitud de cliente o el vencimiento del ciclo de vida del bloque pueden eliminar una versión de objeto. Consulte "Gestione objetos con S3 Object Lock".
- Los usuarios de inquilinos S3 pueden añadir una configuración del ciclo de vida a sus bloques que especifica una acción de caducidad. Si existe un ciclo de vida de un bloque, StorageGRID almacena un objeto hasta que se cumpla la fecha o el número de días especificados en la acción Expiración, a menos que el cliente elimine primero el objeto. Consulte "Cree una configuración del ciclo de vida de S3".
- Un cliente S3 o Swift puede emitir una solicitud de eliminación de objeto. StorageGRID siempre prioriza las solicitudes de eliminación de clientes por encima del ciclo de vida de los bloques S3 o ILM al determinar si se debe eliminar o conservar un objeto.

Cómo los administradores de grid controlan la retención de objetos

Los administradores de grid utilizan las instrucciones de colocación de ILM para controlar la duración de los objetos almacenados. Cuando una regla de ILM coincide con los objetos, StorageGRID almacena esos

objetos hasta que haya transcurrido el último periodo de tiempo de la regla de ILM. Los objetos se conservan indefinidamente si se especifica «Forever» para las instrucciones de colocación.

Independientemente de quién controle el tiempo durante el que se retienen los objetos, los ajustes de ILM controlan qué tipos de copias de objetos (replicadas o con código de borrado) se almacenan y dónde se encuentran las copias (nodos de almacenamiento, pools de almacenamiento en cloud o nodos de archivado).

Cómo interaccionan el ciclo de vida de bloque y ILM de S3

Cuando se configura el ciclo de vida de un bloque de S3, las acciones de caducidad del ciclo de vida anulan la política de ILM de los objetos que coinciden con el filtro de ciclo de vida. Como resultado, es posible que un objeto se conserve en la cuadrícula aunque hayan caducado las instrucciones de gestión del ciclo de vida de la información relativas a la ubicación del objeto.

Ejemplos para la retención de objetos

Para comprender mejor las interacciones entre S3 Object Lock, la configuración del ciclo de vida de bloques, las solicitudes de eliminación de clientes y ILM, tenga en cuenta los siguientes ejemplos.

Ejemplo 1: El ciclo de vida de un bloque de S3 mantiene los objetos durante más tiempo que ILM

ILM

Almacene dos copias por 1 año (365 días)

Ciclo de vida del cucharón

Caducidad de objetos en 2 años (730 días)

Resultado

StorageGRID almacena el objeto durante 730 días. StorageGRID utiliza la configuración del ciclo de vida de los bloques para determinar si se debe eliminar o conservar un objeto.

> Si el ciclo de vida de un bloque especifica que los objetos se deben conservar durante más tiempo del ciclo de vida de la información especificado por ILM, StorageGRID sigue usando las instrucciones de colocación de ILM al determinar el número y el tipo de copias que se deben almacenar. En este ejemplo, se seguirán almacenando dos copias del objeto en StorageGRID de los días 366 a 730.

Ejemplo 2: El ciclo de vida de bloque de S3 caduca los objetos antes de ILM

ILM

Almacene dos copias durante 2 años (730 días)

Ciclo de vida del cucharón

Caducar objetos en un año (365 días)

Resultado

StorageGRID elimina ambas copias del objeto después del día 365.

Ejemplo 3: La eliminación de clientes anula el ciclo de vida del bloque y el ILM

ILM

Almacene dos copias en los nodos de almacenamiento «por siempre»

Ciclo de vida del cucharón

Caducidad de objetos en 2 años (730 días)

Solicitud de eliminación de cliente

Emitido el día 400

Resultado

StorageGRID elimina ambas copias del objeto el día 400 en respuesta a la solicitud de eliminación del cliente.

Ejemplo 4: El bloqueo de objetos S3 anula la solicitud de eliminación del cliente

Bloqueo de objetos de S3

La fecha de retención hasta la versión de un objeto es 2026-03-31. No existe un derecho legal.

Regla de ILM que cumpla con las normativas

Almacene dos copias en los nodos de almacenamiento «por siempre»

Solicitud de eliminación de cliente

Emitido el 2024-03-31

Resultado

StorageGRID no eliminará la versión del objeto porque la fecha de retención hasta todavía está a 2 años.

Cómo se eliminan los objetos

StorageGRID puede eliminar objetos en respuesta directa a una solicitud del cliente o de forma automática como resultado del vencimiento del ciclo de vida de un bloque de S3 o de los requisitos de la política de ILM. Comprender las diferentes formas en que se pueden eliminar los objetos y el modo en que StorageGRID gestiona las solicitudes de eliminación puede ayudarle a gestionar los objetos de forma más eficaz.

StorageGRID puede utilizar uno de estos dos métodos para eliminar objetos:

- Eliminación síncrona: Cuando StorageGRID recibe una solicitud de eliminación de cliente, todas las copias de los objetos se eliminan de inmediato. Se informa al cliente de que la eliminación se ha realizado correctamente una vez eliminadas las copias.
- Los objetos se ponen en cola para eliminación: Cuando StorageGRID recibe una solicitud de eliminación, el objeto se pone en cola para su eliminación y se informa al cliente inmediatamente de que esta se ha eliminado correctamente. Las copias de objetos se eliminan más adelante mediante el procesamiento de ILM en segundo plano.

Cuando se eliminan objetos, StorageGRID utiliza el método que optimiza el rendimiento de eliminación, minimiza las posibles acumulaciones de eliminación y libera espacio que se libera con mayor rapidez.

La tabla resume cuándo StorageGRID utiliza cada método.

Método de eliminación	Cuando se utilice
Los objetos se mantienen en la cola para su eliminación	Cuando **cualquiera** de las siguientes condiciones se cumple: • La eliminación automática de objetos ha sido activada por uno de los siguientes eventos: ◦ Se ha alcanzado la fecha de caducidad o el número de días en la configuración del ciclo de vida de un bloque de S3. ◦ El último periodo de tiempo especificado en una regla de ILM transcurre. **Nota:** Los objetos en un depósito que tiene S3 Object Lock habilitado no se pueden eliminar si están bajo una retención legal o si se ha especificado una fecha de retención hasta la fecha pero aún no se cumplen. • Un cliente de S3 o Swift solicita la eliminación y se debe cumplir una o varias de estas condiciones: ◦ Las copias no se pueden eliminar en 30 segundos porque, por ejemplo, una ubicación de objetos no está disponible en este momento. ◦ Las colas de eliminación en segundo plano están inactivas.
Los objetos se quitan de inmediato (eliminación síncrona)	Cuando un cliente S3 o Swift realiza una solicitud de eliminación y **se cumplen todas** las siguientes condiciones: • Todas las copias se pueden eliminar en 30 segundos. • Las colas de eliminación en segundo plano contienen objetos que se van a procesar.

Cuando los clientes S3 o Swift realizan solicitudes de eliminación, StorageGRID empieza añadiendo objetos a la cola de eliminación. A continuación, cambia a realizar una eliminación síncrona. Asegurarse de que la cola de eliminación en segundo plano tiene objetos que procesar permite a StorageGRID procesar las eliminaciones de forma más eficaz, especialmente en los clientes de baja concurrencia, mientras que ayuda a evitar que los clientes eliminen las copias de seguridad.

Tiempo necesario para eliminar objetos

La forma en que StorageGRID elimina los objetos puede afectar a la forma en la que aparece el sistema:

- Cuando StorageGRID realiza la eliminación síncrona, StorageGRID puede tardar hasta 30 segundos en devolver un resultado al cliente. Esto significa que la eliminación puede parecer más lenta, aunque en realidad se eliminan copias más rápidamente de lo que están cuando StorageGRID pone en cola objetos para su eliminación.
- Si supervisa con atención el rendimiento de eliminación durante una eliminación masiva, puede observar que la tasa de eliminación parece lenta después de eliminar un cierto número de objetos. Este cambio ocurre cuando StorageGRID pasa de poner objetos en cola para su eliminación a realizar una eliminación síncrona. La reducción aparente en la tasa de eliminación no significa que las copias de objetos se van a eliminar más lentamente. Por el contrario, indica que, en promedio, ahora se libera espacio con más rapidez.

Si elimina un gran número de objetos y la prioridad es liberar espacio rápidamente, considere la posibilidad de usar una solicitud de cliente para eliminar objetos en lugar de eliminarlos con ILM u otros métodos. En general, el espacio se libera más rápidamente cuando los clientes lo eliminan, ya que StorageGRID puede

utilizar la eliminación síncrona.

La cantidad de tiempo necesario para liberar espacio después de eliminar un objeto depende de varios factores:

- Si las copias de objetos se eliminan de forma síncrona o se ponen en cola para su eliminación más adelante (para solicitudes de eliminación de clientes).
- Otros factores, como el número de objetos de la cuadrícula o la disponibilidad de los recursos de grid cuando las copias de objetos se colocan en cola para su eliminación (tanto para los eliminaciones del cliente como para otros métodos).

Cómo se eliminan los objetos con versiones de S3

Cuando se habilita el control de versiones para un bloque de S3, StorageGRID sigue el comportamiento de Amazon S3 al responder a las solicitudes de eliminación, ya provenga de un cliente S3, el vencimiento de un ciclo de vida de un bloque de S3 o los requisitos de la política de ILM.

Cuando los objetos se versionan, las solicitudes de eliminación de objetos no eliminan la versión actual del objeto y no liberan espacio. En su lugar, una solicitud de eliminación de objeto crea un marcador de eliminación de cero bytes como la versión actual del objeto, lo que hace que la versión anterior del objeto sea «no actual». Un marcador de supresión de objeto se convierte en un marcador de supresión de objeto caducado cuando es la versión actual y no hay versiones no actuales.

Aunque el objeto no se haya quitado, StorageGRID se comporta como si la versión actual del objeto ya no estuviera disponible. Las solicitudes a ese objeto devuelven 404 NotFound. Sin embargo, debido a que los datos de objeto no actuales no se han eliminado, las solicitudes que especifican una versión no actual del objeto pueden tener éxito.

Para liberar espacio al eliminar objetos con versiones o para eliminar marcadores de borrado, utilice una de las siguientes opciones:

- **Solicitud de cliente S3**: Especifique el ID de versión de objeto en la solicitud de ELIMINACIÓN DE objeto S3 (`DELETE /object?versionId=ID`). Tenga en cuenta que esta solicitud sólo elimina copias de objetos para la versión especificada (las otras versiones todavía ocupan espacio).
- **Ciclo de vida del cucharón**: Utilice `NoncurrentVersionExpiration` acción en la configuración del ciclo de vida del bloque. Cuando se cumple el número de días sin currentDays especificado, StorageGRID elimina permanentemente todas las copias de las versiones de objetos no actuales. Estas versiones de objetos no se pueden recuperar.

  La `NewerNoncurrentVersions` La acción en la configuración del ciclo de vida del bloque especifica el número de versiones no actuales retenidas en un segmento S3 con versiones. Si hay más versiones no corrientes que `NewerNoncurrentVersions` Especifica, StorageGRID elimina las versiones anteriores cuando ha transcurrido el valor NoncurrentDays. La `NewerNoncurrentVersions` El umbral anula las reglas de ciclo de vida proporcionadas por ILM, lo que significa que un objeto no actual con una versión dentro del `NewerNoncurrentVersions` El umbral se conserva si ILM solicita su eliminación.

  Para eliminar marcadores de supresión de objetos caducados, utilice la `Expiration` acción con una de las siguientes etiquetas: `ExpiredObjectDeleteMarker`, `Days`, o. `Date`.

- **ILM**: "Clonar una política activa" Y añada dos reglas de ILM a la nueva política:
  - Primera regla: Utilice la hora no corriente como hora de referencia para que coincida con las versiones no actuales del objeto. Pulg "Paso 1 (introduzca detalles) del asistente Create an ILM Rule", Seleccione **Sí** para la pregunta, “¿Aplicar esta regla solo a versiones de objetos más antiguas (en

cubos S3 con control de versiones activado)?”

- Segunda regla: Utilice **tiempo de ingesta** para que coincida con la versión actual. La regla “Tiempo no corriente” debe aparecer en la política sobre la regla **Tiempo de ingesta**.

> ILM no se puede utilizar para quitar marcadores de eliminación de objetos actuales. Utilice una solicitud de cliente S3 o un ciclo de vida de cubo S3 para eliminar los marcadores de eliminación de objetos actuales.

- * Eliminar objetos en el cubo *: Utilice el administrador de inquilinos a. "suprimir todas las versiones de objetos", incluyendo marcadores de borrado, de un cubo.

  Cuando se elimina un objeto versionado, StorageGRID crea un marcador de eliminación de cero bytes como la versión actual del objeto. Todos los objetos y marcadores de supresión deben eliminarse para poder eliminar un depósito con versiones.

  - Los marcadores de eliminación creados en StorageGRID 11,7 o versiones anteriores solo se pueden eliminar mediante las solicitudes de clientes de S3; además, no se pueden eliminar mediante ILM, las reglas de ciclo de vida de los bloques ni la eliminación de objetos de las operaciones de bloque.
  - Elimine los marcadores de un bloque que se haya creado en StorageGRID 11,8 o versiones posteriores puede eliminar mediante ILM, las reglas de ciclo de vida de los bloques, la eliminación de objetos en operaciones de bloque o una eliminación explícita de clientes S3. Los marcadores de eliminación caducados en StorageGRID 11,8 o posterior se deben eliminar mediante reglas de ciclo de vida del bloque o mediante una solicitud de cliente explícita de S3 con un ID de versión especificado.

Información relacionada

- "USE LA API DE REST DE S3"
- "Ejemplo 4: Reglas de ILM y políticas para objetos con versiones de S3"

Crear y asignar grados de almacenamiento

Los grados de almacenamiento identifican el tipo de almacenamiento que utiliza un nodo de almacenamiento. Puede crear grados de almacenamiento si desea que las reglas de ILM coloquen determinados objetos en ciertos nodos de almacenamiento.

Antes de empezar

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

Acerca de esta tarea

Cuando instala StorageGRID por primera vez, el grado de almacenamiento **default** se asigna automáticamente a cada nodo de almacenamiento en su sistema. Como sea necesario, puede definir opcionalmente grados de almacenamiento personalizados y asignarlos a diferentes nodos de almacenamiento.

El uso de grados de almacenamiento personalizados permite crear pools de almacenamiento ILM que contienen solo un tipo específico de nodo de almacenamiento. Por ejemplo, quizás desee almacenar determinados objetos en los nodos de almacenamiento más rápidos, como los dispositivos de almacenamiento all-flash StorageGRID.

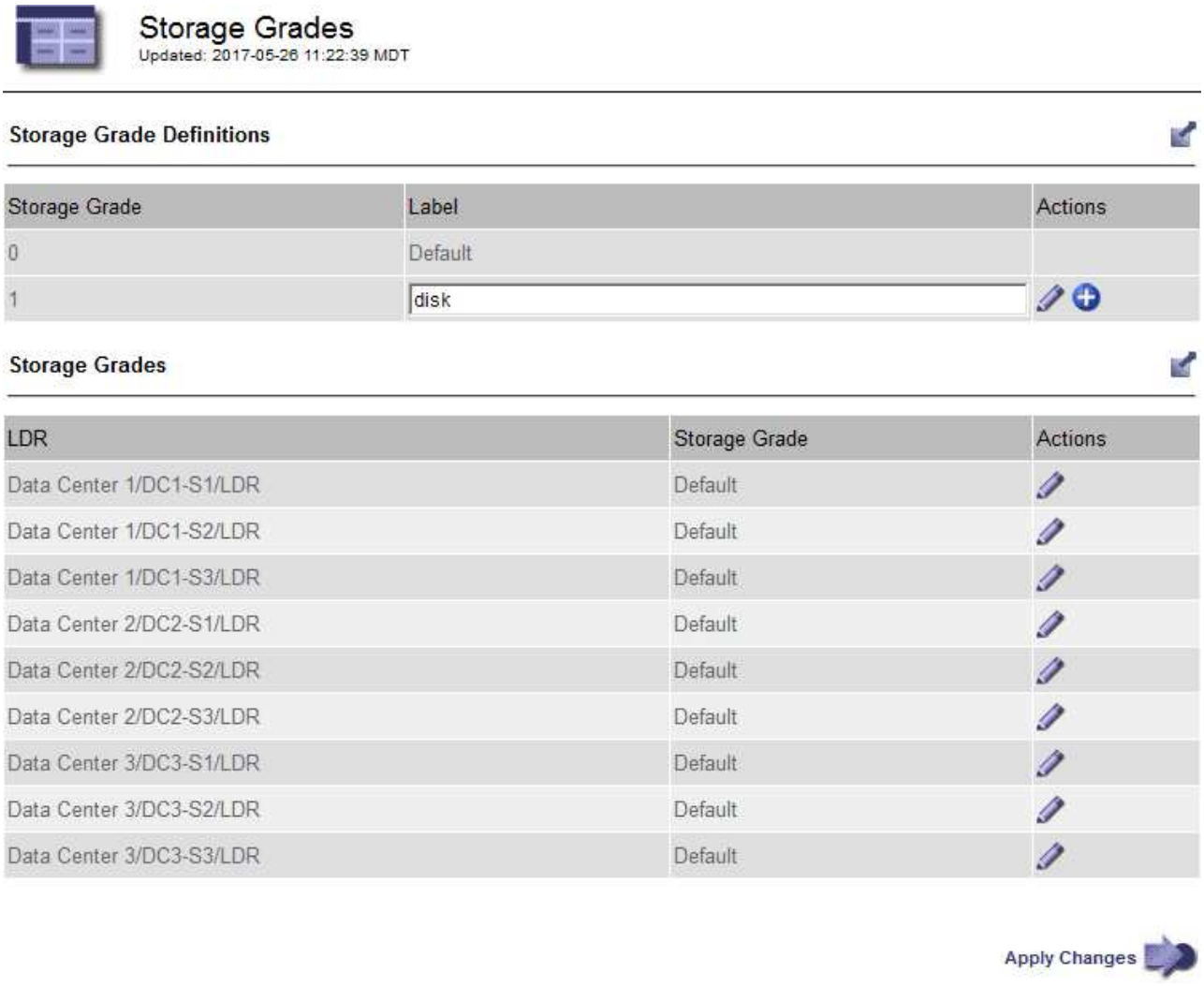
Los nodos de almacenamiento se pueden configurar durante la instalación de modo que solo contengan metadatos de objetos y no datos de objetos. Los nodos de almacenamiento solo de metadatos no se pueden asignar a un grado de almacenamiento. Para obtener más información, consulte "Tipos de nodos de almacenamiento".

Si el grado de almacenamiento no es una preocupación (por ejemplo, todos los nodos de almacenamiento son idénticos), puede omitir este procedimiento y usar la selección **Incluye todos los grados de almacenamiento** para el grado de almacenamiento cuando usted "cree pools de almacenamiento". El uso de esta selección garantiza que el pool de almacenamiento incluirá todos los nodos de almacenamiento en el sitio, independientemente de su grado de almacenamiento.

No cree más grados de almacenamiento de los necesarios. Por ejemplo, no cree una categoría de almacenamiento para cada nodo de almacenamiento. En su lugar, asigne cada grado de almacenamiento a dos o más nodos. Las leyes de almacenamiento asignadas a un solo nodo pueden provocar reversiones de ILM si ese nodo deja de estar disponible.

Pasos

1. Seleccione **ILM** > **grados de almacenamiento**.
2. Definir grados de almacenamiento personalizados:
   a. Para cada grado de almacenamiento personalizado que desee agregar, seleccione **Insertar** para agregar una fila.
   b. Introduzca una etiqueta descriptiva.



c. Seleccione **aplicar cambios**.

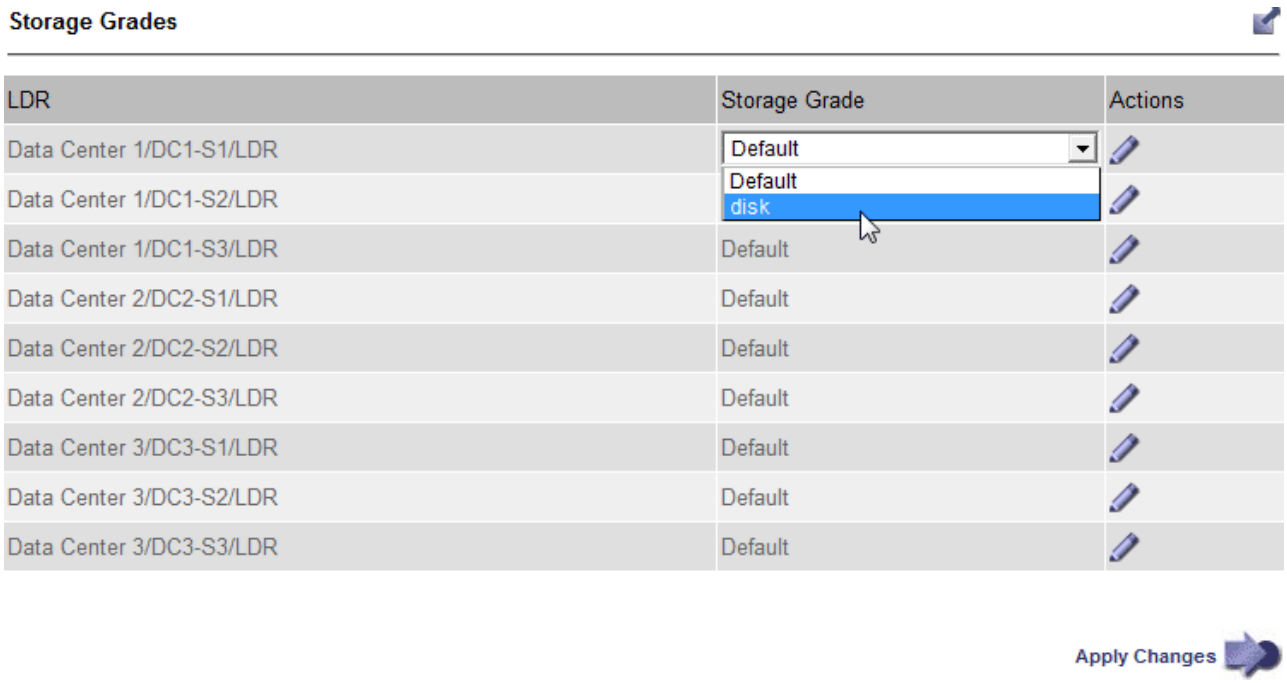
d. Opcionalmente, si necesita modificar una etiqueta guardada, seleccione **Editar** Y selecciona **Aplicar cambios**.

No se pueden eliminar los grados de almacenamiento.

3. Asigne nuevos grados de almacenamiento a los nodos de almacenamiento:

a. Localice el nodo de almacenamiento en la lista LDR y seleccione su icono **Editar** .

b. Seleccione el grado de almacenamiento adecuado en la lista.



Asigne un nivel de almacenamiento solo una vez a un nodo de almacenamiento determinado. Un nodo de almacenamiento recuperado del error mantiene el grado de almacenamiento anteriormente asignado. No cambie esta asignación después de activar la política de ILM. Si se modifica la asignación, los datos se almacenan según el nuevo grado de almacenamiento.

a. Seleccione **aplicar cambios**.

Usar pools de almacenamiento

¿Qué es un pool de almacenamiento?

Un pool de almacenamiento es una agrupación lógica de nodos de almacenamiento o nodos de archivado.

Al instalar StorageGRID, se crea automáticamente un pool de almacenamiento por sitio. Es posible configurar pools de almacenamiento adicionales según sea necesario para cumplir sus requisitos de almacenamiento.

Los nodos de almacenamiento se pueden configurar durante la instalación para que contengan datos de objetos y metadatos de objetos, o solo metadatos del objeto. Los nodos de almacenamiento solo de metadatos no se pueden usar en pools de almacenamiento. Para obtener más información, consulte "Tipos de nodos de almacenamiento".

La compatibilidad con los nodos de archivo está obsoleta y se eliminará en una versión futura. El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades.

Los pools de almacenamiento tienen dos atributos:

- **Grado de almacenamiento**: Para nodos de almacenamiento, el rendimiento relativo del almacenamiento de respaldo.

- **Sitio**: El centro de datos donde se almacenarán los objetos.

Los pools de almacenamiento se utilizan en las reglas de ILM para determinar dónde se almacenan los datos de objetos y el tipo de almacenamiento utilizado. Cuando se configuran las reglas de ILM para la replicación, se deben seleccionar uno o varios pools de almacenamiento que incluyen nodos de almacenamiento o nodos de archivado. Cuando se crean perfiles de código de borrado, se selecciona un pool de almacenamiento que incluye nodos de almacenamiento.

Directrices para crear pools de almacenamiento

Configura y utiliza pools de almacenamiento para protegerse frente a la pérdida de datos distribuyendo los datos entre varios sitios. Las copias replicadas y las copias con código de borrado requieren diferentes configuraciones de pools de almacenamiento.

Consulte "Ejemplos de habilitación de la protección contra pérdida de sitios mediante replicación y código de borrado".

Directrices para todos los pools de almacenamiento

- Mantenga las configuraciones del pool de almacenamiento de la forma más sencilla posible. No cree más pools de almacenamiento de los necesarios.
- Cree pools de almacenamiento con tantos nodos como sea posible. Cada pool de almacenamiento debe contener dos o más nodos. Un pool de almacenamiento con nodos insuficientes puede provocar registros de gestión del ciclo de vida de la información si un nodo deja de estar disponible.
- Evite crear o usar pools de almacenamiento que se solapen (contienen uno o varios de los mismos nodos). Si los pools de almacenamiento se solapan, es posible que se guarden más de una copia de datos de objetos en el mismo nodo.
- En general, no use el pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores) ni el sitio Todos los sitios. Estos elementos se actualizan automáticamente para incluir los nuevos sitios que agregue en una expansión, lo cual podría no ser el comportamiento que desea.

Directrices para los pools de almacenamiento utilizados para copias replicadas

- De protección contra pérdida de sitio con "replicación", especifique uno o más pools de almacenamiento específicos del sitio en la "Instrucciones de colocación para cada regla de ILM".

  Se crea automáticamente un pool de almacenamiento para cada sitio durante la instalación de StorageGRID.

  El uso de un pool de almacenamiento para cada sitio garantiza que las copias de objetos replicados se coloquen exactamente donde se espere (por ejemplo, una copia de cada objeto en cada sitio para la protección frente a pérdida de sitio).

- Si agrega un sitio en una expansión, cree un nuevo pool de almacenamiento que contenga solo el nuevo sitio. A continuación, "Actualice las reglas de ILM" para controlar qué objetos se almacenan en el nuevo sitio.
- Si la cantidad de copias es inferior a la cantidad de pools de almacenamiento, el sistema distribuye las copias para equilibrar el uso de disco entre los pools.
- Si los pools de almacenamiento se superponen (contienen los mismos nodos de almacenamiento), es posible que todas las copias del objeto se guarden en un solo sitio. Debe asegurarse de que los pools de almacenamiento seleccionados no contengan los mismos nodos de almacenamiento.

Directrices para los pools de almacenamiento utilizados para las copias con código de borrado

- De protección contra pérdida de sitio con "código de borrado", cree pools de almacenamiento que consten de al menos tres sitios. Si un pool de almacenamiento incluye solo dos sitios, no puede usar ese pool de almacenamiento para el código de borrado. No hay esquemas de codificación de borrado disponibles para un pool de almacenamiento que tenga dos ubicaciones.
- La cantidad de nodos de almacenamiento y sitios incluidos en el pool de almacenamiento determina cuáles "esquemas de código de borrado" están disponibles.
- Si es posible, un pool de almacenamiento debe incluir más de la cantidad mínima de nodos de almacenamiento necesarios para el esquema de codificación de borrado que seleccione. Por ejemplo, si utiliza un esquema de codificación de borrado 6+3, debe contar con al menos nueve nodos de almacenamiento. Sin embargo, se recomienda tener al menos un nodo de almacenamiento adicional por sitio.
- Distribuya nodos de almacenamiento en todos los sitios de la forma más equitativa posible. Por ejemplo, para admitir un esquema de codificación de borrado 6+3, configure un pool de almacenamiento que incluya al menos tres nodos de almacenamiento en tres sitios.
- Si tiene requisitos de alto rendimiento, no se recomienda el uso de un pool de almacenamiento que incluya varios sitios si la latencia de red entre los sitios es superior a 100 ms. A medida que aumenta la latencia, la velocidad a la que StorageGRID puede crear, colocar y recuperar fragmentos de objetos disminuye considerablemente debido al descenso del rendimiento de la red TCP.

  La disminución del rendimiento afecta a las tasas máximas alcanzables de ingesta y recuperación de objetos (cuando se seleccionan equilibrados o estrictos como comportamiento de procesamiento) o puede provocar retrasos en la cola de ILM (cuando se selecciona Dual commit como comportamiento de procesamiento). Consulte "Comportamiento de procesamiento de reglas de ILM".

  > Si su grid incluye solo un sitio, no podrá usar el pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores) o el sitio predeterminado Todos los sitios en un perfil de código de borrado. Este comportamiento evita que el perfil no sea válido si se agrega un segundo sitio.

- No se pueden usar nodos de archivo para datos con código de borrado.

Directrices para los pools de almacenamiento utilizados para copias archivadas

> La compatibilidad con los nodos de archivo está obsoleta y se eliminará en una versión futura. El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades.
>
> La opción Cloud Tiering - Simple Storage Service (S3) también queda obsoleta. Si está utilizando un nodo de archivado con esta opción, "Migre sus objetos a un pool de almacenamiento en la nube" en su lugar.
>
> Además, debe eliminar los nodos de archivado de la política de gestión de la vida útil de la información activa en StorageGRID 11,7 o versiones anteriores. La eliminación de datos de objetos almacenados en nodos de archivado simplificará las actualizaciones futuras. Consulte "Trabajar con reglas de ILM y políticas de ILM".

- No puede crear un pool de almacenamiento que incluya nodos de almacenamiento y nodos de archivado. Las copias archivadas requieren un pool de almacenamiento que sólo incluya nodos de archivado.

- Cuando se utiliza un pool de almacenamiento que incluye nodos de archivado, también se debe mantener al menos una copia replicada o con código de borrado en un pool de almacenamiento que incluya nodos de almacenamiento.
- Si la configuración global Bloqueo de objetos S3 está habilitada y está creando una regla de ILM compatible, no puede utilizar un pool de almacenamiento que incluya nodos de archivado. Consulte las instrucciones para gestionar objetos con el bloqueo de objetos de S3.
- Si el tipo de destino de un nodo de archivado es Cloud Tiering - simple Storage Service (S3), el nodo de archivado debe estar en su propio pool de almacenamiento.

Habilite la protección contra pérdida de sitio

Si la implementación de StorageGRID incluye más de un sitio, puede usar la replicación y el código de borrado con los pools de almacenamiento configurados correctamente para habilitar la protección contra pérdida de sitio.

La replicación y el código de borrado necesitan diferentes configuraciones de pools de almacenamiento:

- Para utilizar la replicación para la protección contra pérdida de sitio, utilice los pools de almacenamiento específicos de sitios que se crean automáticamente durante la instalación de StorageGRID. A continuación, cree reglas de ILM con "instrucciones de colocación" esto especifica varios pools de almacenamiento para que se coloque una copia de cada objeto en cada sitio.
- Para utilizar código de borrado para la protección contra pérdida de sitio, "cree pools de almacenamiento que consten de varios sitios". A continuación, cree reglas de ILM que usen un pool de almacenamiento que conste de varios sitios y cualquier esquema de código de borrado disponible.

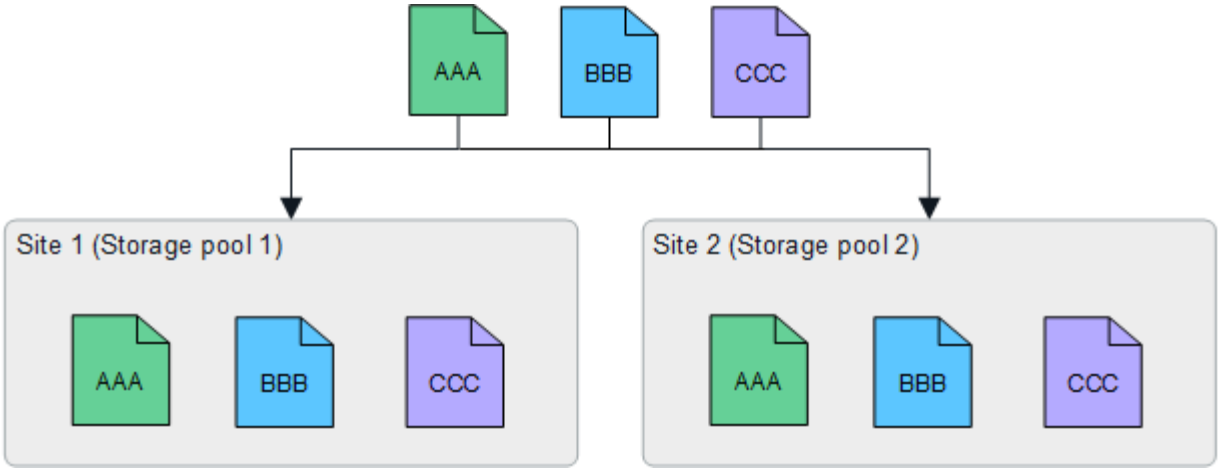
> ⚠ A la hora de configurar su implementación de StorageGRID para la protección contra pérdida de sitio, también debe tener en cuenta los efectos de "opciones de procesamiento" y.. "coherencia".

Ejemplo de replicación

De forma predeterminada, se crea un pool de almacenamiento para cada sitio durante la instalación de StorageGRID. Tener pools de almacenamiento compuestos solo por un sitio le permite configurar reglas de ILM que utilizan la replicación para la protección contra pérdida de sitio. En este ejemplo:

- El grupo de almacenamiento 1 contiene el sitio 1
- El grupo de almacenamiento 2 contiene el sitio 2
- La regla de ILM contiene dos ubicaciones:
  - Almacene objetos replicando la copia de 1 en el sitio 1
  - Almacene objetos replicando la copia de 1 en el sitio 2

Ubicaciones de reglas de ILM:



Si se pierde un sitio, hay copias de los objetos disponibles en el otro.

Ejemplo de código de borrado

Tener pools de almacenamiento compuestos por más de un sitio por pool de almacenamiento permite configurar reglas de ILM que utilicen código de borrado para la protección contra pérdida de sitio. En este ejemplo:

- El grupo de almacenamiento 1 contiene los sitios 1 a 3
- La regla de ILM contiene una ubicación: Almacenar objetos mediante código de borrado mediante un esquema EC 4+2 en el pool de almacenamiento 1, que contiene tres sitios

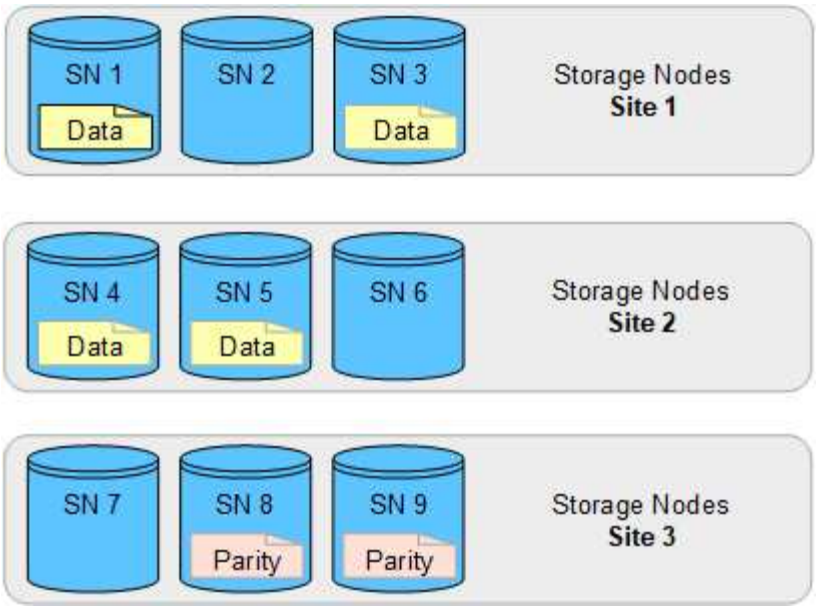
Ubicaciones de reglas de ILM:

En este ejemplo:

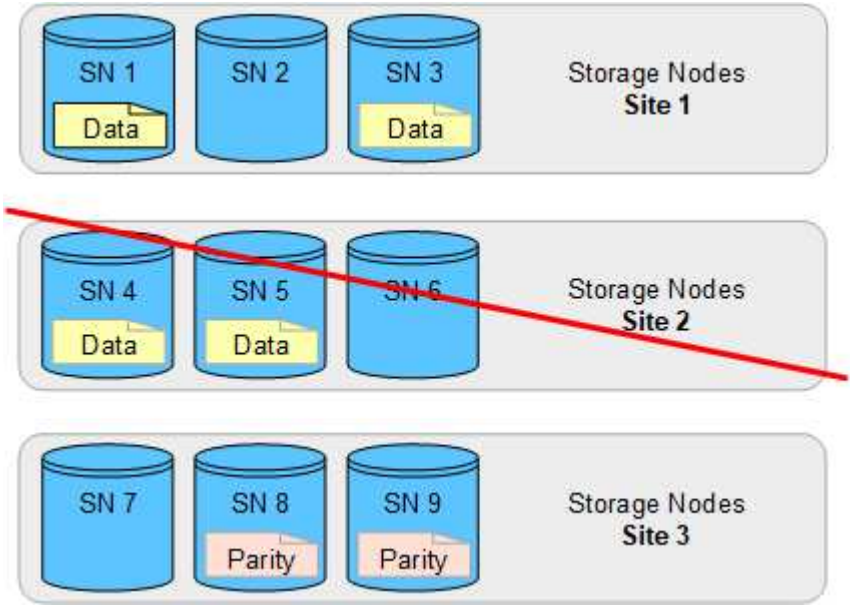
- La regla de ILM utiliza un esquema de código de borrado 4+2.
- Cada objeto se divide en cuatro fragmentos de datos iguales y dos fragmentos de paridad se calculan a partir de los datos del objeto.
- Cada uno de los seis fragmentos se almacena en un nodo diferente en tres sitios de centro de datos para proporcionar protección de datos ante fallos de nodos o pérdidas de sitios.

> Se permite el código de borrado en pools de almacenamiento que contienen cualquier número de sitios *excepto* dos sitios.

Regla de ILM que utiliza esquema de código de borrado 4+2:



Si se pierde un sitio, es posible recuperar los datos:



Cree un pool de almacenamiento

Se crean pools de almacenamiento para determinar dónde el sistema StorageGRID almacena los datos de objetos y el tipo de almacenamiento utilizado. Cada pool de almacenamiento incluye uno o más sitios y una o más calidades de almacenamiento.

> Cuando se instala StorageGRID 11,8 en un nuevo grid, se crean automáticamente pools de almacenamiento para cada sitio. Sin embargo, si instaló inicialmente StorageGRID 11,6 o una versión anterior, los pools de almacenamiento no se crean automáticamente para cada sitio.

Si desea crear pools de almacenamiento en cloud para almacenar datos de objetos fuera del sistema StorageGRID, consulte "Información sobre el uso de Cloud Storage Pools".

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Revisó las directrices para crear pools de almacenamiento.

Acerca de esta tarea

Los pools de almacenamiento determinan dónde se almacenan los datos de objeto. La cantidad de pools de almacenamiento que necesita depende del número de sitios del grid y de los tipos de copias que desee: Replicadas o codificadas por borrado.

- Para la replicación y la codificación de borrado a un solo sitio, cree un pool de almacenamiento para cada sitio. Por ejemplo, si desea almacenar copias de objetos replicados en tres sitios, cree tres pools de almacenamiento.
- Para la codificación de borrado en tres o más sitios, cree un pool de almacenamiento que incluya una entrada para cada sitio. Por ejemplo, si desea borrar objetos de código en tres sitios, cree un pool de almacenamiento.

> No incluya el sitio Todos los sitios en un pool de almacenamiento que se utilizará en un perfil de código de borrado. En su lugar, agregue una entrada independiente al pool de almacenamiento para cada sitio que almacene los datos con código de borrado. Consulte este paso por ejemplo.

- Si tiene más de un grado de almacenamiento, no cree un pool de almacenamiento que incluya diferentes grados de almacenamiento en un solo sitio. Consulte "Directrices para crear pools de almacenamiento".

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

   En la pestaña Storage Pools, se muestra todos los pools de almacenamiento definidos.

   > Para las instalaciones nuevas de StorageGRID 11,6 o versiones anteriores, el pool de almacenamiento Todos los nodos de almacenamiento se actualiza automáticamente cada vez que se añaden sitios de centros de datos nuevos. No utilice este pool en reglas de ILM.

2. Para crear una nueva agrupación de almacenamiento, seleccione **Crear**.
3. Introduzca un nombre único para el pool de almacenamiento. Utilice un nombre que sea fácil de identificar cuando configure perfiles de código de borrado y reglas de ILM.
4. En la lista desplegable **Sitio**, seleccione un sitio para esta agrupación de almacenamiento.

   Cuando selecciona un sitio, el número de nodos de almacenamiento y nodos de archivado de la tabla se actualiza automáticamente.

   En general, no utilice el sitio Todos los sitios en ningún pool de almacenamiento. Las reglas de ILM que utilizan un pool de almacenamiento All Sites colocan los objetos en cualquier sitio disponible, lo que le otorga menos control de la ubicación de los objetos. Además, un pool de almacenamiento All Sites utiliza inmediatamente los nodos de almacenamiento en un sitio nuevo, lo que podría no ser el comportamiento esperado.

5. En la lista desplegable **Storage grade**, seleccione el tipo de almacenamiento que se utilizará si una regla de ILM utiliza este grupo de almacenamiento.

   El grado de almacenamiento, *incluye todos los grados de almacenamiento*, incluye todos los nodos de

almacenamiento en el sitio seleccionado. El nivel de almacenamiento predeterminado de los nodos de archivado incluye todos los nodos de archivado en el sitio seleccionado. Si creó grados de almacenamiento adicionales para los nodos de almacenamiento del grid, estos se enumeran en el menú desplegable.

6. Si desea utilizar el grupo de almacenamiento en un perfil de codificación de borrado de varios sitios, seleccione **Agregar más nodos** para agregar una entrada para cada sitio al grupo de almacenamiento.

> Se le impide crear entradas duplicadas o crear un pool de almacenamiento que incluya tanto el grado de almacenamiento de los nodos de archivado como cualquier grado de almacenamiento que contenga nodos de almacenamiento.
>
> Se le advertirá si agrega más de una entrada con diferentes grados de almacenamiento para un sitio.

Para eliminar una entrada, seleccione el icono de eliminación ✕.

7. Cuando esté satisfecho con sus selecciones, seleccione **Guardar**.

El nuevo pool de almacenamiento se añadirá a la lista.

Ver detalles del pool de almacenamiento

Es posible ver los detalles de un pool de almacenamiento para determinar dónde se usa el pool de almacenamiento y para ver qué nodos y calidades de almacenamiento se incluyen.

Antes de empezar

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

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

La tabla Storage Pools incluye la siguiente información para cada pool de almacenamiento que incluye nodos de almacenamiento:

- **Nombre**: El nombre exclusivo para mostrar de la agrupación de almacenamiento.
- **Node count**: El número de nodos en el pool de almacenamiento.
- **Uso de almacenamiento**: El porcentaje del espacio total utilizable que se ha utilizado para los datos de objetos en este nodo. Este valor no incluye metadatos de objetos.
- * Capacidad total*: El tamaño del pool de almacenamiento, que equivale a la cantidad total de espacio utilizable para los datos de objetos para todos los nodos del pool de almacenamiento.
- **Uso de ILM**: Cómo se está utilizando actualmente el pool de almacenamiento. Es posible que un pool de almacenamiento no se utilice o que se utilice en una o más reglas de ILM, perfiles de código de borrado, o ambas.

> No se puede eliminar un pool de almacenamiento si se está utilizando.

2. Para ver los detalles de un pool de almacenamiento específico, seleccione su nombre.

Se muestra la página de detalles del pool de almacenamiento.

3. Vea la pestaña * Nodos * para obtener información sobre los nodos de almacenamiento o los nodos de archivo incluidos en el grupo de almacenamiento.

   En la tabla se incluye la siguiente información para cada nodo:

   - Nombre del nodo
   - Nombre del sitio
   - Grado de almacenamiento
   - Uso de almacenamiento: El porcentaje del espacio útil total para datos de objeto que se ha utilizado para el nodo de almacenamiento. Este campo no está visible para los pools de nodos de archivado.

   > El mismo valor de Uso de almacenamiento (%) también se muestra en el gráfico Almacenamiento usado - Datos de objeto para cada nodo de almacenamiento (seleccione **NODOS** > ***NODO de almacenamiento*** > **Almacenamiento**).

4. Seleccione la pestaña **ILM usage** para determinar si el pool de almacenamiento se está utilizando actualmente en reglas de ILM o perfiles de codificación de borrado.
5. Opcionalmente, vaya a la página de reglas de ILM * para conocer y administrar las reglas que utilizan el grupo de almacenamiento.

   Consulte "Instrucciones para trabajar con reglas de ILM".

Editar pool de almacenamiento

Es posible editar un pool de almacenamiento para cambiar su nombre o para actualizar los sitios y las calificaciones de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Ha revisado el "directrices para crear pools de almacenamiento".
- Si prevé editar un pool de almacenamiento utilizado por una regla en la política de ILM activa, habrá pensado en cómo afectarán los cambios a la ubicación de los datos de los objetos.

Acerca de esta tarea

Si va a añadir un nuevo sitio o nivel de almacenamiento a un pool de almacenamiento que se usa en la política de ILM activa, tenga en cuenta que los nodos de almacenamiento del sitio nuevo o el grado de almacenamiento no se utilizarán automáticamente. Para forzar a StorageGRID a utilizar un sitio o nivel de almacenamiento nuevo, debe activar una nueva política de ILM después de guardar el pool de almacenamiento editado.

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.
2. Seleccione la casilla de comprobación del pool de almacenamiento que desea editar.

   No se puede editar el pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y versiones anteriores).

3. Seleccione **Editar**.
4. Según sea necesario, cambie el nombre del pool de almacenamiento.
5. Según sea necesario, seleccione otros sitios y grados de almacenamiento.

> Se le impide cambiar el sitio o el grado de almacenamiento si el grupo de almacenamiento se utiliza en un perfil de código de borrado y el cambio provocaría que el esquema de código de borrado dejara de ser válido. Por ejemplo, si un pool de almacenamiento utilizado en un perfil de código de borrado incluye actualmente un grado de almacenamiento con un solo sitio, se le impide utilizar un grado de almacenamiento con dos sitios, ya que el cambio haría que el esquema de código de borrado no sea válido.

6. Seleccione **Guardar**.

Después de terminar

Si añadió un nuevo sitio o grado de almacenamiento a un pool de almacenamiento usado en la política de gestión del ciclo de vida de la información activa, active una nueva política de gestión del ciclo de vida de la información para forzar a StorageGRID a usar el nuevo sitio o el grado de almacenamiento. Por ejemplo, Clone la política de ILM existente y luego active el clon. Consulte "Trabaje con las reglas de ILM y las políticas de ILM".

Quitar un pool de almacenamiento

Es posible quitar un pool de almacenamiento que no se está usando.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.
2. Revise la columna Uso de ILM de la tabla para determinar si se puede quitar el pool de almacenamiento.

   No se puede quitar un pool de almacenamiento si se está utilizando en una regla de gestión de la vida útil de la información o en un perfil de código de borrado. Según sea necesario, seleccione ***storage pool name*** > **ILM usage** para determinar dónde se utiliza el pool de almacenamiento.

3. Si el pool de almacenamiento que desea quitar no se está utilizando, seleccione la casilla de comprobación.
4. Seleccione **Quitar**.
5. Seleccione **OK**.

Utilice Cloud Storage Pools

¿Qué es un pool de almacenamiento en cloud?

Un pool de almacenamiento en cloud permite utilizar ILM para mover datos de objetos fuera de su sistema StorageGRID. Por ejemplo, es posible que desee mover objetos a los que se accede con poca frecuencia a un almacenamiento en cloud de bajo coste, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o el nivel de acceso

de archivado en el almacenamiento de Microsoft Azure Blob. O bien, puede que quiera mantener un backup en cloud de objetos de StorageGRID para mejorar la recuperación ante desastres.

Desde el punto de vista de la gestión del ciclo de vida de la información, un pool de almacenamiento en cloud es similar al de un pool de almacenamiento. Para almacenar objetos en cualquiera de las ubicaciones, debe seleccionar el pool al crear las instrucciones de ubicación para una regla de ILM. Sin embargo, si bien los pools de almacenamiento constan de nodos de almacenamiento o nodos de archivado dentro del sistema StorageGRID, un pool de almacenamiento en cloud consta de un bloque externo (S3) o un contenedor (almacenamiento blob de Azure).

> El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API S3 está obsoleto y ha sido reemplazado por pools de almacenamiento en la nube de ILM, que ofrecen más funcionalidad. Si actualmente está utilizando un nodo de archivado con la opción Cloud Tiering - Simple Storage Service (S3), "Migre sus objetos a un pool de almacenamiento en la nube" en su lugar.

La tabla compara los pools de almacenamiento con los pools de almacenamiento en cloud y muestra las similitudes y las diferencias a alto nivel.

	Del banco de almacenamiento	**Pool de almacenamiento en cloud**
¿Cómo se crea?	Uso de la opción **ILM** > **agrupaciones de almacenamiento** en Grid Manager.	Usando la opción **ILM** > **Storage Pools** > **Cloud Storage Pools** en Grid Manager. Debe configurar el bloque o contenedor externo para poder crear el Cloud Storage Pool.
¿Cuántos pools se pueden crear?	Ilimitada.	Hasta 10.

	Del banco de almacenamiento	Pool de almacenamiento en cloud
¿Dónde se almacenan los objetos?	En uno o más nodos de almacenamiento o nodos de archivado dentro de StorageGRID.	En un bloque de Amazon S3, un contenedor de almacenamiento de Azure Blob o Google Cloud externo al sistema StorageGRID. Si Cloud Storage Pool es un bloque de Amazon S3: • Opcionalmente, se puede configurar un ciclo de vida de bloque para pasar los objetos a un almacenamiento a largo plazo de bajo coste, como Amazon S3 Glacier o S3 Glacier Deep Archive. El sistema de almacenamiento externo debe admitir la clase de almacenamiento Glacier y la API S3 RestoreObject. • Puede crear pools de almacenamiento en el cloud para usarlos con los servicios de cloud comercial (C2S) de AWS, compatibles con la región secreta de AWS. Si Cloud Storage Pool es un contenedor de almacenamiento de Azure Blob, StorageGRID realiza la transición del objeto al nivel de archivado. **Nota:** En general, no configure la gestión del ciclo de vida del almacenamiento de Azure Blob para el contenedor utilizado para un Cloud Storage Pool. Las operaciones de RestoreObject en objetos del Cloud Storage Pool pueden verse afectadas por el ciclo de vida configurado.
¿Qué controla la ubicación de objetos?	Una regla de ILM en las políticas de ILM activas.	Una regla de ILM en las políticas de ILM activas.
¿Qué método de protección de datos se utiliza?	Codificación de replicación o borrado.	Replicación.
¿Cuántas copias de cada objeto se permiten?	Múltiples.	Una copia en el pool de almacenamiento cloud y, opcionalmente, una o varias copias en StorageGRID. **Nota:** No puedes almacenar un objeto en más de un Pool de almacenamiento en la nube en un momento dado.
¿Cuáles son las ventajas?	Los objetos son accesibles rápidamente en cualquier momento.	Almacenamiento de bajo coste.

	Del banco de almacenamiento	Pool de almacenamiento en cloud
		Nota: Los datos de FabricPool no se pueden organizar en niveles en los grupos de almacenamiento en la nube. Los objetos con bloqueo de objetos S3 activado no se pueden colocar en pools de Cloud Storage.

Ciclo de vida de un objeto de Cloud Storage Pool

Antes de implementar Cloud Storage Pools, revise el ciclo de vida de los objetos que se almacenan en cada tipo de pool de almacenamiento en cloud.

S3: Ciclo de vida de un objeto de Cloud Storage Pool

Los pasos describen las etapas del ciclo de vida de un objeto que se almacena en un pool de almacenamiento en cloud S3.

> "Glacier" se refiere tanto a la clase de almacenamiento Glacier como a la clase de almacenamiento Glacier Deep Archive, con una excepción: La clase de almacenamiento Glacier Deep Archive no admite el nivel de restauración acelerada. Solo se admite la recuperación masiva o estándar.

> Google Cloud Platform (GCP) admite la recuperación de objetos de un almacenamiento a largo plazo sin necesidad de una operación POSTERIOR a la restauración.

1. **Objeto almacenado en StorageGRID**

   Para iniciar el ciclo de vida, una aplicación cliente almacena un objeto en StorageGRID.

2. **Objeto movido a S3 Cloud Storage Pool**
   - Cuando el objeto coincide con una regla de ILM que utiliza un S3 Cloud Storage Pool como ubicación, StorageGRID mueve el objeto al bloque de S3 externo especificado por el Cloud Storage Pool.
   - Cuando el objeto se ha movido al pool de almacenamiento en la nube de S3, la aplicación cliente puede recuperarlo mediante una solicitud GetObject de S3 de StorageGRID, a menos que el objeto se haya trasladado al almacenamiento de Glacier.
3. **Objeto que ha pasado a Glacier (estado no recuperable)**
   - Opcionalmente, se puede cambiar el objeto al almacenamiento Glacier. Por ejemplo, el bloque externo de S3 puede utilizar la configuración del ciclo de vida para mover un objeto al almacenamiento Glacier de inmediato o después de varios días.

     > Si desea realizar la transición de objetos, debe crear una configuración del ciclo de vida para el bucket externo de S3, y debe usar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y sea compatible con la API S3 RestoreObject.

> No utilice Cloud Storage Pools para objetos que han ingerido los clientes Swift. SWIFT no admite las solicitudes RestoreObject, por lo que StorageGRID no podrá recuperar ningún objeto Swift que se haya realizado la transición al almacenamiento S3 Glacier. La emisión de una solicitud de objeto GET de Swift para recuperar estos objetos fallará (403 Prohibido).

- Durante la transición, la aplicación cliente puede utilizar una solicitud S3 HeadObject para supervisar el estado del objeto.

4. **Objeto restaurado desde el almacenamiento Glacier**

   Si se ha realizado la transición de un objeto al almacenamiento de Glacier, la aplicación cliente puede emitir una solicitud S3 RestoreObject para restaurar una copia que se pueda recuperar en el Cloud Storage Pool S3. La solicitud especifica cuántos días debe estar disponible la copia en el Cloud Storage Pool y en el nivel de acceso a datos que se usará en la operación de restauración (acelerada, estándar o masiva). Cuando se alcanza la fecha de vencimiento de la copia recuperable, la copia se devuelve automáticamente a un estado no recuperable.

   > Si también existen una o varias copias del objeto en los nodos de almacenamiento de StorageGRID, no es necesario restaurar el objeto desde Glacier emitiendo una solicitud RestoreObject. En su lugar, la copia local se puede recuperar directamente mediante una solicitud GetObject.

5. **Objeto recuperado**

   Una vez que se ha restaurado un objeto, la aplicación cliente puede emitir una solicitud GetObject para recuperar el objeto restaurado.

Azure: Ciclo de vida de un objeto de Cloud Storage Pool

Los pasos describen las etapas del ciclo de vida de un objeto que se almacena en un pool de almacenamiento en cloud de Azure.

1. **Objeto almacenado en StorageGRID**

   Para iniciar el ciclo de vida, una aplicación cliente almacena un objeto en StorageGRID.

2. **Objeto movido a Azure Cloud Storage Pool**

   Cuando el objeto coincide con una regla de gestión de la vida útil de la información que utiliza un pool de almacenamiento en cloud de Azure como ubicación, StorageGRID mueve el objeto al contenedor de almacenamiento externo de Azure Blob especificado por el pool de almacenamiento en cloud.

   > No utilice Cloud Storage Pools para objetos que han ingerido los clientes Swift. SWIFT no admite las solicitudes RestoreObject, por lo que StorageGRID no podrá recuperar ningún objeto Swift que se haya realizado la transición al nivel de archivado de almacenamiento de Azure Blob. La emisión de una solicitud de objeto GET de Swift para recuperar estos objetos fallará (403 Prohibido).

3. **Objeto que ha pasado a la capa de archivado (estado no recuperable)**

   Inmediatamente después de mover el objeto a Azure Cloud Storage Pool, StorageGRID realiza una transición automática del objeto al nivel de archivado de almacenamiento de Azure Blob.

4. **Objeto restaurado desde el nivel de archivo**

   Si un objeto se ha trasladado al nivel de archivado, la aplicación cliente puede emitir una solicitud S3 RestoreObject para restaurar una copia recuperable en Azure Cloud Storage Pool.

   Cuando StorageGRID recibe el RestoreObject, hace la transición temporal del objeto al nivel Cool de almacenamiento de Azure Blob. Tan pronto como se alcanza la fecha de caducidad en la solicitud RestoreObject, StorageGRID devuelve el objeto al nivel Archive.

   > Si también existen una o varias copias del objeto en los nodos de almacenamiento de StorageGRID, no es necesario restaurar el objeto desde el nivel de acceso de archivado emitiendo una solicitud RestoreObject. En su lugar, la copia local se puede recuperar directamente mediante una solicitud GetObject.

5. **Objeto recuperado**

   Una vez que un objeto se ha restaurado en Azure Cloud Storage Pool, la aplicación cliente puede emitir una solicitud GetObject para recuperar el objeto restaurado.

Información relacionada

"USE LA API DE REST DE S3"

Cuándo usar Cloud Storage Pools

Con Cloud Storage Pools, puede crear un backup o organizar los datos en niveles en una ubicación externa. Además, puede hacer backups o organizar los datos en más de un cloud.

Backup de datos de StorageGRID en ubicaciones externas

Puede usar un pool de almacenamiento en cloud para realizar backup de objetos StorageGRID en una ubicación externa.

Si no se puede acceder a las copias en StorageGRID, se pueden utilizar los datos de objetos en el pool de almacenamiento en cloud para atender las solicitudes de los clientes. Sin embargo, es posible que necesite emitir una solicitud S3 RestoreObject para acceder a la copia del objeto de backup en Cloud Storage Pool.

Los datos del objeto en un pool de almacenamiento en cloud también se pueden utilizar para recuperar los datos perdidos de StorageGRID debido a un fallo del volumen de almacenamiento o del nodo de almacenamiento. Si la única copia restante de un objeto se encuentra en un pool de almacenamiento en el cloud, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.

Para implantar una solución de backup:

1. Cree un único pool de almacenamiento en el cloud.
2. Configure una regla de ILM que almacene copias de objetos en los nodos de almacenamiento de forma simultánea (como copias replicadas o codificadas por borrado) y una única copia de objetos en el Cloud Storage Pool.
3. Añada la regla a la política de ILM. A continuación, simule y active la directiva.

Organice los datos en niveles desde StorageGRID a ubicaciones externas

Puede utilizar un pool de almacenamiento en cloud para almacenar objetos fuera del sistema StorageGRID. Por ejemplo, supongamos que tiene un gran número de objetos que necesita retener, pero espera tener acceso a esos objetos rara vez, si es que alguna vez. Puede usar un pool de almacenamiento en cloud para organizar los objetos en niveles para reducir el almacenamiento y liberar espacio en StorageGRID.

Para implementar una solución por niveles:

1. Cree un único pool de almacenamiento en el cloud.
2. Configure una regla de ILM que mueva objetos que no se usen frecuentemente desde nodos de almacenamiento a Cloud Storage Pool.
3. Añada la regla a la política de ILM. A continuación, simule y active la directiva.

Mantenga varios extremos de cloud

Puede configurar varios extremos de Cloud Storage Pool si desea organizar en niveles o realizar backups de datos de objetos en más de una nube. Los filtros de las reglas de ILM permiten especificar los objetos que se almacenan en cada Cloud Storage Pool. Por ejemplo, es posible que desee almacenar objetos de algunos clientes o buckets en Amazon S3 Glacier y objetos de otros inquilinos o buckets en el almacenamiento de Azure Blob. O bien, es posible que desee mover datos entre el almacenamiento de Amazon S3 Glacier y Azure Blob.

> Cuando se utilizan varios extremos de Cloud Storage Pool, tenga en cuenta que un objeto se puede almacenar solo en un Cloud Storage Pool cada vez.

Para implementar varios extremos de cloud:

1. Cree hasta 10 pools de almacenamiento en cloud.
2. Configure las reglas de ILM para almacenar los datos de los objetos adecuados en el momento adecuado en cada pool de almacenamiento de cloud. Por ejemplo, almacene objetos del bloque A en el Cloud Storage Pool A y almacene objetos del bloque B en el Cloud Storage Pool B. O bien, almacene objetos en el pool de almacenamiento en cloud A durante cierto tiempo y muévalos a Cloud Storage Pool B.
3. Añada las reglas a la política de ILM. A continuación, simule y active la directiva.

Consideraciones para Cloud Storage Pools

Si planea utilizar un pool de almacenamiento en cloud para mover objetos desde el sistema StorageGRID, debe revisar las consideraciones que hay que tener en cuenta a la hora de configurar y utilizar pools de almacenamiento en cloud.

Consideraciones generales

- En general, el almacenamiento de archivado en cloud, como el almacenamiento de Amazon S3 Glacier o Azure Blob, es un lugar económico para almacenar datos de objetos. No obstante, los costes para recuperar datos del almacenamiento de archivado en el cloud son relativamente altos. Para alcanzar el coste general más bajo, debe tener en cuenta cuándo y con qué frecuencia accederá a los objetos en el pool de almacenamiento en cloud. El uso de un Cloud Storage Pool solo se recomienda para el contenido al que espera acceder con poca frecuencia.
- No utilice Cloud Storage Pools para objetos que han ingerido los clientes Swift. SWIFT no admite las solicitudes RestoreObject, por lo que StorageGRID no podrá recuperar ningún objeto Swift que se haya realizado la transición al almacenamiento S3 Glacier o al nivel de archivado de almacenamiento de Azure

Blob. La emisión de una solicitud de objeto GET de Swift para recuperar estos objetos fallará (403 Prohibido).

- No se puede usar Cloud Storage Pools con FabricPool debido a la latencia añadida de recuperar un objeto del destino de Cloud Storage Pool.
- Los objetos con bloqueo de objetos S3 activado no se pueden colocar en pools de Cloud Storage.
- Si el bucket S3 de destino para un pool de almacenamiento en la nube tiene S3 Object Lock habilitado, el intento de configurar la replicación de bucket (PutBucketReplication) fallará con un error ACCESSDENIED.

Consideraciones sobre los puertos utilizados para Cloud Storage Pools

Para garantizar que las reglas de ILM puedan mover objetos desde y hacia el Cloud Storage Pool especificado, debe configurar la red o las redes que contienen los nodos de almacenamiento del sistema. Debe asegurarse de que los siguientes puertos puedan comunicarse con el pool de almacenamiento en cloud.

De forma predeterminada, los pools de almacenamiento en cloud utilizan los puertos siguientes:

- **80**: Para los URI de punto final que comienzan con http
- **443**: Para los URI de punto final que comienzan con https

Es posible especificar un puerto diferente cuando se crea o se edita un pool de almacenamiento en el cloud.

Si utiliza un servidor proxy no transparente, también debe hacerlo "configurar un proxy de almacenamiento" para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

Consideraciones sobre los costos

El acceso al almacenamiento en el cloud por medio de un pool de almacenamiento en el cloud requiere conectividad de red al cloud. Debe tener en cuenta el coste de la infraestructura de red que utilizará para acceder al cloud y aprovisionarlo adecuadamente, en función de la cantidad de datos que espera mover entre StorageGRID y el cloud con el pool de almacenamiento en cloud.

Cuando StorageGRID se conecta al extremo externo de Flash Storage Pool, emite distintas solicitudes para supervisar la conectividad y garantizar que puede ejecutar las operaciones requeridas. Aunque se asociarán algunos costes adicionales con estas solicitudes, el coste de supervisar un Cloud Storage Pool solo debería ser una pequeña fracción del coste total de almacenar objetos en S3 o Azure.

Es posible que deba incurrir en costes más significativos si necesita mover objetos desde un extremo de almacenamiento en cloud externo a StorageGRID. Los objetos pueden moverse de nuevo a StorageGRID en cualquiera de estos casos:

- La única copia del objeto se encuentra en un Pool de almacenamiento en cloud y en su lugar decide almacenar el objeto en StorageGRID. En este caso, volverá a configurar las reglas y políticas de ILM. Cuando se produce la evaluación de la gestión de la vida útil de la información, StorageGRID emite varias solicitudes para recuperar el objeto desde el pool de almacenamiento en cloud. A continuación, StorageGRID crea el número especificado de copias replicadas o codificadas de borrado en forma local. Cuando el objeto se mueve de nuevo a StorageGRID, se elimina la copia en el pool de almacenamiento en el cloud.
- Se pierden los objetos debido a un fallo en el nodo de almacenamiento. Si la única copia restante de un objeto se encuentra en un pool de almacenamiento en el cloud, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.

Cuando se devuelven objetos a StorageGRID desde un pool de almacenamiento en el cloud, StorageGRID emite varias solicitudes al extremo de pool de almacenamiento en cloud para cada objeto. Antes de mover un gran número de objetos, póngase en contacto con el soporte técnico para obtener ayuda a la hora de calcular el plazo de tiempo y los costes asociados.

S3: Permisos necesarios para el bloque de Cloud Storage Pool

La política de bloque para el bloque externo de S3 usado para un Cloud Storage Pool debe otorgar permiso StorageGRID para mover un objeto al bloque, obtener el estado de un objeto, restaurar un objeto del almacenamiento Glacier cuando sea necesario y más. Lo ideal es que StorageGRID tenga acceso de control total al cucharón (`s3:*`); sin embargo, si esto no es posible, la directiva bucket debe conceder los siguientes permisos S3 a StorageGRID:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: Consideraciones para el ciclo de vida del bloque externo

El movimiento de objetos entre StorageGRID y el bloque de S3 externo especificado en el pool de almacenamiento en cloud está controlado por las reglas de ILM y las políticas de ILM activas en StorageGRID. Por el contrario, la configuración del ciclo de vida de ese bloque controla la transición de objetos desde el bloque S3 externo especificado en Cloud Storage Pool a Amazon S3 Glacier o S3 Glacier Deep Archive (o a una solución de almacenamiento que implementa la clase de almacenamiento Glacier).

Si desea realizar la transición de objetos desde Cloud Storage Pool, debe crear la configuración de ciclo de vida adecuada en el depósito externo de S3, y debe utilizar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y admita la API S3 RestoreObject.

Por ejemplo, supongamos que desea que se realice inmediatamente la transición de todos los objetos movidos de StorageGRID al pool de almacenamiento en cloud al almacenamiento Amazon S3 Glacier. Debe crear una configuración de ciclo de vida en el bloque S3 externo que especifique una única acción (**transición**) de la siguiente forma:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Esta regla transitaría todos los objetos de bloques al Amazon S3 Glacier el día en que se crearon (es decir, el día en que se movieron de StorageGRID a la agrupación de almacenamiento en cloud).

> Al configurar el ciclo de vida del cucharón externo, no utilice nunca acciones **Expiración** para definir cuándo caducan los objetos. Las acciones de caducidad hacen que el sistema de almacenamiento externo elimine los objetos caducados. Si más adelante intenta acceder a un objeto caducado de StorageGRID, no se encuentra el objeto eliminado.

Si desea realizar la transición de objetos del Cloud Storage Pool a S3 Glacier Deep Archive (en lugar de Amazon S3 Glacier), especifique `<StorageClass>DEEP_ARCHIVE</StorageClass>` en el ciclo de vida de la cuchara. Sin embargo, tenga en cuenta que no puede utilizar el `Expedited` organice en niveles los objetos de S3 Glacier Deep Archive.

Azure: Consideraciones para el nivel de acceso

Al configurar una cuenta de almacenamiento de Azure, puede configurar el nivel de acceso predeterminado en Hot o Cool. Al crear una cuenta de almacenamiento para usar con un pool de almacenamiento en el cloud, se debe usar el nivel de función como nivel predeterminado. Aunque StorageGRID establece inmediatamente el nivel Archivado cuando se mueven objetos al pool de almacenamiento en el cloud, el uso de una configuración predeterminada de caliente garantiza que no se cobrará una tarifa de eliminación anticipada de los objetos que se quitan del nivel de refrigeración antes del mínimo de 30 días.

Azure: Gestión del ciclo de vida no compatible

No use gestión del ciclo de vida del almacenamiento de Azure Blob para el contenedor que se usa con un pool de almacenamiento en cloud. Las operaciones de ciclo de vida pueden interferir en las operaciones de Cloud Storage Pool.

Información relacionada

- "Cree un pool de almacenamiento en el cloud"

Compare los pools de almacenamiento en cloud y la replicación de CloudMirror

Cuando comience a usar pools de almacenamiento en cloud, podría ser útil comprender las similitudes y diferencias entre los pools de almacenamiento en cloud y el servicio de

replicación CloudMirror de StorageGRID.

	Pool de almacenamiento en cloud	Servicio de replicación de CloudMirror
¿Cuál es el objetivo principal?	Actúa como destino de archivado. La copia de objeto del Pool de almacenamiento en cloud puede ser la única copia del objeto, o bien puede ser una copia adicional. Esto es, en lugar de conservar dos copias en el sitio, puede conservar una copia dentro de StorageGRID y enviar una copia al Pool de almacenamiento en cloud.	Permite que un inquilino replique automáticamente objetos de un bloque en StorageGRID (origen) a un bloque S3 externo (destino). Crea una copia independiente de un objeto en una infraestructura S3 independiente.
¿Cómo se configura?	Se definen del mismo modo que los pools de almacenamiento, mediante Grid Manager o la API de gestión de grid. Se puede seleccionar como ubicación en una regla de ILM. Si bien un pool de almacenamiento consta de un grupo de nodos de almacenamiento, un pool de almacenamiento en el cloud se define mediante un extremo remoto de S3 o Azure (dirección IP, credenciales, etc.).	Un usuario inquilino "Configura la replicación de CloudMirror" Al definir un extremo de CloudMirror (dirección IP, credenciales, etc.) con el administrador de inquilinos o la API de S3. Una vez configurado el extremo de CloudMirror, se puede configurar cualquier bloque que sea propiedad de esa cuenta de inquilino para que apunte al extremo de CloudMirror.
¿Quién es responsable de su configuración ?	Normalmente, un administrador de grid	Normalmente, un usuario inquilino
¿Cuál es el destino?	• Cualquier infraestructura compatible de S3 (incluido Amazon S3) • Nivel de Azure Blob Archive • Google Cloud Platform (GCP)	• Cualquier infraestructura compatible de S3 (incluido Amazon S3) • Google Cloud Platform (GCP)
¿Qué hace que los objetos se muevan al destino?	Una o más reglas de ILM en las políticas de ILM activas. Las reglas de ILM definen los objetos que StorageGRID se mueve al Cloud Storage Pool y cuándo se mueven los objetos.	Acción de ingerir un nuevo objeto en un depósito de origen que se haya configurado con un punto final de CloudMirror. Los objetos que existían en el bloque de origen antes de que se configurara con el extremo de CloudMirror no se replican, a menos que se modifiquen.

	Pool de almacenamiento en cloud	Servicio de replicación de CloudMirror
¿Cómo se recuperan los objetos?	Las aplicaciones deben solicitar a StorageGRID para recuperar objetos que se hayan movido a un pool de almacenamiento en cloud. Si se transición la única copia de un objeto al almacenamiento de archivado, StorageGRID gestiona el proceso de restauración del objeto para que se pueda recuperar.	Debido a que la copia duplicada en el bloque de destino es una copia independiente, las aplicaciones pueden recuperar el objeto realizando solicitudes ya sea a StorageGRID o al destino de S3. Por ejemplo, supongamos que usa la replicación de CloudMirror para reflejar objetos en una organización asociada. El partner puede utilizar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario usar StorageGRID.
¿Puede leer directamente desde el destino?	No StorageGRID gestiona los objetos movidos a un pool de almacenamiento en cloud. Las solicitudes de lectura deben dirigirse a StorageGRID (y StorageGRID será responsable de la recuperación del pool de almacenamiento en cloud).	Sí, porque la copia duplicada es una copia independiente.
¿Qué ocurre si un objeto se elimina del origen?	El objeto también se elimina del Cloud Storage Pool.	La acción de eliminación no se replica. Un objeto eliminado ya no existe en el bloque StorageGRID, pero sigue existiendo en el bloque de destino. Del mismo modo, los objetos del bloque de destino se pueden eliminar sin que ello afecte al origen.
¿Cómo accede a los objetos tras un desastre (el sistema StorageGRID no está operativo)?	Los nodos StorageGRID con errores deben recuperarse. Durante este proceso, es posible que se restauren copias de los objetos replicados con las copias del Cloud Storage Pool.	Las copias de objetos en el destino de CloudMirror son independientes de la StorageGRID, por lo que se podrá acceder a ellas directamente antes de que se recuperen los nodos StorageGRID.

Cree un pool de almacenamiento en el cloud

Un Cloud Storage Pool especifica un único bloque externo de Amazon S3 u otro proveedor compatible con S3 o contenedor de almacenamiento de Azure Blob.

Al crear un grupo de almacenamiento en la nube, se especifica el nombre y la ubicación del contenedor o depósito externo que StorageGRID usará para almacenar objetos, el tipo de proveedor de nube (almacenamiento de Amazon S3/GCP o Azure Blob) y la información que StorageGRID necesita para acceder al contenedor o depósito externo.

StorageGRID valida el pool de almacenamiento en cloud tan pronto como lo guarde, por lo que debe asegurarse de que existe el bloque o contenedor especificado en el pool de almacenamiento en el cloud y sea posible acceder a él.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".
- Ha revisado el "Consideraciones para Cloud Storage Pools".
- Ya existe el depósito o contenedor externo al que hace referencia Cloud Storage Pool y conoce su nombre y ubicación.
- Para acceder al depósito o contenedor, tiene la siguiente información para el tipo de autenticación que elegirá:

  Tecla de acceso S3

  Para el cubo externo S3

  - El ID de clave de acceso de la cuenta que posee el bloque externo.
  - La clave de acceso secreta asociada.

  Como alternativa, puede especificar Anonymous para el tipo de autenticación.

  Portal de acceso C2S

  Para servicios en la nube comercial (C2S) S3 SERVICE

  Tiene lo siguiente:

  - URL completa que StorageGRID utilizará para obtener credenciales temporales del servidor del portal de acceso C2S (CAP), incluidos todos los parámetros API necesarios y opcionales asignados a su cuenta C2S.
  - Certificado de CA de servidor emitido por una entidad de certificación (CA) gubernamental apropiada. StorageGRID utiliza este certificado para comprobar la identidad del servidor CAP. El certificado de CA del servidor debe utilizar la codificación PEM.
  - Certificado de cliente emitido por una autoridad de certificación gubernamental (CA) apropiada. StorageGRID utiliza este certificado para identificarse al servidor CAP. El certificado de cliente debe utilizar la codificación PEM y debe tener acceso a su cuenta C2S.
  - Clave privada codificada con PEM para el certificado de cliente.
  - Frase de acceso para descifrar la clave privada para el certificado de cliente, si está cifrada.

  > Si el certificado de cliente se cifrará, utilice el formato tradicional para el cifrado. El formato cifrado PKCS #8 no es compatible.

  Almacenamiento de Azure Blob

  Para el contenedor externo

  - Identificador de Recursos Uniforme (URI) utilizado para acceder al contenedor Blob Storage.
  - Nombre de la cuenta de almacenamiento y la clave de cuenta. Puede usar el portal de Azure para encontrar estos valores.

Pasos

1. Selecciona **ILM** > **Pools de almacenamiento** > **Pools de almacenamiento en la nube**.
2. Seleccione **Crear**, luego ingrese la siguiente información:

Campo	Descripción
Nombre de Cloud Storage Pool	Un nombre que describe brevemente el pool de almacenamiento en el cloud y su propósito. Utilice un nombre que será fácil de identificar al configurar las reglas de ILM.
Tipo de proveedor	Qué proveedor de cloud utilizará para este pool de almacenamiento en cloud: • **Amazon S3/GCP**: Seleccione esta opción para un proveedor compatible con Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) u otro proveedor compatible con S3. • **Almacenamiento de Azure Blob**
Cubo o contenedor	El nombre del bloque externo de S3 o contenedor de Azure. No se puede cambiar este valor después de guardar Cloud Storage Pool.

3. Según la selección del tipo de proveedor, introduzca la información de punto final de servicio.

Amazon S3/GCP

a. Para el protocolo, seleccione HTTPS o HTTP.

> No utilice conexiones HTTP para datos confidenciales.

b. Introduzca el nombre de host. Ejemplo:

`s3-aws-region.amazonaws.com`

c. Seleccione el estilo de URL:

Opción	Descripción
Detección automática	Intente detectar automáticamente qué estilo de URL usar, en función de la información proporcionada. Por ejemplo, si especifica una dirección IP, StorageGRID utilizará una dirección URL de tipo path. Seleccione esta opción sólo si no conoce el estilo específico que desea utilizar.
Estilo hospedado virtual	Use una URL de estilo alojada virtual para acceder al bloque. Las URL de estilo hospedado virtual incluyen el nombre del bucket como parte del nombre de dominio. Ejemplo: `https://bucket-name.s3.company.com/key-name`
Estilo de ruta	Utilice una dirección URL de estilo de ruta para acceder al bloque. Las URL de estilo de ruta incluyen el nombre del cubo al final Ejemplo: `https://s3.company.com/bucket-name/key-name` **Nota:** La opción de URL de estilo de ruta no se recomienda y se descartará en una futura versión de StorageGRID.

d. De manera opcional, introduzca el número de puerto o utilice el puerto predeterminado: 443 para HTTPS o 80 para HTTP.

Almacenamiento de Azure Blob

a. Con uno de los siguientes formatos, introduzca el URI para el punto final de servicio.

- `https://host:port`
- `http://host:port`

Ejemplo: `https://myaccount.blob.core.windows.net:443`

Si no especifica un puerto, por defecto el puerto 443 se utiliza para HTTPS y el puerto 80 se utiliza para HTTP.

4. Seleccione **continuar**. A continuación, seleccione el tipo de autenticación e introduzca la información requerida para el extremo de Cloud Storage Pool:

Clave de acceso

Solo para el tipo de proveedor de Amazon S3/GCP

a. Para **ID de clave de acceso**, ingrese el ID de clave de acceso de la cuenta que posee el depósito externo.
b. Para **Clave de acceso secreta**, ingrese la clave de acceso secreta.

CAP (portal de acceso C2S)

Para servicios en la nube comercial (C2S) S3 SERVICE

a. Para **URL de credenciales temporales**, ingrese la URL completa que StorageGRID usará para obtener credenciales temporales del servidor CAP, incluyendo todos los parámetros API requeridos y opcionales asignados a su cuenta C2S.
b. Para **Certificado CA de servidor**, seleccione **Examinar** y cargue el certificado CA codificado con PEM que StorageGRID utilizará para verificar el servidor CAP.
c. Para **Certificado de cliente**, seleccione **Examinar** y cargue el certificado codificado con PEM que StorageGRID utilizará para identificarse en el servidor CAP.
d. Para **Clave privada del cliente**, seleccione **Examinar** y cargue la clave privada codificada con PEM para el certificado del cliente.
e. Si la clave privada del cliente está cifrada, introduzca la frase de acceso para descifrar la clave privada del cliente. De lo contrario, deje en blanco el campo **Client private key passphrase**.

Almacenamiento de Azure Blob

a. Para **Nombre de cuenta**, ingrese el nombre de la cuenta de almacenamiento de Blob que posee el contenedor de servicio externo.
b. Para **Clave de cuenta**, ingresa la clave secreta para la cuenta de almacenamiento de Blob.

Anónimo

No se requiere información adicional.

5. Seleccione **continuar**. A continuación, elija el tipo de verificación de servidor que desea utilizar:

Opción	Descripción
Utilice los certificados de CA raíz en el sistema operativo del nodo de almacenamiento	Utilice los certificados de CA de cuadrícula instalados en el sistema operativo para asegurar las conexiones.
Utilizar certificado de CA personalizado	Usar un certificado de CA personalizado. Seleccione **Browse** y cargue el certificado codificado PEM.
No verifique el certificado	El certificado utilizado para la conexión TLS no se verifica.

6. Seleccione **Guardar**.

Cuando guarda un pool de almacenamiento en cloud, StorageGRID hace lo siguiente:

- Valida que el depósito o contenedor y el punto final del servicio existen y que se puede acceder a ellos mediante las credenciales que ha especificado.
- Escribe un archivo de marcador en el bloque o contenedor para identificarlo como un Cloud Storage Pool. No elimine nunca este archivo, que se denomina `x-ntap-sgws-cloud-pool-uuid`.

  Si la validación de Cloud Storage Pool falla, recibirá un mensaje de error que explica por qué falló la validación. Por ejemplo, puede que se informe un error si hay un error de certificado o si el bloque o el contenedor especificados no existen ya.

7. Si se produce un error, consulte "Instrucciones para solucionar problemas de Cloud Storage Pools", Resuelva cualquier problema y, a continuación, intente guardar el Pool de almacenamiento en cloud de nuevo.

Editar un pool de almacenamiento en el cloud

Puede editar un Pool de almacenamiento en la nube para cambiar su nombre, punto final de servicio u otros detalles; sin embargo, no puede cambiar el bucket de S3 o el contenedor de Azure para un Pool de almacenamiento en la nube.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Ha revisado el "Consideraciones para Cloud Storage Pools".

Pasos

1. Selecciona **ILM** > **Pools de almacenamiento** > **Pools de almacenamiento en la nube**.

   En la tabla Cloud Storage Pools, se enumera los pools de almacenamiento en el cloud.

2. Seleccione la casilla de verificación para el pool de almacenamiento en la nube que desea editar.
3. Selecciona **Acciones** > **Editar**.
4. Según sea necesario, cambie el nombre para mostrar, el extremo de servicio, las credenciales de autenticación o el método de validación de certificados.

   > No puede cambiar el tipo de proveedor, el bucket de S3 o el contenedor de Azure para un Cloud Storage Pool.

   Si cargó anteriormente un certificado de servidor o cliente, puede seleccionar **Detalles del certificado** para revisar el certificado que está en uso actualmente.

5. Seleccione **Guardar**.

   Cuando guarda un pool de almacenamiento en cloud, StorageGRID valida que el bloque o el contenedor y el extremo de servicio existen, y que se pueden acceder a ellos con las credenciales especificadas.

   Si la validación de Cloud Storage Pool falla, se muestra un mensaje de error. Por ejemplo, es posible que se informe un error si existe un error de certificado.

   Consulte las instrucciones para "Solución de problemas de Cloud Storage Pools", Resuelva el problema e intente volver a guardar el grupo de almacenamiento en la nube.

Quitar un pool de almacenamiento en el cloud

Puede quitar un pool de almacenamiento en cloud si no se utiliza en una regla de gestión de la vida útil de la información y no contiene datos de objetos.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".

Si es necesario, utilice ILM para mover datos de objetos

Si el Cloud Storage Pool que desea quitar contiene datos de objetos, debe usar ILM para mover los datos a otra ubicación. Por ejemplo, puede mover los datos a Nodos de almacenamiento en el grid o a otro Pool de almacenamiento en la nube.

Pasos

1. Selecciona **ILM** > **Pools de almacenamiento** > **Pools de almacenamiento en la nube**.
2. Observe la columna Uso de ILM en la tabla para determinar si puede quitar Cloud Storage Pool.

   No puede quitar un pool de almacenamiento de cloud si se está utilizando en una regla de gestión de la vida útil de la información o en un perfil de código de borrado.

3. Si se está utilizando Cloud Storage Pool, seleccione ***cloud storage pool name*** > **ILM usage**.
4. "Clone cada regla de ILM" Que actualmente coloca objetos en el Cloud Storage Pool que desea eliminar.
5. Determine dónde desea mover los objetos existentes gestionados por cada regla clonada.

   Puede utilizar uno o más pools de almacenamiento o un pool de almacenamiento en cloud diferente.

6. Edite cada una de las reglas clonadas.

   Para el Paso 2 del Asistente para crear reglas de ILM, seleccione la nueva ubicación en el campo **Copias en**.

7. "Cree una nueva política de ILM" y reemplace cada una de las reglas antiguas por una regla clonada.
8. Activar la nueva política.
9. Espere a que ILM elimine objetos del Cloud Storage Pool y colóquelos en la nueva ubicación.

Eliminar Pool de Almacenamiento en Nube

Cuando el pool de almacenamiento en cloud está vacío y no se usa en ninguna regla de ILM, puede eliminarlo.

Antes de empezar

- Quitó todas las reglas de ILM que pueden haber utilizado el pool.
- Ha confirmado que el bloque de S3 o el contenedor de Azure no contienen ningún objeto.

  Se produce un error si intenta quitar un Pool de almacenamiento en cloud si contiene objetos. Consulte "Solucione problemas de Cloud Storage Pools".

Cuando se crea un pool de almacenamiento en el cloud, StorageGRID escribe un archivo marcador en el bloque o contenedor para identificarlo como un pool de almacenamiento en el cloud. No elimine este archivo, que tiene el nombre `x-ntap-sgws-cloud-pool-uuid`.

Pasos

1. Selecciona **ILM** > **Pools de almacenamiento** > **Pools de almacenamiento en la nube**.
2. Si la columna ILM usage indica que Cloud Storage Pool no se está usando, seleccione la casilla de comprobación.
3. Seleccione **acciones** > **Quitar**.
4. Seleccione **OK**.

Solucione problemas de Cloud Storage Pools

Utilice estos pasos de solución de problemas para resolver los errores que puede encontrar al crear, editar o eliminar un pool de almacenamiento en la nube.

Determine si se ha producido un error

StorageGRID realiza una comprobación simple del estado de cada pool de almacenamiento en cloud una vez por minuto para garantizar que se pueda acceder al pool de almacenamiento en cloud y que funciona correctamente. Si la comprobación del estado detecta un problema, se muestra un mensaje en la última columna de error de la tabla Cloud Storage Pools de la página Storage Pools.

En la tabla, se muestra el error más reciente detectado para cada pool de almacenamiento en cloud e indica cuánto tiempo se produjo el error.

Además, se activa una alerta de error * de conectividad del grupo de almacenamiento en cloud* si la comprobación del estado detecta que se han producido uno o varios errores nuevos de Cloud Storage Pool en los últimos 5 minutos. Si recibe una notificación por correo electrónico para esta alerta, vaya a la página Grupos de almacenamiento (seleccione **ILM** > **Grupos de almacenamiento**), revise los mensajes de error en la última columna de error y consulte las directrices para la solución de problemas que aparecen a continuación.

Compruebe si se ha resuelto un error

Después de resolver cualquier problema subyacente, puede determinar si se ha resuelto el error. En la página Cloud Storage Pool, seleccione el punto final y seleccione **Borrar error**. Un mensaje de confirmación indica que StorageGRID borró el error para el pool de almacenamiento en el cloud.

Si se ha resuelto el problema subyacente, ya no se muestra el mensaje de error. Sin embargo, si el problema subyacente no se ha solucionado (o si se encuentra un error diferente), el mensaje de error se mostrará en la última columna de error en unos pocos minutos.

Error: Este pool de almacenamiento en cloud contiene contenido inesperado

Es posible ver este mensaje de error cuando se intenta crear, editar o eliminar un pool de almacenamiento en cloud. Este error se produce si el cucharón o el contenedor incluye `x-ntap-sgws-cloud-pool-uuid` Archivo marcador, pero ese archivo no tiene el UUID esperado.

Por lo general, solo verá este error si crea un nuevo pool de almacenamiento en el cloud y otra instancia de StorageGRID ya utiliza el mismo pool de almacenamiento en el cloud.

Intente realizar estos pasos para corregir el problema:

- Compruebe que nadie de su organización utiliza también este pool de almacenamiento en el cloud.
- Elimine el `x-ntap-sgws-cloud-pool-uuid` Archivo e intente configurar de nuevo el Pool de almacenamiento en la nube.

Error: No se pudo crear o actualizar Cloud Storage Pool. Error desde el punto final

Es posible ver este mensaje de error cuando se intenta crear o editar un pool de almacenamiento en el cloud. Este error indica que algún problema de conectividad o configuración impide que StorageGRID escriba en el pool de almacenamiento en el cloud.

Para corregir el problema, revise el mensaje de error desde el punto final.

- Si el mensaje de error contiene `Get *url*: EOF`, Compruebe que el punto final de servicio utilizado para el pool de almacenamiento en la nube no utiliza HTTP para un contenedor o depósito que requiere HTTPS.
- Si el mensaje de error contiene `Get *url*: net/http: request canceled while waiting for connection`, Compruebe que la configuración de red permite a los nodos de almacenamiento acceder al extremo de servicio utilizado para el grupo de almacenamiento en la nube.
- Para todos los demás mensajes de error de punto final, intente uno o más de los siguientes:
  - Cree un contenedor o bloque externo con el mismo nombre que introdujo para el Cloud Storage Pool e intente guardar de nuevo el nuevo Cloud Storage Pool.
  - Corrija el nombre de contenedor o bloque que especificó para Cloud Storage Pool e intente guardar de nuevo el nuevo pool de almacenamiento en cloud.

Error: No se pudo analizar el certificado de CA

Es posible ver este mensaje de error cuando se intenta crear o editar un pool de almacenamiento en el cloud. El error se produce si StorageGRID no pudo analizar el certificado introducido al configurar el pool de almacenamiento en cloud.

Para corregir el problema, compruebe el certificado de CA que proporcionó para los problemas.

Error: No se encontró un pool de almacenamiento en cloud con este ID

Es posible ver este mensaje de error cuando se intenta editar o eliminar un pool de almacenamiento en el cloud. Este error se produce si el extremo devuelve una respuesta 404, que puede significar cualquiera de las siguientes:

- Las credenciales utilizadas para Cloud Storage Pool no tienen permiso de lectura para el depósito.
- El bloque utilizado para el pool de almacenamiento en cloud no incluye el `x-ntap-sgws-cloud-pool-uuid` archivo de marcador.

Intente uno o más de estos pasos para corregir el problema:

- Compruebe que el usuario asociado a la clave de acceso configurada tenga los permisos necesarios.
- Edite el pool de almacenamiento cloud con credenciales que tengan los permisos necesarios.
- Si los permisos son correctos, póngase en contacto con el servicio de soporte técnico.

Error: No se ha podido comprobar el contenido del pool de almacenamiento en cloud. Error desde el punto final

Es posible ver este mensaje de error cuando se intenta eliminar un pool de almacenamiento en el cloud. Este error indica que algún problema de conectividad o configuración impide que StorageGRID lea el contenido del bucket de Cloud Storage Pool.

Para corregir el problema, revise el mensaje de error desde el punto final.

Error: Los objetos ya se han colocado en este cucharón

Es posible ver este mensaje de error cuando se intenta eliminar un pool de almacenamiento en el cloud. No puede eliminar un pool de almacenamiento en cloud si contiene datos que se movieron allí mediante ILM, datos que estaban en el depósito antes de configurar el pool de almacenamiento en cloud o datos que algún otro origen puso en el depósito después de crear el pool de almacenamiento en cloud.

Intente uno o más de estos pasos para corregir el problema:

- Siga las instrucciones para volver a mover objetos a StorageGRID en «Ciclo de vida de un objeto de pool de almacenamiento en cloud».
- Si está seguro de que ILM no colocó los objetos restantes en el Cloud Storage Pool, elimine manualmente los objetos del bloque.

> No elimine nunca manualmente objetos de un pool de almacenamiento en cloud que haya colocado allí ILM. Si más adelante intenta acceder a un objeto eliminado manualmente desde StorageGRID, no se encuentra el objeto eliminado.

Error: El proxy encontró un error externo al intentar acceder al pool de almacenamiento de cloud

Es posible ver este mensaje de error si configuró un proxy de almacenamiento no transparente entre los nodos de almacenamiento y el extremo externo S3 utilizado para el pool de almacenamiento en nube. Este error se produce si el servidor proxy externo no puede alcanzar el punto final de Cloud Storage Pool. Por ejemplo, es posible que el servidor DNS no pueda resolver el nombre de host o que haya un problema de red externo.

Intente uno o más de estos pasos para corregir el problema:

- Compruebe la configuración de Cloud Storage Pool (**ILM** > **agrupaciones de almacenamiento**).
- Compruebe la configuración de redes del servidor proxy de almacenamiento.

Información relacionada

"Ciclo de vida de un objeto de Cloud Storage Pool"

Gestione perfiles de código de borrado

Puede ver los detalles de un perfil de código de borrado y cambiar el nombre de un perfil si es necesario. Puede desactivar un perfil de código de borrado si actualmente no se está utilizando en ninguna regla de ILM.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".

Consulte los detalles del perfil de código de borrado

Puede ver los detalles de un perfil de código de borrado para determinar su estado, el esquema de código de borrado utilizado y otra información.

Pasos

1. Seleccione **ILM** > **codificación de borrado**.
2. Seleccione el perfil. Aparece la página de detalles del perfil.
3. De manera opcional, consulte la pestaña reglas de ILM para ver una lista de reglas de ILM que utilizan el perfil y las políticas de ILM que utilizan esas reglas.
4. Opcionalmente, consulte la pestaña Nodos de almacenamiento para obtener más información sobre cada nodo de almacenamiento en el pool de almacenamiento del perfil, como el sitio donde se encuentra y el uso del almacenamiento.

Cambie el nombre de un perfil de código de borrado

Es posible que desee cambiar el nombre de un perfil de codificación de borrado para que sea más obvio lo que hace el perfil.

Pasos

1. Seleccione **ILM** > **codificación de borrado**.
2. Seleccione el perfil al que desea cambiar el nombre.
3. Seleccione **Cambiar nombre**.
4. Introduzca un nombre único para el perfil de codificación de borrado.

   El nombre del perfil de codificación de borrado se añade al nombre del pool de almacenamiento en la instrucción de ubicación para una regla de ILM.

   > Los nombres de perfil de código de borrado deben ser únicos. Se produce un error de validación si utiliza el nombre de un perfil existente, incluso si dicho perfil se ha desactivado.

5. Seleccione **Guardar**.

Desactivar un perfil de código de borrado

Puede desactivar un perfil de código de borrado si ya no tiene pensado utilizarlo y si el perfil no se está utilizando en ninguna regla de ILM.

> Confirme que no hay operaciones de reparación de datos con código de borrado ni procedimientos de decomiso en curso. Se devuelve un mensaje de error si se intenta desactivar un perfil de código de borrado mientras se realiza alguna de estas operaciones.

Acerca de esta tarea

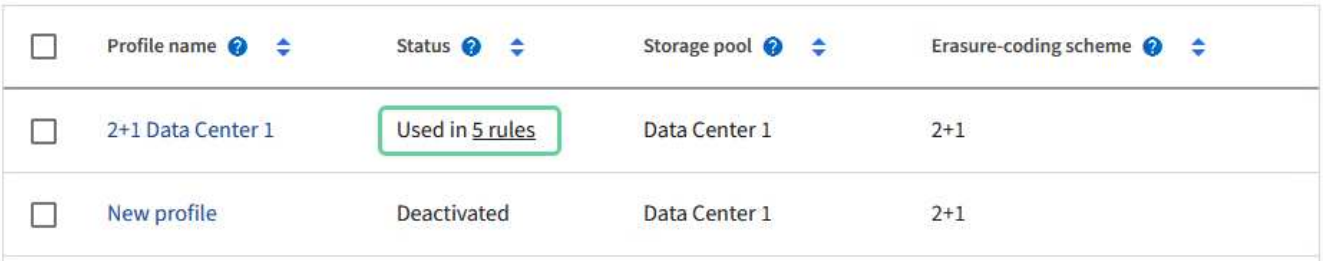
StorageGRID le impide desactivar un perfil de código de borrado si se cumple alguna de las siguientes condiciones:

- El perfil de código de borrado se utiliza actualmente en una regla de ILM.
- El perfil de código de borrado ya no se usa en ninguna regla de ILM, pero los datos de objetos y fragmentos de paridad del perfil siguen existiendo.

Pasos

1. Seleccione **ILM** > **codificación de borrado**.
2. En la pestaña Activo, revise la columna **Estado** para confirmar que el perfil de codificación de borrado que desea desactivar no se utiliza en ninguna regla de ILM.

   No puede desactivar un perfil de código de borrado si se utiliza en alguna regla de ILM. En el ejemplo, se utiliza el perfil de centro de datos 2+1 1 en al menos una regla de ILM.



3. Si el perfil se utiliza en una regla de ILM, siga estos pasos:
   a. Selecciona **ILM** > **Reglas**.
   b. Seleccione cada regla y revise el diagrama de retención para determinar si la regla utiliza el perfil de codificación de borrado que desea desactivar.
   c. Si la regla de ILM utiliza el perfil de código de borrado que desea desactivar, determine si la regla se utiliza en alguna política de ILM.
   d. Complete los pasos adicionales de la tabla, en función del perfil de código de borrado que se utilice.

¿Dónde se ha utilizado el perfil?	Pasos adicionales que se deben realizar antes de desactivar el perfil	Consulte estas instrucciones adicionales
No se usa nunca en ninguna regla de ILM	No se requieren pasos adicionales. Continúe con este procedimiento.	*Ninguno*
En una regla de ILM que nunca se haya usado en ninguna política de ILM	i. Edite o elimine todas las reglas de ILM afectadas. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de código de borrado. ii. Continúe con este procedimiento.	"Trabaje con las reglas de ILM y las políticas de ILM"

¿Dónde se ha utilizado el perfil?	Pasos adicionales que se deben realizar antes de desactivar el perfil	Consulte estas instrucciones adicionales
En una regla de ILM que está actualmente en una política de ILM activa	i. Clone la política. ii. Elimine la regla de ILM que utilice el perfil de código de borrado. iii. Añada una o varias reglas nuevas de ILM para garantizar la protección de los objetos. iv. Guarde, simule y active la nueva directiva. v. Espere a que se aplique la nueva directiva y a que los objetos existentes se muevan a nuevas ubicaciones en función de las nuevas reglas que haya agregado. **Nota:** dependiendo del número de objetos y del tamaño de su sistema StorageGRID, las operaciones de ILM pueden tardar semanas o incluso meses en mover los objetos a nuevas ubicaciones, según las nuevas reglas de ILM. Aunque puede intentar desactivar de forma segura un perfil de codificación de borrado mientras aún está asociado a los datos, la operación de desactivación fallará. Un mensaje de error le informará si el perfil aún no está listo para ser desactivado. vi. Edite o elimine la regla que ha eliminado de la política. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de código de borrado. vii. Continúe con este procedimiento.	"Cree una política de ILM" "Trabaje con las reglas de ILM y las políticas de ILM"
En una regla de ILM que está actualmente en una política de ILM	i. Edite la política. ii. Elimine la regla de ILM que utilice el perfil de código de borrado. iii. Añada una o varias reglas nuevas de ILM para garantizar que todos los objetos estén protegidos. iv. Guarde la política. v. Edite o elimine la regla que ha eliminado de la política. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de código de borrado. vi. Continúe con este procedimiento.	"Cree una política de ILM" "Trabaje con las reglas de ILM y las políticas de ILM"

e. Refresque la página de perfiles de codificación de borrado para asegurarse de que el perfil no se utiliza en una regla de ILM.

4. Si el perfil no se utiliza en una regla de ILM, seleccione el botón de opción y seleccione **Desactivar**. Aparece el cuadro de diálogo Desactivar perfil de codificación de borrado.

> Puede seleccionar varios perfiles para desactivarlos al mismo tiempo, siempre y cuando no se utilice cada perfil en ninguna regla.

5. Si está seguro de que desea desactivar el perfil, seleccione **Desactivar**.

Resultados

- Si StorageGRID puede desactivar el perfil de código de borrado, su estado es Desactivado. Ya no puede seleccionar este perfil para ninguna regla de ILM. No puede reactivar un perfil desactivado.
- Si StorageGRID no puede desactivar el perfil, aparecerá un mensaje de error. Por ejemplo, aparece un mensaje de error si los datos del objeto siguen asociados a este perfil. Es posible que deba esperar varias semanas antes de volver a intentar el proceso de desactivación.

Configurar regiones (opcional solo S3)

Las reglas de ILM pueden filtrar objetos en función de las regiones donde se crean bloques S3, lo que permite almacenar objetos de diferentes regiones en distintas ubicaciones de almacenamiento.

Si desea usar una región de bloque de S3 como filtro de una regla, primero debe crear las regiones que pueden usar los bloques del sistema.

> No puede cambiar la región de un depósito después de haber creado el depósito.

Antes de empezar

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

Acerca de esta tarea

Al crear un bloque de S3, puede especificar que el bloque se cree en una región determinada. El establecimiento de una región permite que el bloque se aproxime geográficamente a los usuarios, lo que ayuda a optimizar la latencia, minimizar los costes y cumplir con los requisitos normativos.

Cuando se crea una regla de ILM, se recomienda utilizar la región asociada con un bloque de S3 como filtro avanzado. Por ejemplo, puede diseñar una regla que se aplique sólo a los objetos de los cubos S3 creados en el `us-west-2` región. Luego, puede especificar que las copias de esos objetos se coloquen en nodos de almacenamiento en un centro de datos dentro de la región para optimizar la latencia.

Al configurar regiones, siga estas directrices:

- De forma predeterminada, se considera que todos los cubos pertenecen al `us-east-1` región.
- Debe crear las regiones mediante Grid Manager para poder especificar una región no predeterminada al crear cubos con el Administrador de inquilinos o la API de Gestión de inquilinos, o con el elemento de solicitud LocationConstraint para las solicitudes de la API PUT Bucket de S3. Se produce un error si una solicitud PUT Bucket utiliza una región que no se ha definido en StorageGRID.
- Debe usar el nombre exacto de la región cuando cree el bloque de S3. Los nombres de región distinguen entre mayúsculas y minúsculas. Los caracteres válidos son números, letras y guiones.

No se considera que la UE sea un alias para la ue-oeste-1. Si desea utilizar la región UE o eu-West-1, debe usar el nombre exacto.

- No puede eliminar ni modificar una región si se utiliza en una regla asignada a cualquier política (activa o inactiva).
- Si utiliza una región no válida como filtro avanzado en una regla de ILM, no puede agregar esa regla a una política.

  Se puede producir una región no válida si utiliza una región como filtro avanzado en una regla de ILM, pero posteriormente la elimina, o si utiliza la API de gestión de grid para crear una regla y especificar una región que no haya definido.

- Si elimina una región después de utilizarla para crear un bloque de S3, deberá volver a agregar la región si alguna vez desea utilizar el filtro avanzado restricción de ubicaciones para buscar objetos en ese bloque.

Pasos

1. Seleccione **ILM** > **Regiones**.

   Aparece la página Regiones, con las regiones definidas actualmente en la lista. **Región 1** muestra la región predeterminada, `us-east-1`, que no se puede modificar o eliminar.

2. Para agregar una región:
   a. Selecciona **Añadir otra región**.
   b. Introduzca el nombre de una región que desea utilizar al crear bloques de S3.

      Debe utilizar este nombre de región exacto como elemento de solicitud LocationConstraint al crear el bloque de S3 correspondiente.

3. Para eliminar una región no utilizada, seleccione el icono de eliminación .

   Aparece un mensaje de error si intenta eliminar una región que se utiliza actualmente en cualquier política (activa o inactiva).

4. Cuando haya terminado de realizar los cambios, seleccione **Guardar**.

   Ahora puede seleccionar estas regiones en la sección Advanced Filters en el paso 1 del asistente de creación de reglas de ILM. Consulte "Usar filtros avanzados en las reglas de ILM".

Cree la regla de ILM

Cree una regla de ILM: Información general

Para gestionar objetos, debe crear un conjunto de reglas de gestión de ciclo de vida de la información (ILM) y organizarlas en una política de ILM.

Cada objeto ingerido en el sistema se evalúa según la política activa. Cuando una regla de la política coincide con los metadatos de un objeto, las instrucciones de la regla determinan las acciones que StorageGRID lleva a cabo para copiar y almacenar ese objeto.

Los metadatos de objetos no se gestionan por las reglas de ILM. En su lugar, los metadatos de objetos se almacenan en una base de datos de Cassandra en lo que se conoce como almacén de metadatos. Se mantienen automáticamente tres copias de los metadatos de objetos en cada sitio para proteger los datos frente a pérdidas.

Elementos de una regla de ILM

Una regla de ILM consta de tres elementos:

- **Criterios de filtrado**: Los filtros básicos y avanzados de una regla definen a qué objetos se aplica la regla. Si un objeto coincide con todos los filtros, StorageGRID aplica la regla y crea las copias de objeto especificadas en las instrucciones de colocación de la regla.
- **Instrucciones de colocación**: Las instrucciones de colocación de una regla definen el número, el tipo y la ubicación de las copias de objetos. Cada regla puede incluir una secuencia de instrucciones de colocación para cambiar el número, el tipo y la ubicación de las copias de objetos a lo largo del tiempo. Cuando expira el período de tiempo para una ubicación, la siguiente evaluación de ILM aplica automáticamente las instrucciones en la siguiente ubicación.
- **Comportamiento de ingesta**: El comportamiento de ingesta de una regla le permite elegir cómo se protegen los objetos filtrados por la regla a medida que se ingieren (cuando un cliente S3 o Swift guarda un objeto en la cuadrícula).

Filtrado de reglas de ILM

Al crear una regla de ILM, puede especificar filtros para identificar a qué objetos se aplica la regla.

En el caso más sencillo, es posible que una regla no utilice ningún filtro. Cualquier regla que no utilice filtros se aplica a todos los objetos, por lo que debe ser la última regla (predeterminada) de una política de ILM. La regla predeterminada proporciona instrucciones de almacenamiento para objetos que no coinciden con los filtros de otra regla.

- Los filtros básicos permiten aplicar diferentes reglas a grupos grandes y distintos de objetos. Estos filtros le permiten aplicar una regla a cuentas de inquilino específicas, cubos S3 específicos o contenedores Swift, o ambos.

  Los filtros básicos le dan una manera sencilla de aplicar diferentes reglas a un gran número de objetos. Por ejemplo, es posible que los registros financieros de su empresa deban almacenarse para cumplir con requisitos normativos; en cambio, los datos del departamento de marketing pueden necesitar almacenarse para facilitar las operaciones diarias. Tras crear cuentas de inquilino independientes para cada departamento o al separar los datos de los diferentes departamentos en bloques S3 independientes, puede crear fácilmente una regla que se aplique a todos los registros financieros y a una segunda regla que se aplique a todos los datos de marketing.

- Los filtros avanzados le proporcionan un control granular. Puede crear filtros para seleccionar objetos según las siguientes propiedades de objeto:
  - Tiempo de ingesta
  - Hora del último acceso
  - Todo o parte del nombre del objeto (clave)
  - Restricción de ubicación (sólo S3)
  - Tamaño del objeto
  - Metadatos del usuario

◦ Etiqueta de objeto (solo S3)

Puede filtrar objetos según criterios muy específicos. Por ejemplo, los objetos almacenados por el departamento de imágenes de un hospital pueden usarse con frecuencia cuando tienen menos de 30 días de antigüedad y no suelen hacerlo después, mientras que los objetos que contienen información de visita del paciente pueden necesitar copiarse al departamento de facturación de la sede de la red sanitaria. Puede crear filtros que identifiquen cada tipo de objeto en función del nombre del objeto, el tamaño, las etiquetas de objetos de S3 o cualquier otro criterio relevante para, a continuación, crear reglas independientes para almacenar cada conjunto de objetos de la forma adecuada.

Puede combinar filtros según sea necesario en una sola regla. Por ejemplo, el departamento de marketing podría querer almacenar archivos de imagen de gran tamaño de forma diferente a sus registros de proveedor, mientras que el departamento de recursos humanos podría necesitar almacenar registros de personal en una región específica e información de políticas de forma centralizada. En este caso, puede crear reglas que filtren por cuenta de arrendatario para segregar los registros de cada departamento, mientras utiliza filtros en cada regla para identificar el tipo específico de objetos al que se aplica la regla.

Instrucciones para colocar las reglas de ILM

Las instrucciones de colocación determinan dónde, cuándo y cómo se almacenan los datos de objetos. Una regla de ILM puede incluir una o varias instrucciones de ubicación. Cada instrucción de colocación se aplica a un único período de tiempo.

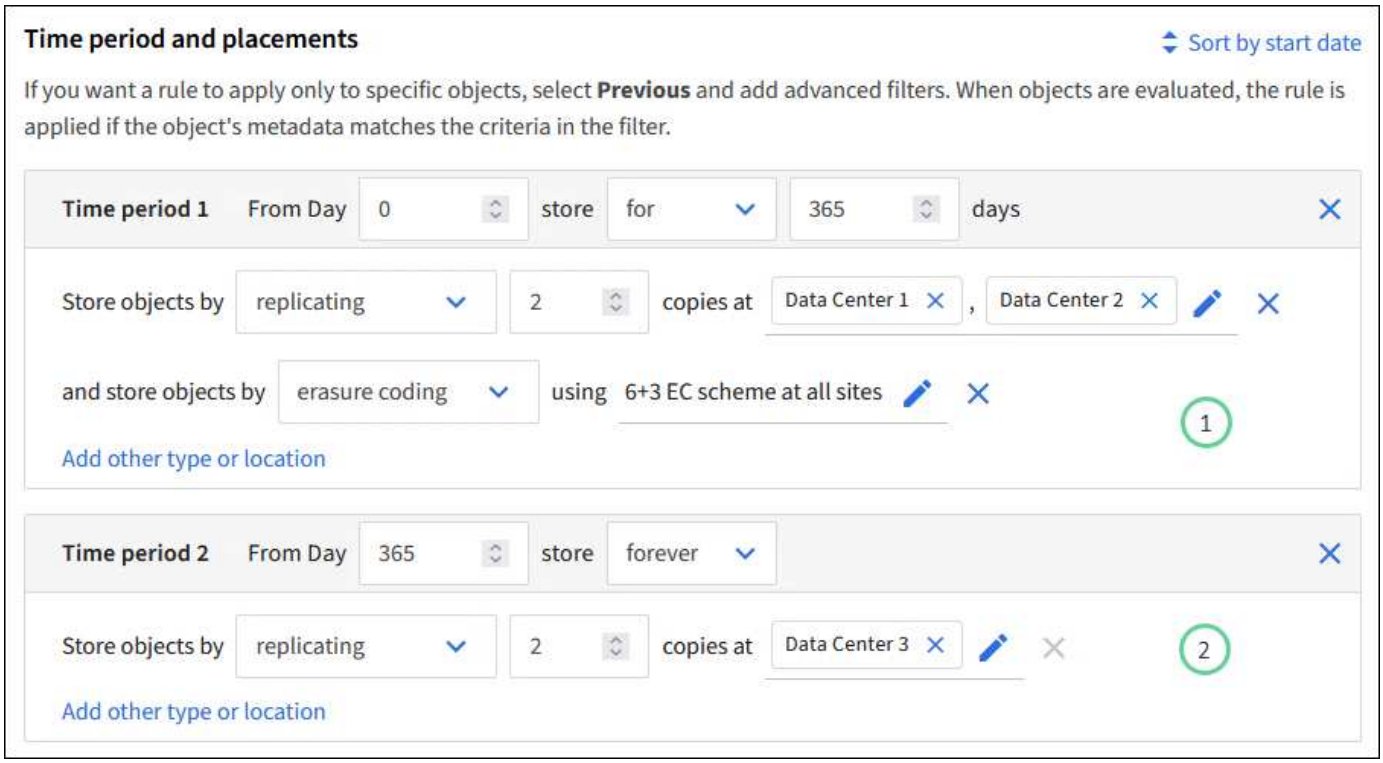
Al crear instrucciones de colocación:

- Para empezar, especifique el tiempo de referencia, que determina cuándo se inician las instrucciones de colocación. El tiempo de referencia podría ser el momento en que un objeto se ingiere, cuando se accede a un objeto, cuando un objeto con versiones se convierte en no actual o en un tiempo definido por el usuario.
- A continuación, especifique cuándo se aplicará la ubicación en relación con el tiempo de referencia. Por ejemplo, una ubicación puede comenzar el día 0 y continuar durante 365 días, en relación con el momento en que se ingirió el objeto.
- Por último, debe especificar el tipo de copias (codificación de replicación o borrado) y la ubicación donde se almacenan las copias. Por ejemplo, puede que desee almacenar dos copias replicadas en dos sitios diferentes.

Cada regla puede definir varias ubicaciones para un único período de tiempo y ubicaciones diferentes para diferentes períodos de tiempo.

- Para colocar objetos en varias ubicaciones durante un solo período de tiempo, seleccione **Añadir otro tipo o ubicación** para agregar más de una línea para ese período de tiempo.
- Para colocar objetos en diferentes ubicaciones en diferentes períodos de tiempo, seleccione **Agregar otro período de tiempo** para agregar el siguiente período de tiempo. A continuación, especifique una o más líneas dentro del período de tiempo.

En el ejemplo se muestran dos instrucciones de colocación en la página Definir ubicaciones del asistente Crear reglas de ILM.



La primera instrucción de colocación (1) tiene dos líneas para el primer año:

- La primera línea crea dos copias de objetos replicadas en dos sitios de centro de datos.
- La segunda línea crea una copia 6+3 con código de borrado utilizando todos los sitios del centro de datos.

La segunda instrucción de colocación (2) crea dos copias al año siguiente y guarda esas copias para siempre.

Cuando defina el conjunto de instrucciones de colocación para una regla, debe asegurarse de que al menos una instrucción de colocación comienza en el día 0, de que no haya espacios entre los períodos de tiempo definidos. y que la instrucción de colocación final continúa para siempre o hasta que ya no se requiere ninguna copia de objeto.

Cuando cada período de tiempo de la regla caduca, se aplican las instrucciones de colocación del contenido para el próximo período de tiempo. Se crean nuevas copias de objetos y se eliminan todas las copias innecesarias.

Comportamiento de procesamiento de reglas de ILM

El comportamiento de la ingesta controla si las copias de objetos se colocan inmediatamente según las instrucciones de la regla o si se realizan copias provisionales y se aplican las instrucciones de colocación más adelante. Para las reglas de ILM hay disponibles los siguientes comportamientos de consumo:

- **Balanceado**: StorageGRID intenta hacer todas las copias especificadas en la regla ILM en la ingesta; si esto no es posible, se hacen copias provisionales y se devuelve éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.
- **Estricto**: Todas las copias especificadas en la regla ILM deben hacerse antes de que el éxito se devuelva al cliente.
- **Confirmación doble**: StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve el

éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Información relacionada

- "Opciones de procesamiento"
- "Ventajas, desventajas y limitaciones de las opciones de ingesta"
- "Cómo interactúan las reglas de coherencia e ILM para afectar a la protección de datos"

Regla de ILM de ejemplo

Por ejemplo, una regla de ILM podría especificar lo siguiente:

- Aplicar solo a los objetos que pertenecen al inquilino A..
- Realice dos copias replicadas de dichos objetos y almacene cada copia en un sitio diferente.
- Conservar las dos copias «para siempre», lo que significa que StorageGRID no las eliminará automáticamente. En su lugar, StorageGRID conservará estos objetos hasta que se eliminen mediante una solicitud de eliminación del cliente o cuando finalice el ciclo de vida de un bloque.
- Use la opción Equilibrada para el comportamiento de ingesta: La instrucción de ubicación de dos sitios se aplica en cuanto el inquilino A guarda un objeto en StorageGRID, a menos que no sea posible hacer inmediatamente las dos copias requeridas.

  Por ejemplo, si el sitio 2 no se puede acceder cuando el inquilino A guarda un objeto, StorageGRID realizará dos copias provisionales en los nodos de almacenamiento del sitio 1. En cuanto el sitio 2 esté disponible, StorageGRID realizará la copia necesaria en ese sitio.

Información relacionada

- "Qué es un pool de almacenamiento"
- "Qué es un pool de almacenamiento en la nube"

Acceda al asistente Create an ILM Rule

Las reglas de ILM permiten gestionar la ubicación de los datos de objetos con el tiempo. Para crear una regla de ILM, debe usar el asistente Create an ILM Rule.

> Si desea crear la regla de ILM predeterminada para una política, siga el "Instrucciones para crear una regla de ILM predeterminada" en su lugar.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Si desea especificar a qué cuentas de arrendatario se aplica esta regla, tiene la "Permiso para cuentas de inquilino" O ya sabes el ID de cuenta de cada cuenta.
- Si desea que la regla filtre objetos en los metadatos de la última hora de acceso, las actualizaciones de la última hora de acceso deben habilitarse mediante bloque para S3 o por contenedor para Swift.
- Ha configurado los pools de Cloud Storage que desee utilizar. Consulte "Cree el pool de almacenamiento en el cloud".
- Usted está familiarizado con el "opciones de procesamiento".
- Si necesita crear una regla conforme para usarla con el bloqueo de objetos S3, ya está familiarizado con

la "Requisitos para el bloqueo de objetos de S3".

- Opcionalmente, ha visto el vídeo: "Vídeo: Reglas de gestión del ciclo de vida de la información en StorageGRID 11,8".

Acerca de esta tarea

Al crear reglas de ILM:

- Considere la topología y las configuraciones de almacenamiento del sistema StorageGRID.
- Piense en qué tipos de copias de objetos desea realizar (replicadas o con código de borrado) y el número de copias de cada objeto que se necesitan.
- Determinar qué tipos de metadatos de objetos se usan en las aplicaciones que se conectan al sistema StorageGRID. Las reglas de ILM filtran los objetos en función de sus metadatos.
- Considere dónde desea que las copias de objetos se coloquen a lo largo del tiempo.
- Decida qué opción de ingesta utilizar (Compromiso equilibrado, estricto o doble).

Pasos

1. Selecciona **ILM** > **Reglas**.
2. Seleccione **Crear**. "Paso 1 (Introducir detalles)" Se mostrará el asistente Crear una regla de ILM.

Paso 1 de 3: Introduzca los detalles

El paso **Introducir detalles** del asistente Crear una regla de ILM le permite introducir un nombre y una descripción para la regla y definir filtros para la regla.

La introducción de una descripción y la definición de filtros para la regla son opcionales.

Acerca de esta tarea

Al evaluar un objeto contra un "Regla de ILM", StorageGRID compara los metadatos del objeto con los filtros de la regla. Si los metadatos del objeto coinciden con todos los filtros, StorageGRID utiliza la regla para colocar el objeto. Puede diseñar una regla para aplicarla a todos los objetos, o puede especificar filtros básicos, como uno o más nombres de cuentas de arrendatario o de bloques, o filtros avanzados, como el tamaño del objeto o los metadatos de usuario.

Pasos

1. Introduzca un nombre único para la regla en el campo **Nombre**.
2. Si lo desea, introduzca una breve descripción de la regla en el campo **Descripción**.

   Debe describir el propósito o la función de la regla para poder reconocerla más adelante.

3. De manera opcional, seleccione una o varias cuentas de inquilino de S3 o Swift a las que se aplica esta regla. Si esta regla se aplica a todos los inquilinos, deje este campo en blanco.

   Si no tiene el permiso de acceso raíz o las cuentas de inquilino, no puede seleccionar arrendatarios de la lista. En su lugar, introduzca el ID de inquilino o introduzca varios ID como una cadena delimitada por comas.

4. De manera opcional, especifique los bloques de S3 o los contenedores Swift a los que se aplica esta regla.

Si se selecciona **Aplica a todos los cubos** (predeterminado), la regla se aplica a todos los cubos S3 o contenedores Swift.

5. Para los inquilinos S3, opcionalmente seleccione **Sí** para aplicar la regla solo a versiones de objetos más antiguas en cubos S3 que tienen el control de versiones activado.

   Si selecciona **Sí**, la opción “Hora no corriente” se seleccionará automáticamente para la Hora de referencia en "Paso 2 del asistente Crear una regla de ILM".

   > La hora no actual se aplica solo a objetos S3 en bloques con control de versiones activado. Consulte "Operaciones en cucharones, PutBucketVersioning" y.. "Gestione objetos con S3 Object Lock".

   Puede utilizar esta opción para reducir el impacto del almacenamiento de objetos con versiones mediante el filtrado de versiones de objetos no actuales. Consulte "Ejemplo 4: Reglas de ILM y políticas para objetos con versiones de S3".

6. Opcionalmente, seleccione **Agregar un filtro avanzado** para especificar filtros adicionales.

   Si no configura el filtrado avanzado, la regla se aplica a todos los objetos que coincidan con los filtros básicos. Para obtener más información sobre el filtrado avanzado, consulte Usar filtros avanzados en las reglas de ILM y.. Especifique varios tipos y valores de metadatos.

7. Seleccione **continuar**. "Paso 2 (Definir ubicaciones)" Se mostrará el asistente Crear una regla de ILM.

Usar filtros avanzados en las reglas de ILM

El filtrado avanzado permite crear reglas de ILM que se aplican solo a objetos específicos en función de sus metadatos. Al configurar el filtrado avanzado para una regla, debe seleccionar el tipo de metadatos que desea que coincidan, seleccionar un operador y especificar un valor de metadatos. Cuando se evalúan objetos, la regla de ILM se aplica solo a los objetos que tienen metadatos que coincidan con el filtro avanzado.

En la tabla se muestran los tipos de metadatos que se pueden especificar en los filtros avanzados, los operadores que se pueden utilizar para cada tipo de metadatos y los valores de metadatos esperados.

Tipo de metadatos	Operadores compatibles	Valor de los metadatos
Tiempo de ingesta	• es • no lo es • es antes • es el o antes • es posterior • es el o después	Hora y fecha en la que se ingirió el objeto. **Nota:** Para evitar problemas de recursos al activar una nueva política de ILM, puede usar el filtro avanzado de tiempo de ingesta en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de procesamiento en mayor o igual que el tiempo aproximado en el que la nueva política entrará en vigor para garantizar que los objetos existentes no se muevan innecesariamente.

Tipo de metadatos	Operadores compatibles	Valor de los metadatos
Clave	• es igual a • no es igual • contiene • no contiene • comienza con • no empieza por • termina con • no termina con	Todo o parte de una clave de objeto S3 o Swift única. Por ejemplo, quizás desee hacer coincidir los objetos que terminan con `.txt` o empiece por `test-object/`.
Hora del último acceso	• es • no lo es • es antes • es el o antes • es posterior • es el o después	Hora y fecha en la que se recuperó por última vez el objeto (leído o visualizado). **Nota:** Si planeas hacerlo "utilizar la hora del último acceso" Como filtro avanzado, las actualizaciones de la hora del último acceso deben estar habilitadas para el depósito S3 o el contenedor Swift.
Restricción de ubicación (sólo S3)	• es igual a • no es igual	Región en la que se creó un bloque de S3. Utilice **ILM** > **Regiones** para definir las regiones que se muestran. **Nota:** un valor de US-East-1 coincidirán con objetos en cubos creados en la región US-East-1 así como con objetos en cubos que no tienen una región especificada. Consulte "Configurar regiones (opcional solo S3)".
Tamaño del objeto	• es igual a • no es igual • menor que • menor o igual que • mayor que • mayor o igual que	Tamaño del objeto. El código de borrado se adapta mejor a los objetos de más de 1 MB. No use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

Tipo de metadatos	Operadores compatibles	Valor de los metadatos
Metadatos del usuario	• contiene • termina con • es igual a • existe • comienza con • no contiene • no termina con • no es igual • no existe • no empieza por	Par clave-valor, donde **Nombre de metadatos de usuario** es la clave y **Valor de metadatos** es el valor. Por ejemplo, para filtrar objetos con metadatos de usuario de `color=blue`, especifique `color` Para **Nombre de metadatos de usuario**, `equals` para el operador, y. `blue` Para **Valor de metadatos**. **Nota:** Los nombres de metadatos de usuario no son sensibles a mayúsculas/minúsculas; los valores de metadatos de usuario son sensibles a mayúsculas/minúsculas.
Etiqueta de objeto (solo S3)	• contiene • termina con • es igual a • existe • comienza con • no contiene • no termina con • no es igual • no existe • no empieza por	Par clave-valor, donde **Object tag name** es la clave y **Object tag value** es el valor. Por ejemplo, para filtrar objetos que tienen una etiqueta de objeto de `Image=True`, especifique `Image` Para **Nombre de etiqueta de objeto**, `equals` para el operador, y. `True` Para **Object tag value**. **Nota:** los nombres de las etiquetas de objeto y los valores de las etiquetas de objeto distinguen entre mayúsculas y minúsculas. Debe introducir estos elementos exactamente como se definieron para el objeto.

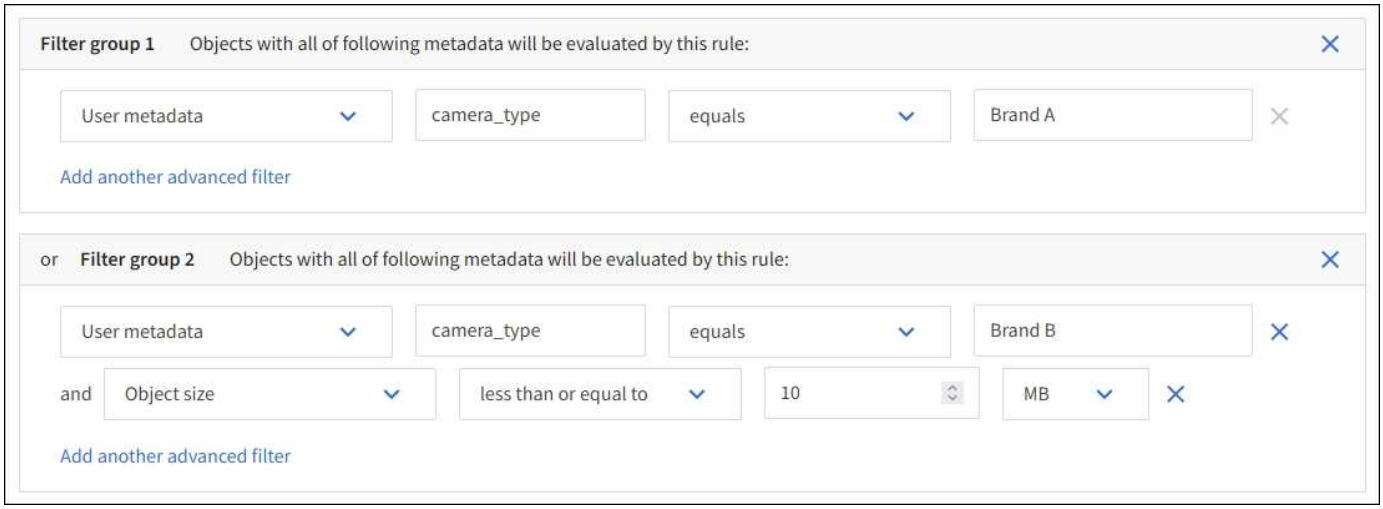
Especifique varios tipos y valores de metadatos

Al definir un filtrado avanzado, es posible especificar varios tipos de metadatos y varios valores de metadatos. Por ejemplo, si desea que una regla coincida con objetos de entre 10 MB y 100 MB de tamaño, debe seleccionar el tipo de metadatos **Tamaño de objeto** y especificar dos valores de metadatos.

- El primer valor de metadatos especifica objetos mayores o iguales a 10 MB.
- El segundo valor de metadatos especifica objetos inferiores o iguales a 100 MB.

El uso de múltiples entradas permite tener un control preciso sobre qué objetos coinciden. En el siguiente ejemplo, la regla se aplica a los objetos que tienen Marca A o Marca B como valor de los metadatos de usuario camera_type. Sin embargo, la regla sólo se aplica a los objetos de Marca B que son menores de 10

MB.



Paso 2 de 3: Definir colocaciones

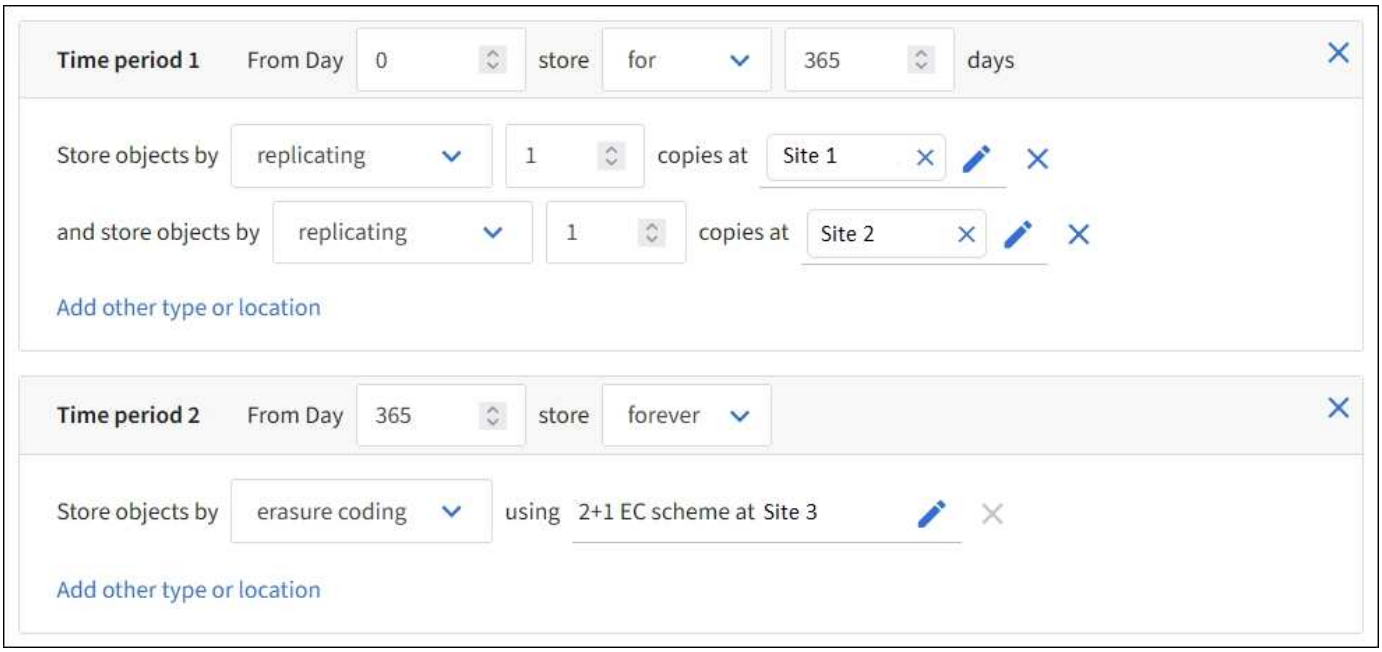
El paso **Definir ubicaciones** del asistente Crear regla de ILM le permite definir las instrucciones de colocación que determinan cuánto tiempo se almacenan los objetos, el tipo de copias (replicadas o con código de borrado), la ubicación de almacenamiento y el número de copias.

Acerca de esta tarea

Una regla de ILM puede incluir una o varias instrucciones de ubicación. Cada instrucción de colocación se aplica a un único período de tiempo. Cuando utilice más de una instrucción, los períodos de tiempo deben ser contiguos y al menos una instrucción debe comenzar en el día 0. Las instrucciones pueden continuar para siempre o hasta que ya no necesite ninguna copia de objeto.

Cada instrucción de colocación puede tener varias líneas si desea crear diferentes tipos de copias o utilizar diferentes ubicaciones durante ese período de tiempo.

En este ejemplo, la regla de ILM almacena una copia replicada en el sitio 1 y una copia replicada en el sitio 2 durante el primer año. Después de un año, se realiza y se guarda una copia con código de borrado al 2+1 en una sola instalación.



Pasos

1. Para **Tiempo de referencia**, seleccione el tipo de tiempo que se utilizará al calcular la hora de inicio de una instrucción de colocación.

Opción	Descripción
Tiempo de ingesta	Hora a la que se ingirió el objeto.
Hora del último acceso	Hora a la que se recuperó por última vez el objeto (leído o visualizado). **Nota:** Para usar esta opción, las actualizaciones de la hora de último acceso deben estar habilitadas para el cubo S3 o el contenedor Swift. Consulte "Utilice la última hora de acceso en las reglas de ILM".
Hora de creación definida por el usuario	Hora especificada en los metadatos definidos por el usuario.
Hora no corriente	Se selecciona automáticamente “Hora no corriente” si seleccionó **Sí** para la pregunta, ¿Aplicar esta regla solo a versiones de objetos anteriores (en bloques S3 con control de versiones activado)? pulg "Paso 1 del asistente Crear una regla de ILM".

Si desea crear una regla compatible, debe seleccionar **tiempo de ingesta**. Consulte "Gestione objetos con S3 Object Lock".

2. En la sección **Período de tiempo y ubicaciones**, introduzca una hora de inicio y una duración para el primer período de tiempo.

   Por ejemplo, puede especificar dónde almacenar objetos para el primer año (*from día 0 store for 365 days*). Al menos una instrucción debe comenzar en el día 0.

3. Si desea crear copias replicadas:
   a. En la lista desplegable **Store objects by**, selecciona **Replicating**.
   b. Seleccione el número de copias que desea realizar.

      Aparecerá una advertencia si cambia el número de copias a 1. Una regla de ILM que crea solo una copia replicada en cualquier periodo de tiempo pone los datos en riesgo de pérdida permanente. Consulte "Por qué no se debe utilizar la replicación de copia única".

      Para evitar el riesgo, realice una o más de las siguientes acciones:

      - Aumentar el número de copias durante el período de tiempo.
      - Añada copias a otros pools de almacenamiento o a un pool de almacenamiento en cloud.
      - Seleccione **código de borrado** en lugar de **Replicating**.

        Puede ignorar con toda tranquilidad esta advertencia si esta regla ya crea varias copias para todos los períodos de tiempo.

   c. En el campo **Copias en**, seleccione los pools de almacenamiento que desea agregar.

      Si especifica sólo un pool de almacenamiento, tenga en cuenta que StorageGRID sólo puede almacenar una copia replicada de un objeto en un nodo de almacenamiento dado. Si el grid incluye tres nodos de almacenamiento y selecciona 4 como número de copias, solo se crearán tres copias—una copia para cada nodo de almacenamiento.

      > Se activa la alerta **colocación de ILM inalcanzable** para indicar que la regla ILM no se pudo aplicar completamente.

      Si especifica más de una agrupación de almacenamiento, tenga en cuenta estas reglas:

      - La cantidad de copias no puede ser mayor que la cantidad de pools de almacenamiento.
      - Si el número de copias es igual al número de pools de almacenamiento, se almacena una copia del objeto en cada pool de almacenamiento.
      - Si el número de copias es inferior al número de pools de almacenamiento, se almacena una copia en el sitio de procesamiento y, a continuación, el sistema distribuye las copias restantes para mantener el uso del disco entre los pools equilibrados, a la vez que se garantiza que ningún sitio obtenga más de una copia de un objeto.
      - Si los pools de almacenamiento se superponen (contienen los mismos nodos de almacenamiento), es posible que todas las copias del objeto se guarden en un solo sitio. Por este motivo, no se especifica el pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores) y otro pool de almacenamiento.
4. Si desea crear una copia con código de borrado:
   a. En la lista desplegable **Almacenar objetos por**, selecciona **código de borrado**.

      > El código de borrado se adapta mejor a los objetos de más de 1 MB. No use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

   b. Si no ha agregado un filtro de tamaño de objeto para un valor superior a 200 KB, seleccione **Anterior** para volver al paso 1. Luego, selecciona **Agregar un filtro avanzado** y establece un filtro **Tamaño de objeto** en cualquier valor mayor que 200 KB.

c. Seleccione el pool de almacenamiento que desea añadir y el esquema de código de borrado que desea usar.

   La ubicación de almacenamiento para una copia con código de borrado incluye el nombre del esquema de código de borrado, seguido del nombre del pool de almacenamiento.

5. Opcionalmente:
   a. Seleccione **Añadir otro tipo o ubicación** para crear copias adicionales en diferentes ubicaciones.
   b. Seleccione **Añadir otro período** para agregar diferentes períodos de tiempo.

      > Los objetos se eliminan automáticamente al final del período de tiempo final, a menos que otro período de tiempo termine con **Forever**.

6. Si desea almacenar objetos en un pool de almacenamiento en cloud:
   a. En la lista desplegable **Store objects by**, selecciona **Replicating**.
   b. Seleccione el campo **Copias en** y, a continuación, seleccione un Pool de almacenamiento en la nube.

      Cuando utilice Cloud Storage Pools, tenga en cuenta estas reglas:

      - No se puede seleccionar más de un Cloud Storage Pool en una sola instrucción de colocación. De forma similar, no puede seleccionar un Cloud Storage Pool y un pool de almacenamiento en las mismas instrucciones de colocación.
      - Solo puede almacenar una copia de un objeto en cualquier Cloud Storage Pool en concreto. Aparece un mensaje de error si configura **copias** en 2 o más.
      - No es posible almacenar más de una copia de objeto en ningún pool de almacenamiento en cloud al mismo tiempo. Aparecerá un mensaje de error si varias ubicaciones que utilizan un Cloud Storage Pool tienen fechas superpuestas o si varias líneas en la misma ubicación utilizan un Cloud Storage Pool.
      - Puede almacenar un objeto en un pool de almacenamiento en cloud a la vez que el objeto se almacena como copias replicadas o con código de borrado en StorageGRID. Sin embargo, debe incluir más de una línea en la instrucción de colocación para el período de tiempo, de modo que pueda especificar el número y los tipos de copias para cada ubicación.

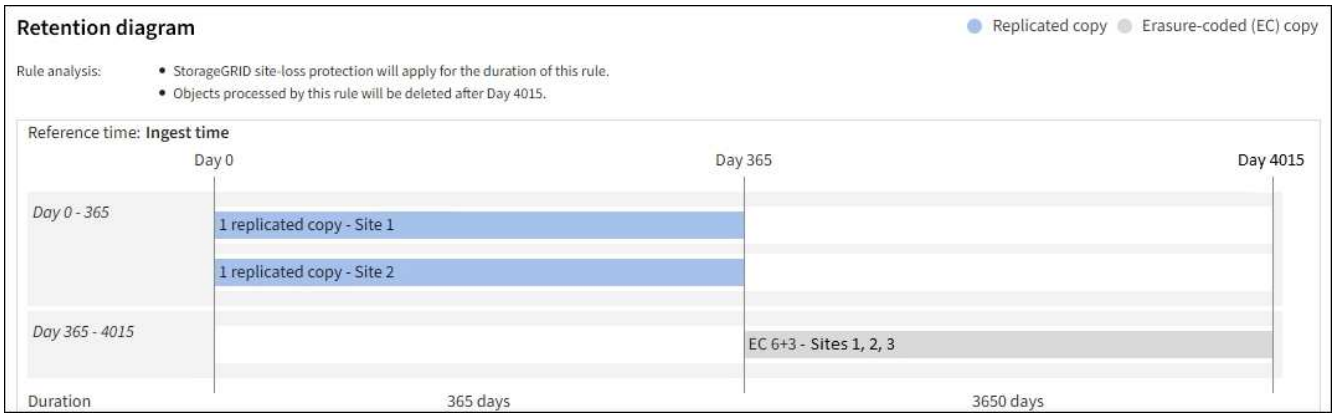
7. En el diagrama de retención, confirme las instrucciones de colocación.

   En este ejemplo, la regla de ILM almacena una copia replicada en el sitio 1 y una copia replicada en el sitio 2 durante el primer año. Transcurrido un año y durante 10 años más, se guardará una copia con código de borrado de 6+3 en tres instalaciones. Después de 11 años en total, los objetos se eliminarán de StorageGRID.

   La sección de análisis de reglas del diagrama de retención indica lo siguiente:

   - La protección contra pérdida de sitios de StorageGRID se aplicará mientras dure esta regla.
   - Los objetos procesados por esta regla se eliminarán después del día 4015.

     > Consulte "Habilite la protección contra pérdida de sitio."



8. Seleccione **continuar**. "Paso 3 (Seleccionar comportamiento de ingesta)" Se mostrará el asistente Crear una regla de ILM.

Utilice la última hora de acceso en las reglas de ILM

Puede utilizar la última hora de acceso como hora de referencia en una regla de ILM. Por ejemplo, quizás desee dejar objetos que se han visto en los últimos tres meses en nodos de almacenamiento local, mientras mueve objetos que no se han visto recientemente a una ubicación externa. También puede usar la última hora de acceso como filtro avanzado si desea que una regla de ILM se aplique únicamente a los objetos a los que se accedió por última vez en una fecha específica.

Acerca de esta tarea

Antes de utilizar la última hora de acceso en una regla de ILM, revise las siguientes consideraciones:

- Cuando se utiliza el último tiempo de acceso como hora de referencia, tenga en cuenta que el cambio de la hora del último acceso de un objeto no desencadena una evaluación inmediata del ciclo de vida de la información útil de la información. En su lugar, las ubicaciones del objeto se evalúan y el objeto se mueve según sea necesario cuando el ILM de segundo plano evalúa el objeto. Esto podría tardar dos semanas o más después de acceder al objeto.

  Tenga en cuenta esta latencia al crear reglas de ILM basadas en el último tiempo de acceso y evite ubicaciones que utilicen períodos de tiempo cortos (menos de un mes).

- Al utilizar la última hora de acceso como filtro avanzado o como hora de referencia, debe habilitar las actualizaciones de la última hora de acceso para los bloques S3. Puede utilizar el "Administrador de inquilinos" o la "API de gestión de inquilinos".

> Las actualizaciones del último tiempo de acceso siempre están habilitadas para contenedores Swift, pero están deshabilitadas de forma predeterminada en bloques S3.

> Tenga en cuenta que habilitar las actualizaciones del tiempo de último acceso puede reducir el rendimiento, especialmente en sistemas con objetos pequeños. El impacto en el rendimiento se produce porque StorageGRID debe actualizar los objetos con marcas de tiempo nuevas cada vez que se recuperan los objetos.

En la siguiente tabla se resume si se actualiza la hora del último acceso para todos los objetos del depósito para distintos tipos de solicitudes.

Tipo de solicitud	Si se actualiza la hora del último acceso cuando se desactivan las actualizaciones de la última hora de acceso	Si se actualiza la hora del último acceso cuando se activan las actualizaciones de la última hora de acceso
Solicitud para recuperar un objeto, su lista de control de acceso o sus metadatos	No	Sí
Solicitud para actualizar los metadatos de un objeto	Sí	Sí
Solicite copiar un objeto de un bloque a otro	• No, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Paso 3 de 3: Seleccione el comportamiento de ingesta

El paso **Seleccionar comportamiento de ingesta** del asistente Crear regla de ILM le permite elegir cómo se protegen los objetos filtrados por esta regla a medida que se ingieren.

Acerca de esta tarea

StorageGRID puede hacer copias provisionales y poner en cola los objetos para la evaluación de ILM más tarde, o puede hacer copias para cumplir las instrucciones de colocación de la regla de forma inmediata.

Pasos

1. Seleccione la "comportamiento de ingesta" para utilizar.

   Para obtener más información, consulte "Ventajas, desventajas y limitaciones de las opciones de ingesta".

   > No puede utilizar la opción Equilibrado o Estricto si la regla utiliza una de estas ubicaciones:
   >
   > - Un pool de almacenamiento en cloud desde el día 0
   > - Un nodo de archivado al día 0
   > - Un pool de almacenamiento en nube o un nodo de archivado cuando la regla utiliza un tiempo de creación definido por el usuario como tiempo de referencia
   >
   > Consulte "Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto".

2. Seleccione **Crear**.

   Se crea la regla de ILM. La regla no se activa hasta que se agrega a un "Política de ILM" y esa política se activa.

   Para ver los detalles de la regla, seleccione el nombre de la regla en la página de reglas de ILM.

Cree una regla de ILM predeterminada

Antes de crear una política de ILM, debe crear una regla predeterminada para colocar los objetos que no coincidan con otra regla en la política. La regla predeterminada no puede utilizar ningún filtro. Debe aplicarse a todos los inquilinos, todos los grupos y todas las versiones del objeto.

Antes de empezar

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

Acerca de esta tarea

La regla predeterminada es la última regla que se debe evaluar en una política de ILM, por lo que no puede utilizar ningún filtro. Las instrucciones de colocación para la regla predeterminada se aplican a cualquier objeto que no coincida con otra regla de la política.

En esta política de ejemplo, la primera regla se aplica solo a los objetos que pertenecen a test-tenant-1. La regla predeterminada, que es última, se aplica a los objetos que pertenecen a todas las demás cuentas de arrendatario.

Al crear la regla predeterminada, tenga en cuenta estos requisitos:

- La regla predeterminada se colocará automáticamente como la última regla cuando la agregue a una política.
- La regla predeterminada no puede utilizar ningún filtro básico o avanzado.
- La regla predeterminada debe aplicarse a todas las versiones de objetos.
- La regla predeterminada debe crear copias replicadas.

No utilice una regla que cree copias con código de borrado como regla predeterminada para una política. Las reglas de código de borrado deberían usar un filtro avanzado para evitar que los objetos más pequeños se codifiquen y se borren.

- En general, la regla predeterminada debería retener objetos para siempre.
- Si está utilizando (o planea habilitar) la configuración global S3 Object Lock, la regla predeterminada debe ser compatible.

Pasos

1. Selecciona **ILM** > **Reglas**.
2. Seleccione **Crear**.

   Se muestra el paso 1 (introduzca detalles) del asistente Crear regla de ILM.

3. Introduzca un nombre único para la regla en el campo **Nombre de regla**.
4. Si lo desea, introduzca una breve descripción de la regla en el campo **Descripción**.
5. Deja el campo **Cuentas de inquilino** en blanco.

   La regla predeterminada debe aplicarse a todas las cuentas de arrendatario.

6. Deje la selección desplegable Nombre del cucharón como **Aplica a todos los cubos**.

   La regla predeterminada debe aplicarse a todos los bloques de S3 y contenedores Swift.

7. Mantenga la respuesta predeterminada, **No**, para la pregunta, "¿Aplicar esta regla solo a versiones de objetos más antiguas (en cubos S3 con control de versiones habilitado)?"
8. No agregue filtros avanzados.

   La regla predeterminada no puede especificar ningún filtro.

9. Seleccione **Siguiente**.

   Aparece el paso 2 (Definir ubicaciones).

10. En Tiempo de referencia, seleccione cualquier opción.

    Si mantuviste la respuesta predeterminada, **No**, para la pregunta, "¿Aplicar esta regla solo a versiones de objetos anteriores?" La hora no actual no se incluirá en la lista desplegable. La regla predeterminada debe aplicar todas las versiones del objeto.

11. Especifique las instrucciones de colocación para la regla predeterminada.
    - La regla predeterminada debería retener objetos para siempre. Aparece una advertencia cuando activa una nueva directiva si la regla predeterminada no conserva objetos para siempre. Debe confirmar que éste es el comportamiento que espera.
    - La regla predeterminada debe crear copias replicadas.

    No utilice una regla que cree copias con código de borrado como regla predeterminada para una política. Las reglas de codificación de borrado deben incluir el filtro avanzado **Tamaño de objeto (MB) mayor que 200 KB** para evitar que los objetos más pequeños sean codificados de borrado.

- Si está utilizando (o tiene previsto habilitar) la configuración global de bloqueo de objetos S3, la regla predeterminada debe ser compatible:
  - Debe crear al menos dos copias de objetos replicados o una copia con código de borrado.
  - Estas copias deben existir en los nodos de almacenamiento durante todo el tiempo que dure cada línea en las instrucciones de colocación.
  - Las copias de objetos no se pueden guardar en un pool de almacenamiento en la nube.
  - Las copias de objetos no se pueden guardar en los nodos de archivado.
  - Al menos una línea de las instrucciones de colocación debe comenzar en el día 0, utilizando el tiempo de ingesta como hora de referencia.
  - Al menos una línea de las instrucciones de colocación debe ser “Para siempre”.

12. Consulte el diagrama de retención para confirmar las instrucciones de colocación.
13. Seleccione **continuar**.

    Aparece el paso 3 (Seleccionar comportamiento de ingesta).

14. Seleccione la opción de ingesta que desea utilizar y seleccione **Crear**.

Gestionar políticas de ILM

Políticas de ILM: Información general

Una política de gestión de ciclo de vida de la información (ILM) es un conjunto ordenado de reglas de ILM que determinan el modo en que el sistema StorageGRID gestiona los datos de objetos a lo largo del tiempo.

> Una política de ILM que se configuró incorrectamente puede provocar la pérdida de datos irrecuperable. Antes de activar una política de ILM, revise con detenimiento la política de ILM y sus reglas de ILM, y simule la política de ILM. Confirme siempre que la política de gestión del ciclo de vida de la información funcionará como se pretende.

Política de ILM predeterminada

Al instalar StorageGRID y agregar sitios, se crea automáticamente una política de ILM predeterminada, de la siguiente manera:

- Si su grid contiene un sitio, la política predeterminada contiene una regla predeterminada que replica dos copias de cada objeto del sitio.
- Si la cuadrícula contiene más de un sitio, la regla predeterminada replica una copia de cada objeto en cada sitio.

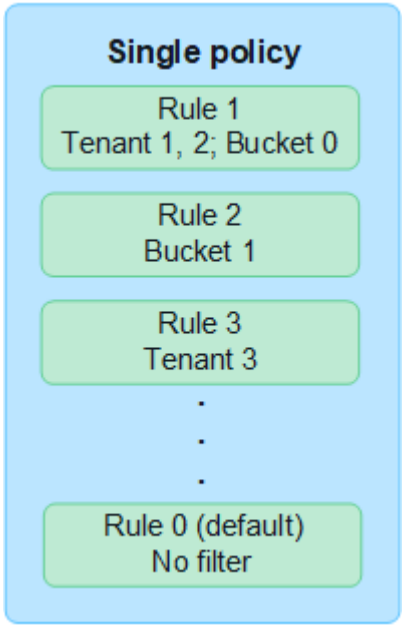
Si la política predeterminada no cumple con sus requisitos de almacenamiento, puede crear sus propias reglas y políticas. Consulte "Cree una regla de ILM" y.. "Cree una política de ILM".

¿Una o muchas políticas de ILM activas?

Puede tener una o varias políticas de ILM activas a la vez.

Una política

Si su grid utilizará un esquema de protección de datos simple con pocas reglas específicas para inquilinos y bloques, use una única política de ILM activa. Las reglas de ILM pueden contener filtros para gestionar diferentes bloques o inquilinos.



Cuando solo tiene una política y cambian los requisitos de un inquilino, debe crear una nueva política de ILM o clonar la política existente para aplicar cambios, simular y, a continuación, activar la nueva política de ILM. Los cambios en la política de ILM pueden provocar movimientos de objetos que podrían tardar muchos días y causar latencia del sistema.

Múltiples políticas

Para proporcionar diferentes opciones de calidad de servicio a clientes, se puede tener más de una política activa a la vez. Cada política puede administrar inquilinos específicos, bloques de S3 y objetos. Al aplicar o cambiar una política para un conjunto específico de inquilinos u objetos, las políticas aplicadas a otros inquilinos y objetos no se ven afectadas.

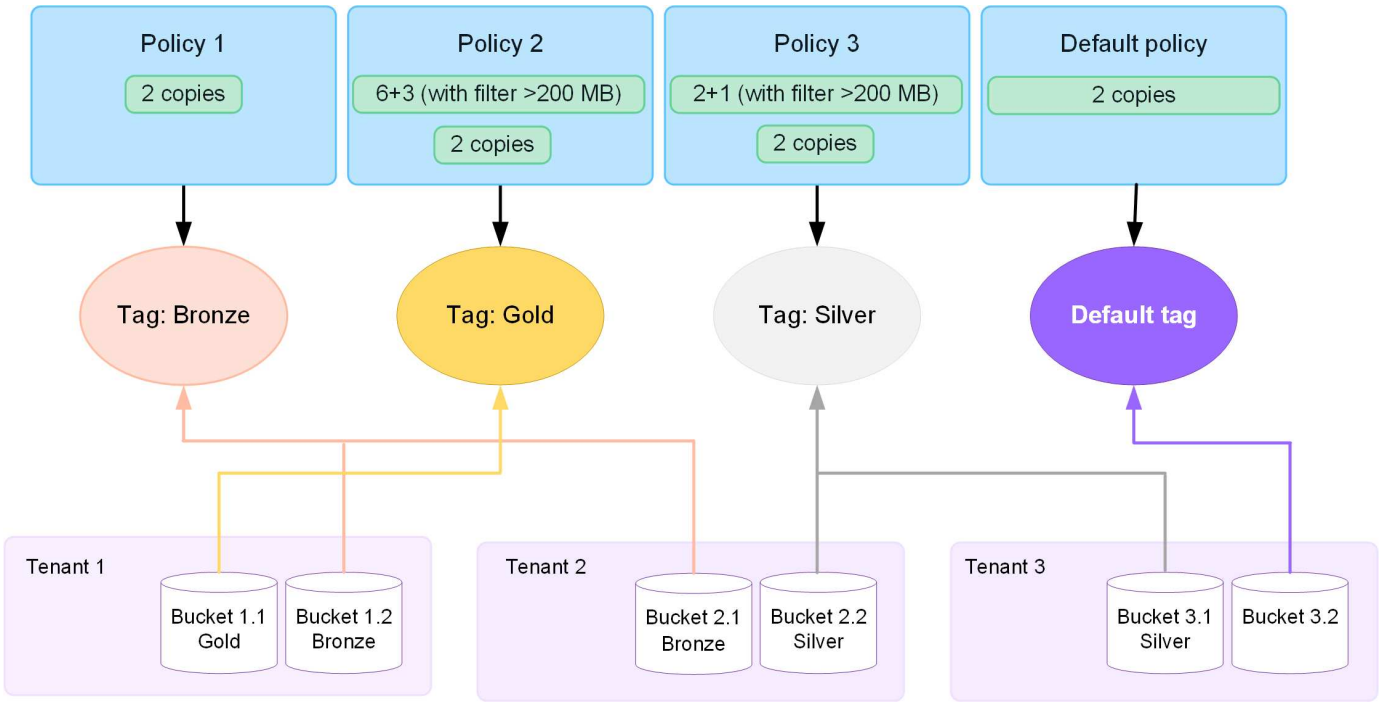
Etiquetas de políticas de ILM

Si desea permitir a los inquilinos cambiar fácilmente entre varias políticas de protección de datos por bloque, use varias políticas de ILM con *ILM policy tags*. Debe asignar cada política de ILM a una etiqueta y, a continuación, los inquilinos etiquetan un bloque para aplicar la política a ese bloque. Solo puede establecer etiquetas de políticas de ILM en bloques de S3.

Por ejemplo, puede tener tres etiquetas llamadas Gold, Silver y Bronze. Puede asignar una política de ILM a cada etiqueta, en función del tiempo y la ubicación en la que esa política almacena objetos. Los inquilinos pueden elegir la política que quieren usar etiquetando sus bloques. Un bloque con la etiqueta Gold se gestiona mediante la política Gold y recibe el nivel Gold de protección de datos y rendimiento.

Etiqueta de política de ILM predeterminada

Una etiqueta de política de ILM predeterminada se crea automáticamente al instalar StorageGRID. Cada cuadrícula debe tener una política activa asignada a la etiqueta predeterminada. La política predeterminada se aplica a todos los objetos de contenedores Swift y a todos los bloques S3 sin etiquetar.



¿Cómo evalúa objetos una política de ILM?

Una política de ILM activa controla la ubicación, la duración y la protección de datos de los objetos.

Cuando los clientes guardan objetos en StorageGRID, los objetos se evalúan con respecto al conjunto ordenado de reglas de ILM de la política, de la siguiente manera:

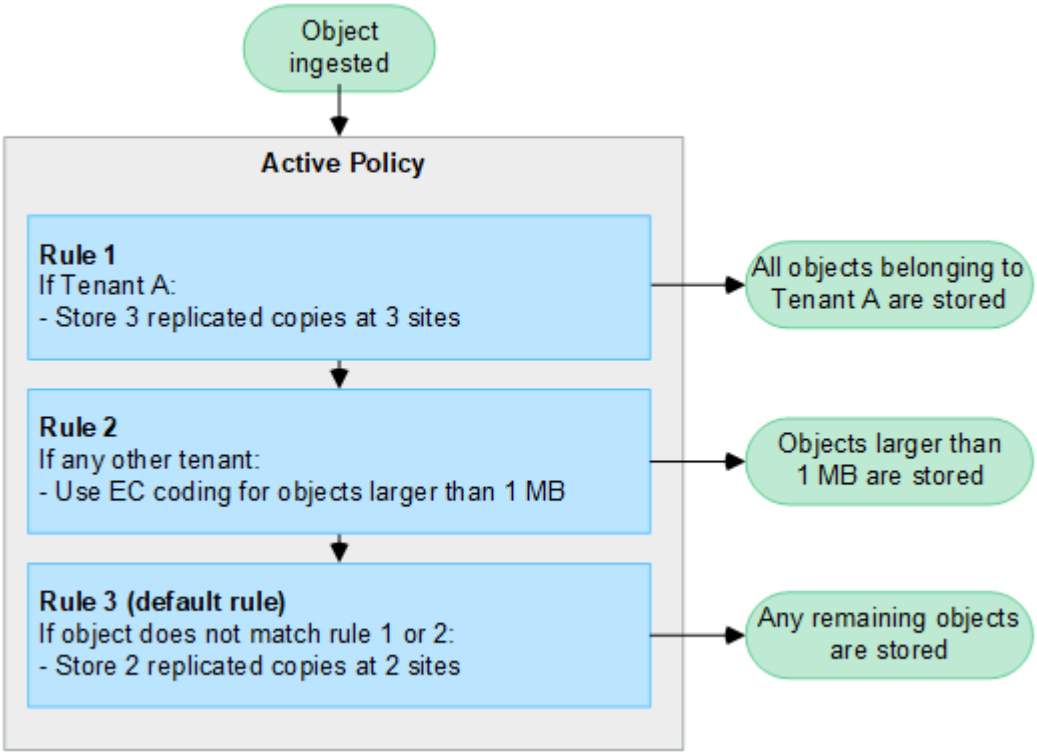
1. Si los filtros de la primera regla de la política coinciden con un objeto, el objeto se procesa según el comportamiento de procesamiento de esa regla y se almacena según las instrucciones de ubicación de esa regla.
2. Si los filtros de la primera regla no coinciden con el objeto, el objeto se evalúa con cada regla subsiguiente de la política hasta que se realiza una coincidencia.
3. Si ninguna regla coincide con un objeto, se aplican las instrucciones de comportamiento de procesamiento y colocación de la regla predeterminada de la directiva. La regla predeterminada es la última regla de una directiva. La regla predeterminada debe aplicarse a todos los inquilinos, a todos los cubos S3 o a los contenedores Swift y a todas las versiones de objetos y no puede utilizar ningún filtro avanzado.

Ejemplo de política de ILM

Por ejemplo, una política de ILM podría contener tres reglas de ILM que especifiquen lo siguiente:

- **Regla 1: Copias replicadas para el Inquilino A**
  - Haga coincidir todos los objetos que pertenecen al inquilino A..
  - Almacene estos objetos como tres copias replicadas en tres sitios.
  - Los objetos que pertenecen a otros arrendatarios no coinciden con la Regla 1, por lo que se evalúan según la Regla 2.
- **Regla 2: Codificación de borrado para objetos mayores de 1 MB**
  - Hacer coincidir todos los objetos de otros inquilinos, pero solo si son mayores de 1 MB. Estos objetos de mayor tamaño se almacenan mediante codificación de borrado 6+3 en tres instalaciones.
  - No coincide con los objetos de 1 MB o menos, por lo que estos objetos se evalúan con la Regla 3.

- **Regla 3: 2 copias 2 data centers** (predeterminado)
  - Es la última regla y la predeterminada de la política. No utiliza filtros.
  - Realice dos copias replicadas de todos los objetos que no coincidan con la Regla 1 o la Regla 2 (objetos que no pertenezcan al arrendatario A que tengan 1 MB o menos).



¿Qué son las políticas activas e inactivas?

Cada sistema StorageGRID debe tener al menos una política de ILM activa. Si desea tener más de una política de ILM activa, debe crear etiquetas de políticas de ILM y asignar una política a cada etiqueta. A continuación, los inquilinos aplican las etiquetas a bloques de S3. La política predeterminada se aplica a todos los objetos de los cubos que no tengan una etiqueta de política asignada.

Cuando se crea por primera vez una política de ILM, se seleccionan una o varias reglas de ILM y se organizan en un orden específico. Después de simular la política para confirmar su comportamiento, la activa.

Cuando activa una política de ILM, StorageGRID utiliza esa política para gestionar todos los objetos, incluidos los objetos existentes y los objetos que se acaban de procesar. Es posible que los objetos existentes se muevan a nuevas ubicaciones cuando se implementen las reglas de ILM en la nueva política.

Si activa más de una política de ILM a la vez, y los inquilinos aplican etiquetas de políticas a bloques de S3, los objetos de cada bloque se gestionarán según la política asignada a la etiqueta.

Un sistema StorageGRID realiza un seguimiento del historial de políticas que se han activado o desactivado.

Consideraciones que tener en cuenta para crear una política de ILM

- Utilice únicamente la política proporcionada por el sistema, la política de copias de línea base 2, en los sistemas de prueba. Para StorageGRID 11,6 y versiones anteriores, la regla Crear 2 copias en esta política utiliza el pool de almacenamiento Todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.

El pool de almacenamiento Todos los nodos de almacenamiento se crea automáticamente durante la instalación de StorageGRID 11,6 y versiones anteriores. Si actualiza a una versión posterior de StorageGRID, el pool de Todos los nodos de almacenamiento seguirá existiendo. Si instala StorageGRID 11,7 o una versión posterior como una instalación nueva, no se crea el pool Todos los nodos de almacenamiento.

- Al diseñar una nueva política, tenga en cuenta todos los diferentes tipos de objetos que se podrían procesar en el grid. Asegúrese de que la política incluye reglas para coincidir y colocar estos objetos según sea necesario.
- Mantenga la política de ILM de la forma más sencilla posible. Esto evita situaciones potencialmente peligrosas en las que los datos de objetos no se protegen como se deben realizar cambios en el sistema StorageGRID a lo largo del tiempo.
- Asegúrese de que las reglas de la política están en el orden correcto. Cuando se activa la directiva, las reglas del orden indicado evalúan los objetos nuevos y existentes, empezando por la parte superior. Por ejemplo, si la primera regla de una política coincide con un objeto, ese objeto no será evaluado por ninguna otra regla.
- La última regla de todas las políticas de ILM es la regla de ILM predeterminada, que no puede usar ningún filtro. Si un objeto no ha sido coincidente con otra regla, la regla predeterminada controla dónde se coloca ese objeto y durante cuánto tiempo se retiene.
- Antes de activar una nueva política, revise los cambios que realice la política en la ubicación de objetos existentes. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

Crear políticas de ILM

Cree una o más políticas de ILM para satisfacer sus requisitos de calidad de servicio.

Tener una política de ILM activa permite aplicar las mismas reglas de ILM a todos los inquilinos y bloques.

Tener varias políticas de ILM activas permite aplicar las reglas de ILM adecuadas a inquilinos y bloques específicos para satisfacer múltiples requisitos de calidad de servicio.

Cree una política de ILM

Acerca de esta tarea

Antes de crear su propia política, compruebe que "Política de ILM predeterminada" no cumple los requisitos de almacenamiento.

Utilice únicamente las políticas proporcionadas por el sistema, la política de 2 copias (para cuadrículas de un sitio) o la copia 1 por sitio (para cuadrículas de varios sitios), en los sistemas de prueba. Para StorageGRID 11,6 y versiones anteriores, la regla predeterminada de esta política utiliza el pool de almacenamiento Todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.

Si la "Se ha activado la configuración de bloqueo de objeto global S3", Debe asegurarse de que la política de ILM cumple con los requisitos de los depósitos que tienen S3 Object Lock activado. En esta sección, siga las instrucciones que mencionan tener S3 Object Lock habilitado.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".
- Ya tienes "Reglas de ILM creadas" En función de si el bloqueo de objetos S3 está activado.

  S3 Bloqueo de objetos no activado
  - Ya tienes "Se han creado las reglas de ILM" desea agregar a la política. Según sea necesario, puede guardar una política, crear reglas adicionales y, a continuación, editar la política para agregar las nuevas reglas.
  - Ya tienes "Se ha creado una regla de ILM predeterminada" que no contiene ningún filtro.

  S3 Bloqueo de objetos activado
  - La "La configuración de bloqueo de objetos global S3 ya está activada" Para el sistema StorageGRID.
  - Ya tienes "Se han creado las reglas de ILM conforme a las normativas y no conformes" desea agregar a la política. Según sea necesario, puede guardar una política, crear reglas adicionales y, a continuación, editar la política para agregar las nuevas reglas.
  - Ya tienes "Se ha creado una regla de ILM predeterminada" para la directiva que cumple con las normativas.

- Opcionalmente, ha visto el vídeo: "Vídeo: Políticas de gestión del ciclo de vida de la información en StorageGRID 11,8"

Consulte también "Cree una política de ILM: Información general".

Pasos

1. Seleccione **ILM** > **políticas**.

   Si la configuración global Bloqueo de objetos S3 está habilitada, la página de políticas de ILM indica qué reglas de ILM son compatibles.

2. Determine cómo se desea crear la política de ILM.

   Crear una nueva política
   a. Seleccione **Crear política**.

   Clone la política existente
   a. Seleccione la casilla de verificación de la política con la que desea comenzar y, a continuación, seleccione **Clonar**.

   Edite la política existente
   a. Si una política está inactiva, puede editarla. Seleccione la casilla de verificación para la política inactiva con la que desea comenzar y, a continuación, seleccione **Editar**.

3. En el campo **Nombre de la política**, introduzca un nombre único para la política.
4. Opcionalmente, en el campo **Motivo del cambio**, introduzca el motivo por el que está creando una nueva

política.

5. Para agregar reglas a la política, selecciona **Seleccionar reglas**. Seleccione un nombre de regla para ver la configuración de esa regla.

   Si está clonando una política:

   - Se seleccionan las reglas que utiliza la política que se está clonando.
   - Si la política que está clonando usa reglas sin filtros que no sean la regla predeterminada, se le solicitará que elimine todas las reglas, excepto una de ellas.
   - Si la regla predeterminada usa un filtro, se le solicitará que seleccione una nueva regla predeterminada.
   - Si la regla predeterminada no es la última regla, puede mover la regla al final de la nueva política.

S3 Bloqueo de objetos no activado

a. Seleccione una regla predeterminada para la política. Para crear una nueva regla predeterminada, seleccione **ILM rules page**.

   La regla predeterminada se aplica a cualquier objeto que no coincida con otra regla de la política. La regla predeterminada no puede utilizar ningún filtro y siempre se evalúa en último lugar.

   > No utilice la regla Make 2 copies como regla predeterminada para una política. La regla make 2 copies utiliza un único pool de almacenamiento, todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.

S3 Bloqueo de objetos activado

a. Seleccione una regla predeterminada para la política. Para crear una nueva regla predeterminada, seleccione **ILM rules page**.

   La lista de reglas contiene solo las reglas que son compatibles y no utilizan ningún filtro.

   > No utilice la regla Make 2 copies como regla predeterminada para una política. La regla make 2 copies utiliza un único pool de almacenamiento, todos los nodos de almacenamiento, que contiene todos los sitios. Si utiliza esta regla, es posible que se coloquen varias copias de un objeto en el mismo sitio.

b. Si necesita una regla “predeterminada” diferente para los objetos en cubos S3 no compatibles, seleccione **Incluir una regla sin filtros para cubos S3 no compatibles** y seleccione una regla no compatible que no use un filtro.

   Por ejemplo, es posible que desee utilizar un pool de almacenamiento en la nube para almacenar objetos en depósitos que no tienen S3 Object Lock habilitado.

   > Sólo puede seleccionar una regla no compatible que no utilice un filtro.

Consulte también "Ejemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3".

6. Cuando haya terminado de seleccionar la regla predeterminada, seleccione **Continuar**.
7. Para el paso Otras reglas, seleccione cualquier otra regla que desee agregar a la política. Estas reglas utilizan al menos un filtro (cuenta de arrendatario, nombre de depósito, filtro avanzado o tiempo de referencia no actual). Luego selecciona **Seleccionar**.

   La ventana Crear una política muestra ahora las reglas seleccionadas. La regla predeterminada está al final, con las demás reglas encima.

   Si el bloqueo de objetos S3 está activado y también ha seleccionado una regla predeterminada no compatible, dicha regla se agrega como la segunda regla en la política.

   > Aparece una advertencia si alguna regla no retiene los objetos para siempre. Al activar esta política, debe confirmar que desea que StorageGRID elimine objetos cuando transcurran las instrucciones de colocación de la regla por defecto (a menos que un ciclo de vida del depósito mantenga los objetos durante un período de tiempo más largo).

8. Arrastre las filas de las reglas no predeterminadas para determinar el orden en el que se evaluarán estas reglas.

   No puede mover la regla predeterminada. Si el bloqueo de objetos S3 está activado, tampoco puede mover la regla predeterminada no compatible si se ha seleccionado una.

   > Debe confirmar que las reglas de ILM se encuentran en el orden correcto. Cuando se activa la directiva, las reglas del orden indicado evalúan los objetos nuevos y existentes, empezando por la parte superior.

9. Según sea necesario, seleccione **Seleccionar reglas** para agregar o eliminar reglas.
10. Cuando haya terminado, seleccione **Guardar**.
11. Repita estos pasos para crear políticas de ILM adicionales.
12. Simule una política de gestión de la vida útil. Siempre debe simular una política antes de activarla para asegurarse de que funciona como se esperaba.

Simular una política

Simule una política sobre objetos de prueba antes de activar la política y aplicarla a los datos de producción.

Antes de empezar

- Conoce el bloque/clave-objeto de S3 o el contenedor/nombre-objeto Swift para cada objeto que desea probar.

Pasos

1. Use un cliente S3 o Swift o el "S3 Consola", ingerir los objetos necesarios para probar cada regla.
2. En la página de políticas de ILM, seleccione la casilla de verificación de la política y, a continuación, seleccione **Simular**.
3. En el campo **Object**, ingrese el S3 `bucket/object-key` O el Swift `container/object-name` para un objeto de prueba. Por ejemplo: `bucket-01/filename.png`.
4. Si el control de versiones S3 está activado, opcionalmente introduzca un ID de versión para el objeto en el campo **ID de versión**.
5. Seleccione **simular**.

6. En la sección Resultados de Simulation, confirme que la regla correcta coincide con cada objeto.
7. Para determinar qué pool de almacenamiento o perfil de código de borrado está en vigor, seleccione el nombre de la regla coincidente para ir a la página de detalles de regla.

> Revise cualquier cambio en la ubicación de los objetos existentes replicados y con código de borrado. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

Resultados

Cualquier modificación de las reglas de la política se reflejará en los resultados de Simulation y mostrará la nueva coincidencia y la anterior. La ventana de política de simulación conserva los objetos que ha probado hasta que seleccione **Borrar todo** o el icono Eliminar ✕ Para cada objeto de la lista de resultados de Simulation.

Información relacionada

"Ejemplo de simulaciones de políticas de ILM"

Activar una política

Cuando se activa una única nueva política de ILM, los objetos existentes y los objetos recién procesados se gestionan con esa política. Al activar varias políticas, las etiquetas de políticas de ILM asignadas a bloques determinan los objetos que se van a gestionar.

Antes de activar una nueva política:

1. Simule la política para confirmar que se comporta como se espera.
2. Revise cualquier cambio en la ubicación de los objetos existentes replicados y con código de borrado. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

> Los errores de un política de ILM pueden provocar la pérdida de datos irrecuperable.

Acerca de esta tarea

Cuando activa una política de ILM, el sistema distribuye la nueva política a todos los nodos. Sin embargo, es posible que la nueva directiva activa no surta efecto hasta que todos los nodos de grid estén disponibles para recibir la nueva directiva. En algunos casos, el sistema espera implementar una nueva política activa para garantizar que los objetos de cuadrícula no se eliminen accidentalmente. Específicamente:

- Si realiza cambios en las políticas que **aumenten la redundancia o durabilidad de los datos**, esos cambios se implementarán inmediatamente. Por ejemplo, si activa una nueva política que incluye una regla de tres copias en lugar de una regla de dos copias, dicha política se implementará de forma inmediata porque aumenta la redundancia de datos.
- Si realiza cambios de política que **podrían disminuir la redundancia o durabilidad de los datos**, esos cambios no se implementarán hasta que todos los nodos de la red estén disponibles. Por ejemplo, si activa una nueva política que utiliza una regla de dos copias en lugar de una regla de tres copias, la nueva política aparecerá en la pestaña Política activa, pero no surtirá efecto hasta que todos los nodos estén en línea y disponibles.

Pasos

Siga los pasos para activar una política o varias políticas:

Active una política

Siga estos pasos si sólo tendrá una política activa. Si ya tiene una o más políticas activas y está activando políticas adicionales, siga los pasos para activar varias políticas.

1. Cuando esté listo para activar una política, seleccione **ILM** > **Políticas**.

   Alternativamente, puede activar una sola política desde la página **ILM** > **Etiquetas de política**.

2. En la pestaña Políticas, seleccione la casilla de verificación de la política que desea activar y, a continuación, seleccione **Activar**.
3. Siga el paso apropiado:
   - Si un mensaje de advertencia le pide que confirme que desea activar la directiva, seleccione **Aceptar**.
   - Si aparece un mensaje de advertencia que contiene detalles sobre la política:
     i. Revise los detalles para asegurarse de que la política gestionaría los datos según lo esperado.
     ii. Si la regla predeterminada almacena objetos durante un número limitado de días, revise el diagrama de retención y, a continuación, escriba ese número de días en el cuadro de texto.
     iii. Si la regla predeterminada almacena objetos para siempre, pero una o más reglas tienen retención limitada, escriba **sí** en el cuadro de texto.
     iv. Seleccione **Activar política**.

Activar varias políticas

Para activar varias políticas, debe crear etiquetas y asignar una política a cada etiqueta.

> Cuando hay varias etiquetas en uso, si los inquilinos reasignan frecuentemente las etiquetas de política a los buckets, el rendimiento de los grid puede verse afectado. Si tiene inquilinos que no son de confianza, considere la posibilidad de usar solo la etiqueta predeterminada.

1. Selecciona **ILM** > **Etiquetas de política**.
2. Seleccione **Crear**.
3. En el cuadro de diálogo Crear etiqueta de política, escriba un nombre de etiqueta y, opcionalmente, una descripción para la etiqueta.

   > Los nombres y las descripciones de las etiquetas son visibles para los inquilinos. Elija valores que ayuden a los inquilinos a tomar una decisión informada al seleccionar etiquetas de política para asignarlas a sus bloques. Por ejemplo, si la política asignada suprimirá objetos después de un período de tiempo, podría comunicarlo en la descripción. No incluya información confidencial en estos campos.

4. Seleccione **Crear etiqueta**.
5. En la tabla de etiquetas de políticas de ILM, use el menú desplegable para seleccionar una política y asignarla.
6. Si aparecen advertencias en la columna Limitaciones de política, seleccione **Ver detalles de política** para revisar la política.

7. Asegúrese de que cada política gestionara los datos según lo previsto.
8. Selecciona **Activar políticas asignadas**. O bien, seleccione **Borrar cambios** para eliminar la asignación de la política.
9. En el cuadro de diálogo Activar políticas con nuevas etiquetas, revise las descripciones de cómo gestionarán los objetos cada etiqueta, política y regla. Realice los cambios necesarios para garantizar que las políticas gestionen los objetos según lo esperado.
10. Cuando esté seguro de que desea activar las políticas, escriba **sí** en el cuadro de texto y, a continuación, seleccione **Activar políticas**.

Información relacionada

"Ejemplo 6: Cambiar una política de ILM"

Ejemplo de simulaciones de políticas de ILM

Los ejemplos de simulaciones de políticas de ILM ofrecen directrices para estructurar y modificar simulaciones para su entorno.

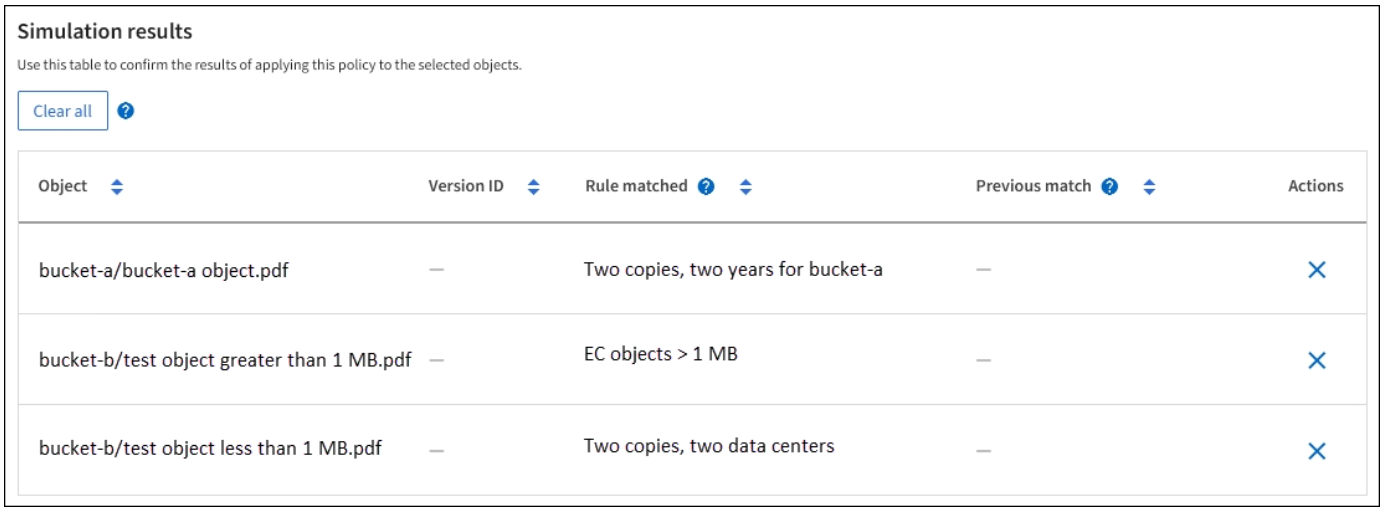
Ejemplo 1: Verifique las reglas al simular una política de ILM

En este ejemplo se describe cómo verificar reglas al simular una política.

En este ejemplo, la **política de ILM de ejemplo** se está simulando contra los objetos ingeridos en dos bloques. La política incluye tres reglas, como sigue:

- La primera regla, **dos copias, dos años para el segmento a**, se aplica sólo a los objetos en el bloque a.
- La segunda regla, **objetos EC > 1 MB**, se aplica a todos los cubos pero filtra a los objetos superiores a 1 MB.
- La tercera regla, **dos copias, dos centros de datos**, es la regla por defecto. No incluye ningún filtro ni utiliza el tiempo de referencia no corriente.

Después de simular la política, confirme que cada objeto ha coincidido con la regla correcta.



En este ejemplo:

- `bucket-a/bucket-a object.pdf` coincide correctamente con la primera regla, que filtra los objetos de

`bucket-a`.

- `bucket-b/test object greater than 1 MB.pdf` está en `bucket-b`, así que no coincide con la primera regla. En lugar de ello, la segunda regla coincide correctamente, que filtra los objetos de más de 1 MB.
- `bucket-b/test object less than 1 MB.pdf` no coincide con los filtros de las dos primeras reglas, por lo que se colocará por la regla predeterminada, que no incluye ningún filtro.

Ejemplo 2: Reordenar reglas al simular una política de ILM

En este ejemplo se muestra cómo puede reordenar las reglas para cambiar los resultados al simular una directiva.

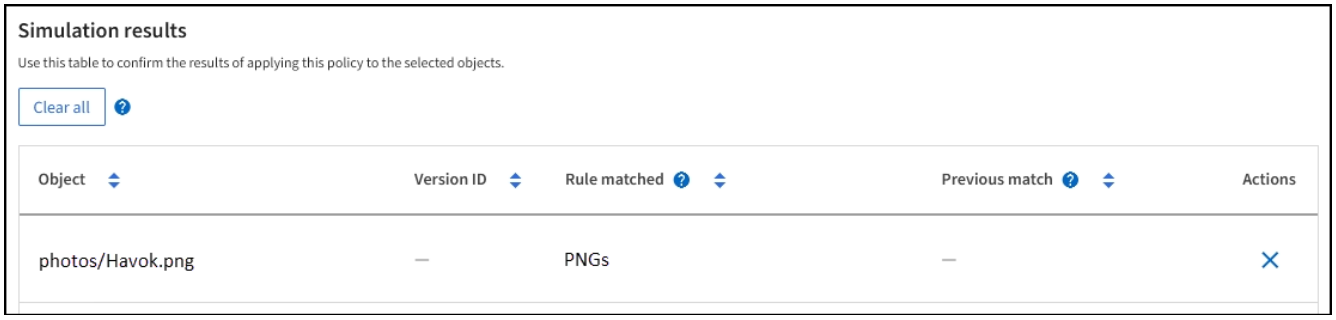
En este ejemplo, se está simulando la política **Demo**. Esta política, que está destinada a encontrar objetos que tienen metadatos de usuario de series=x-men, incluye tres reglas de la siguiente manera:

- La primera regla, **PNgs**, filtra los nombres de clave que terminan en `.png`.
- La segunda regla, **X-men**, se aplica sólo a los objetos para el arrendatario A y filtros para `series=x-men` metadatos del usuario.
- La última regla, **dos copias de dos centros de datos**, es la regla predeterminada, que coincide con cualquier objeto que no coincida con las dos primeras reglas.

Pasos

1. Después de agregar las reglas y guardar la directiva, seleccione **simular**.
2. En el campo **Object**, introduzca el bucket/object-key de S3 o el nombre de objeto/contenedor de Swift para un objeto de prueba y seleccione **Simulate**.

   Aparecen los resultados de Simulation, que muestran la `Havok.png` El objeto coincide con la regla **PNgs**.

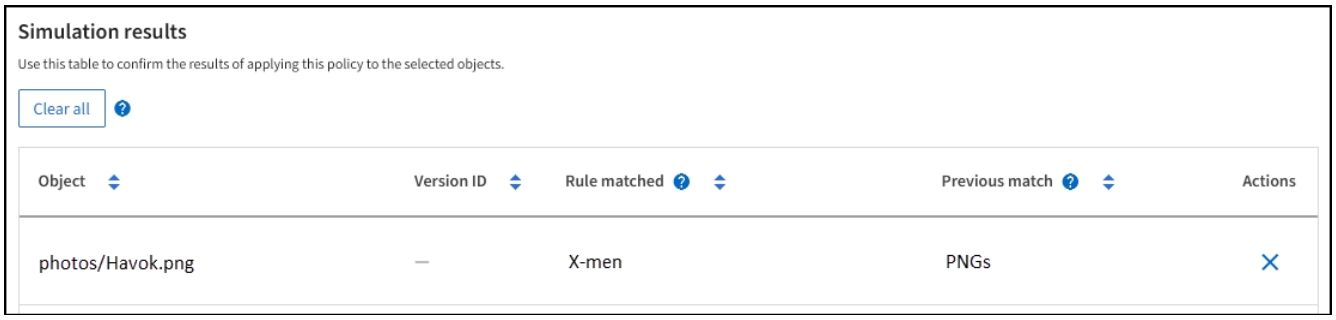


   Sin embargo, `Havok.png` Estaba destinado a probar la regla **X-MEN**.

3. Para resolver el problema, vuelva a ordenar las reglas.
   a. Seleccione **Finish** para cerrar la ventana Simulate ILM Policy.
   b. Seleccione **Editar** para editar la directiva.
   c. Arrastre la regla **X-men** hasta la parte superior de la lista.
   d. Seleccione **Guardar**.
4. Seleccione **simular**.

   Los objetos probados anteriormente se vuelven a evaluar con la directiva actualizada y se muestran los nuevos resultados de simulación. En el ejemplo, la columna Regla coincidente muestra que la `Havok.png`

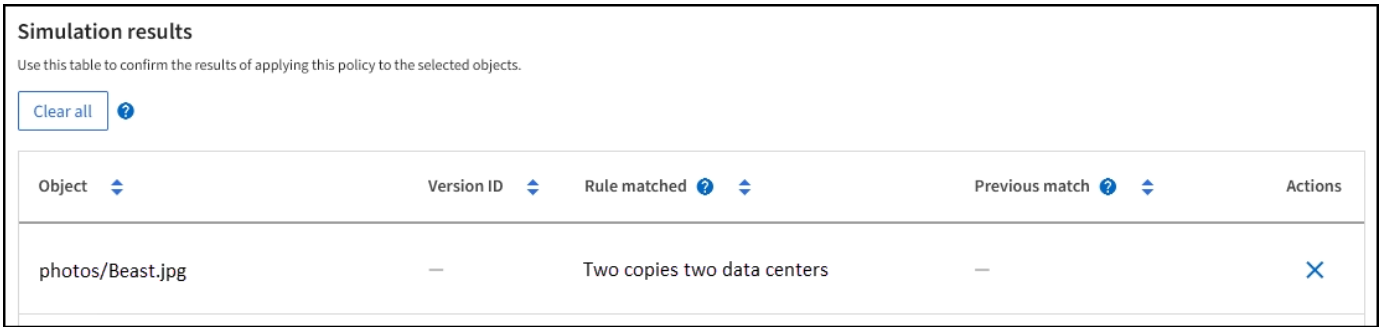
Ahora Object coincide con la regla de metadatos X-men, según lo esperado. La columna Coincidencia anterior muestra que la regla NGs coincide con el objeto en la simulación anterior.



Ejemplo 3: Corrija una regla al simular una política de ILM

Este ejemplo muestra cómo simular una política, corregir una regla en la política y continuar con la simulación.

En este ejemplo, se está simulando la política **Demo**. Esta política está destinada a encontrar objetos que tienen `series=x-men` metadatos del usuario. Sin embargo, se produjeron resultados inesperados al simular esta política con la `Beast.jpg` objeto. En lugar de coincidir con la regla de metadatos de X-men, el objeto coincide con la regla predeterminada, dos copias de dos centros de datos.



Cuando un objeto de prueba no coincide con la regla esperada de la directiva, debe examinar cada regla de la directiva y corregir cualquier error.

Pasos

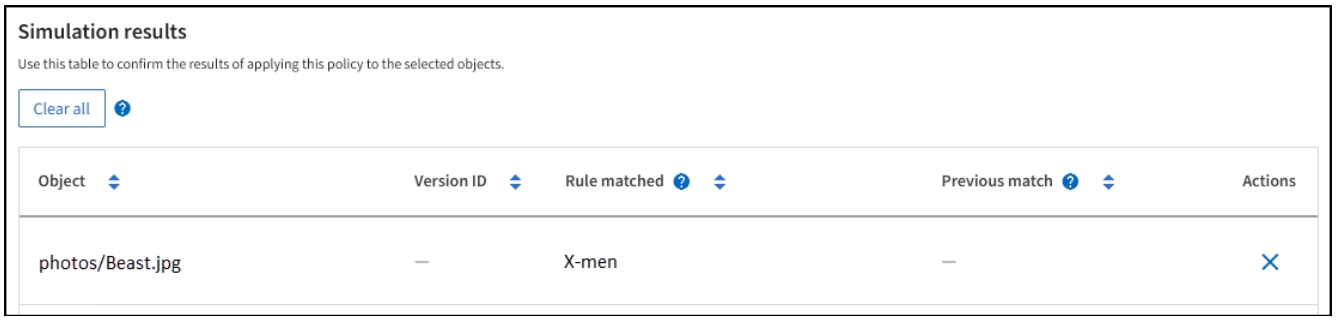
1. Seleccione **Finalizar** para cerrar el diálogo de políticas de simulación. En la página de detalles de la política, seleccione **Diagrama de retención**. A continuación, seleccione **Expandir todo** o **Ver detalles** para cada regla según sea necesario.
2. Revise la cuenta de arrendatario de la regla, el tiempo de referencia y los criterios de filtrado.

   Como ejemplo, supongamos que los metadatos para la regla X-men se ingresaron como “x-men01” en lugar de “x-men”.

3. Para resolver el error, corrija la regla de la siguiente manera:
   - Si la regla forma parte de la política, puede clonar la regla o eliminar la regla de la política y, a continuación, editarla.
   - Si la regla forma parte de la política activa, debe clonar esa regla. No puede editar ni eliminar una regla de la política activa.
4. Vuelva a ejecutar la simulación.

   En este ejemplo, la regla X-men corregida ahora coincide con `Beast.jpg` objeto basado en `series=x-`

`men` los metadatos del usuario, según lo esperado.



Gestione etiquetas de políticas de ILM

Puede ver detalles de etiqueta de política de ILM, editar una etiqueta o quitar una etiqueta.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "permisos de acceso requeridos".

Vea los detalles de la etiqueta de la política de ILM

Para ver los detalles de una etiqueta:

1. Selecciona **ILM** > **Etiquetas de política**.
2. Seleccione el nombre de la política de la tabla. Aparece la página de detalles de la etiqueta.
3. En la página de detalles, vea el historial anterior de políticas asignadas.
4. Para ver una política, selecciónela.

Editar la etiqueta de política de ILM

> Los nombres y las descripciones de las etiquetas son visibles para los inquilinos. Elija valores que ayuden a los inquilinos a tomar una decisión informada al seleccionar etiquetas de política para asignarlas a sus bloques. Por ejemplo, si la política asignada suprimirá objetos después de un período de tiempo, podría comunicarlo en la descripción. No incluya información confidencial en estos campos.

Para editar la descripción de una etiqueta existente:

1. Selecciona **ILM** > **Etiquetas de política**.
2. Seleccione la casilla de verificación para la etiqueta y luego seleccione **Editar**.

   También puede seleccionar el nombre de la etiqueta. Aparece la página de detalles de la etiqueta, y puede seleccionar **Editar** en esa página.

3. Cambie la descripción de la etiqueta según sea necesario
4. Seleccione **Guardar**.

Quite la etiqueta de política de ILM

Al eliminar una etiqueta de política, se aplicará la política por defecto a todos los depósitos asignados a esa etiqueta.

Para eliminar una etiqueta:

1. Selecciona **ILM** > **Etiquetas de política**.
2. Seleccione la casilla de verificación para la etiqueta y luego seleccione * Eliminar *. Se muestra un cuadro de diálogo de confirmación.

   También puede seleccionar el nombre de la etiqueta. Aparece la página de detalles de la etiqueta, y puede seleccionar **Eliminar** en esa página.

3. Seleccione **Sí** para eliminar la etiqueta.

Comprobar una política de ILM con la búsqueda de metadatos de objetos

Después de activar una política de ILM, debe procesar objetos de prueba representativos en el sistema StorageGRID. A continuación, debe realizar una búsqueda de metadatos de objetos para confirmar que las copias se están creando como intencionadas y se encuentran en las ubicaciones correctas.

Antes de empezar

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

Pasos

1. Procese el objeto.
2. Seleccione **ILM** > **Búsqueda de metadatos de objetos**.
3. Escriba el identificador del objeto en el campo **Identificador**. Es posible introducir un UUID, CBID, bucket/object-key de S3 o nombre de objeto/contenedor de Swift.
4. De manera opcional, introduzca un ID de versión para el objeto (solo S3).
5. Seleccione **Buscar**.

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

   - Metadatos del sistema, incluidos:
     - Identificador de objeto (UUID)

    - nombre del objeto
    - nombre del contenedor
    - Tipo de resultado (objeto, marcador de borrado, cubo S3 o contenedor Swift)
    - Nombre o ID de cuenta de inquilino
    - el tamaño lógico del objeto
    - fecha y hora de creación del objeto por primera vez
    - fecha y hora de la última modificación del 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.

    > ⓘ La siguiente captura de pantalla es un ejemplo. Los resultados variarán en función de la versión de StorageGRID.

System Metadata

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

Replicated Copies

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

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


6. Confirme que el objeto se almacena en la ubicación o las ubicaciones correctas y que es el tipo de copia correcto.

> Si la opción Auditoría está activada, también puede supervisar el registro de auditoría del mensaje ORLM Object Rules met. El mensaje de auditoría ORLM puede proporcionarle más información sobre el estado del proceso de evaluación de ILM, pero no puede proporcionar información sobre la corrección de la ubicación de los datos de objetos ni la integridad de la política de ILM. Debe evaluar esto usted mismo. Para obtener más información, consulte "Revisar los registros de auditoría".

Información relacionada

- "USE LA API DE REST DE S3"
- "Use la API DE REST de Swift"

Funciona con políticas de ILM y reglas de ILM

A medida que cambian sus requisitos de almacenamiento, es posible que deba

implementar más políticas o modificar las reglas de ILM asociadas con una política. Puede ver las métricas de ILM para determinar el rendimiento del sistema.

Antes de empezar

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

Vea las políticas de ILM

Para ver las políticas de ILM activas e inactivas y el historial de activación de políticas:

1. Seleccione **ILM** > **políticas**.
2. Selecciona **Políticas** para ver una lista de políticas activas e inactivas. La tabla muestra el nombre de cada política, las etiquetas a las que está asignada la política y si la política está activa o inactiva.
3. Selecciona **Historial de activación** para ver una lista de las fechas de inicio y finalización de la activación de las políticas.
4. Seleccione un nombre de política para ver los detalles de la política.

> Si ve los detalles de una política cuyo estado se ha editado o eliminado, aparecerá un mensaje en el que se explica que está viendo la versión de la política que estaba activa para el intervalo de tiempo especificado y que se ha editado o suprimido desde entonces.

Editar una política de ILM

Sólo puede editar una política inactiva. Si desea editar una política activa, desactívela o cree un clon y edítelo.

Para editar una política:

1. Seleccione **ILM** > **políticas**.
2. Seleccione la casilla de verificación de la política que desea editar y, a continuación, seleccione **Editar**.
3. Edite la política siguiendo las instrucciones de "Crear políticas de ILM".
4. Simule la política antes de volver a activarla.

> Una política de ILM que se configuró incorrectamente puede provocar la pérdida de datos irrecuperable. Antes de activar una política de ILM, revise con detenimiento la política de ILM y sus reglas de ILM, y simule la política de ILM. Confirme siempre que la política de gestión del ciclo de vida de la información funcionará como se pretende.

Clonar una política de ILM

Para clonar una política de ILM:

1. Seleccione **ILM** > **políticas**.
2. Seleccione la casilla de verificación de la política que desea clonar y luego seleccione **Clonar**.
3. Cree una nueva política que empiece por la política que ha clonado siguiendo las instrucciones de "Crear políticas de ILM".

Una política de ILM que se configuró incorrectamente puede provocar la pérdida de datos irrecuperable. Antes de activar una política de ILM, revise con detenimiento la política de ILM y sus reglas de ILM, y simule la política de ILM. Confirme siempre que la política de gestión del ciclo de vida de la información funcionará como se pretende.

Quitar una política de ILM

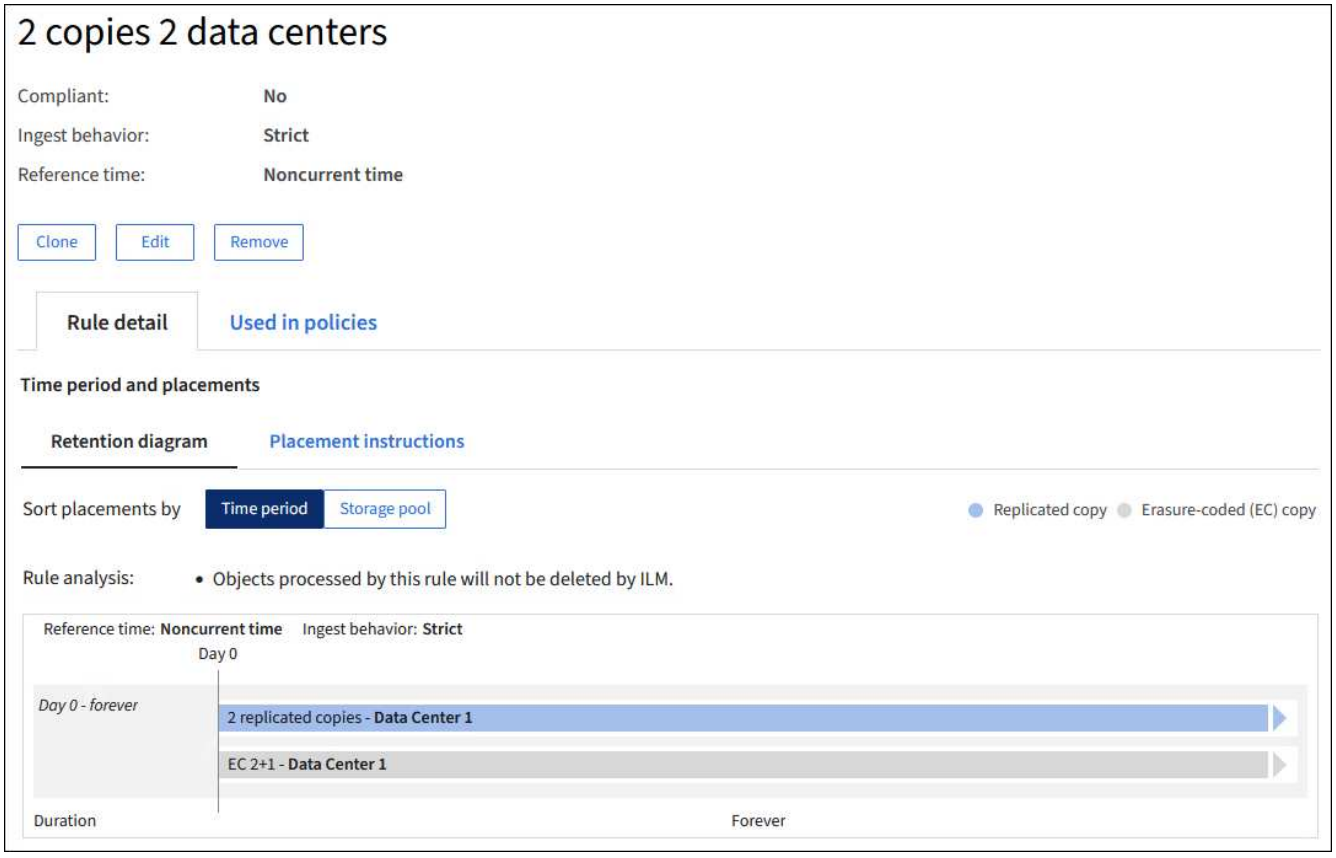
Solo puede quitar una política de ILM si está inactiva. Para eliminar una política:

1. Seleccione **ILM** > **políticas**.
2. Seleccione la casilla de verificación para la política inactiva que desea eliminar.
3. Seleccione **Quitar**.

Vea los detalles de las reglas de ILM

Para ver los detalles de una regla de ILM, incluido el diagrama de retención y las instrucciones de colocación de la regla:

1. Selecciona **ILM** > **Reglas**.
2. Seleccione el nombre de la regla cuyos detalles desea ver. Ejemplo:



Además, puede utilizar la página de detalles para clonar, editar o eliminar una regla. No puede editar o eliminar una regla si se utiliza en alguna política.

Clonar una regla de ILM

Puede clonar una regla existente si desea crear una nueva regla que utilice algunos de los valores de la regla existente. Si necesita editar una regla que se utiliza en cualquier política, clone la regla en su lugar y realice cambios en el clon. Después de realizar cambios en el clon, puede eliminar la regla original de la política y sustituirla por la versión modificada según sea necesario.

> No puede clonar una regla de gestión de la vida útil de la información si se creó con StorageGRID versión 10,2 o anterior.

Pasos

1. Selecciona **ILM** > **Reglas**.
2. Seleccione la casilla de verificación para la regla que desea clonar y luego seleccione **Clonar**. Como alternativa, seleccione el nombre de la regla y, a continuación, seleccione **Clonar** en la página de detalles de la regla.
3. Actualice la regla clonada siguiendo los pasos para Editar una regla de ILM y.. "Usar filtros avanzados en reglas de ILM".

   Al clonar una regla de ILM, debe introducir un nombre nuevo.

Editar una regla de ILM

Es posible que deba editar una regla de ILM para cambiar un filtro o una instrucción de ubicación.

No puede editar una regla si se utiliza en alguna política de ILM. En cambio, puedes hacerlo clonar la regla y realice los cambios necesarios en la copia clonada.

> Una política de ILM que se configuró incorrectamente puede provocar la pérdida de datos irrecuperable. Antes de activar una política de ILM, revise con detenimiento la política de ILM y sus reglas de ILM, y simule la política de ILM. Confirme siempre que la política de gestión del ciclo de vida de la información funcionará como se pretende.

Pasos

1. Selecciona **ILM** > **Reglas**.
2. Confirme que la regla que desea editar no se utiliza en ninguna política de ILM.
3. Si la regla que desea editar no está en uso, seleccione la casilla de verificación de la regla y seleccione * Acciones * > * Editar **. Alternativamente, seleccione el nombre de la regla y luego seleccione *Editar** en la página de detalles de la regla.
4. Complete los pasos del asistente Edit ILM Rule. Según sea necesario, siga los pasos de "Creación de una regla de ILM" y.. "Usar filtros avanzados en reglas de ILM".

   Al editar una regla de ILM, no es posible cambiar su nombre.

Quite una regla de ILM

Para que la lista de reglas de ILM actuales sea gestionable, elimine las reglas de ILM que probablemente no use.

Pasos

Para eliminar una regla de ILM utilizada actualmente en una política activa:

1. Clone la política.
2. Quite la regla de ILM del clon de políticas.
3. Guarde, simule y active la nueva directiva para asegurarse de que los objetos están protegidos como se espera.
4. Vaya a los pasos para eliminar una regla de ILM utilizada actualmente en una política inactiva.

Para eliminar una regla de ILM utilizada actualmente en una política inactiva:

1. Seleccione la política inactiva.
2. Quite la regla de ILM de la política o. elimine la política.
3. Vaya a los pasos para eliminar una regla de ILM que no está en uso actualmente.

Para eliminar una regla de ILM que no se está utilizando actualmente:

1. Selecciona **ILM** > **Reglas**.
2. Confirme que la regla que desea eliminar no se utiliza en ninguna política.
3. Si la regla que desea eliminar no está en uso, seleccione la regla y seleccione * Acciones * > * Eliminar *. Puede seleccionar varias reglas y eliminarlas todas al mismo tiempo.
4. Seleccione **Sí** para confirmar que desea eliminar la regla de ILM.

Ver las métricas de ILM

Se pueden ver métricas para ILM, como el número de objetos de la cola y la tasa de evaluación. Puede supervisar estas métricas para determinar el rendimiento del sistema. Una cola grande o una tasa de evaluación puede indicar que el sistema no es capaz de mantener el ritmo de la tasa de consumo, la carga de las aplicaciones cliente es excesiva o que existe alguna condición anormal.

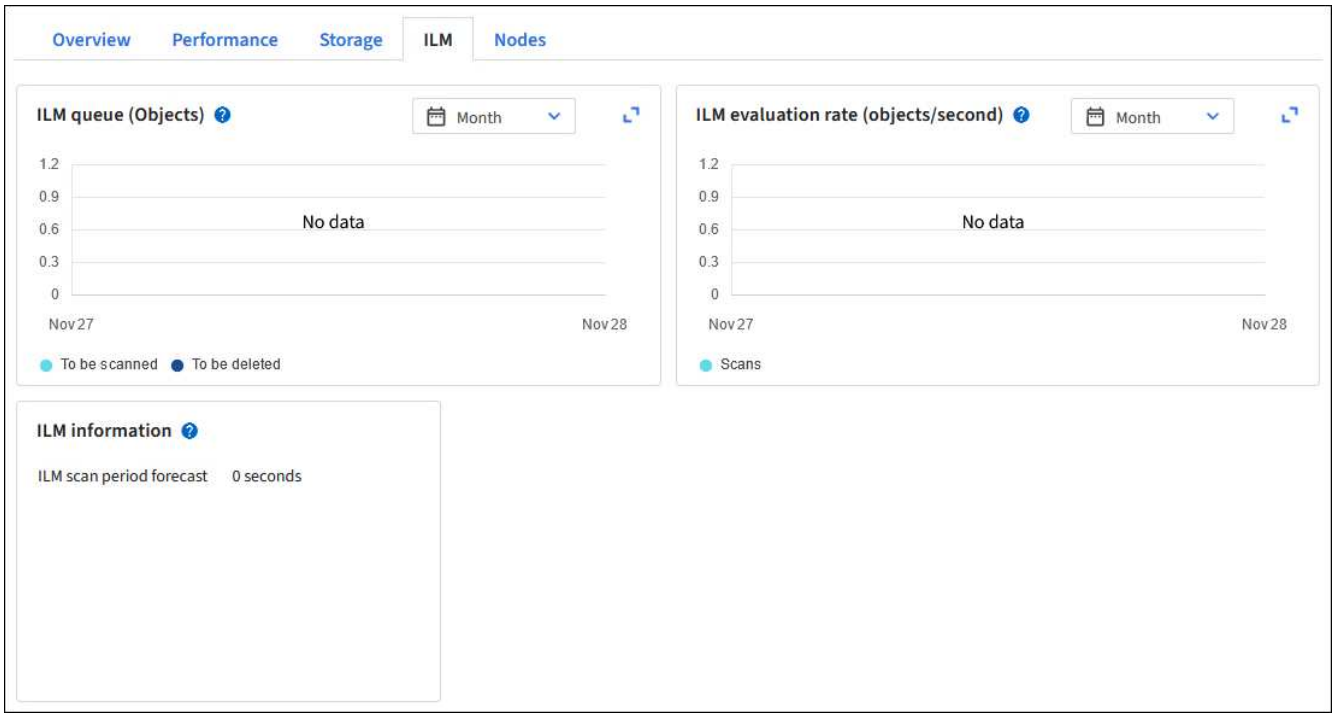
Pasos

1. Selecciona **Dashboard** > **ILM**.

   Como la consola se puede personalizar, es posible que la pestaña ILM no esté disponible.

2. Supervise las métricas en la pestaña ILM.

   Puede seleccionar el signo de interrogación Para ver una descripción de los elementos en la pestaña ILM.



Utilice el bloqueo de objetos de S3

Gestione objetos con S3 Object Lock

Como administrador de grid, puede habilitar el bloqueo de objetos de S3 GB en su sistema StorageGRID e implementar una política de gestión del ciclo de vida de la información conforme a la normativa para garantizar que los objetos de bloques de S3 específicos no se eliminen ni se sobrescriban durante un período de tiempo determinado.

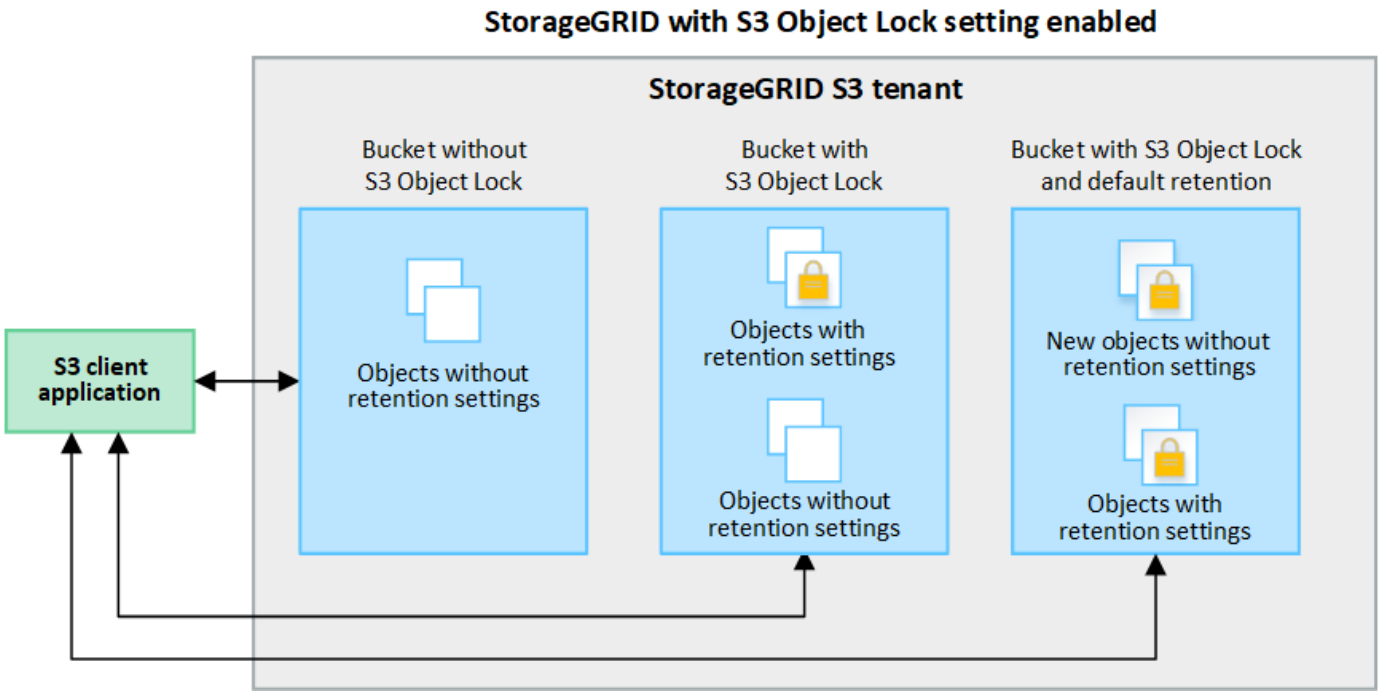
¿Qué es el bloqueo de objetos de S3?

La función StorageGRID S3 Object Lock es una solución de protección de objetos equivalente a S3 Object Lock en Amazon simple Storage Service (Amazon S3).

Tal y como se muestra en la figura, cuando se habilita la opción global de bloqueo de objetos de S3 para un sistema StorageGRID, una cuenta de inquilino de S3 puede crear bloques con o sin la función de bloqueo de objetos de S3 habilitada. Si un bucket tiene S3 Object Lock habilitado, se requiere el control de versiones de bucket y se habilita automáticamente.

Si un bucket tiene S3 Object Lock habilitado, las aplicaciones cliente S3 pueden especificar, de manera opcional, la configuración de retención para cualquier versión de objeto guardada en ese bucket.

Además, un bloque que tiene S3 Object Lock habilitado puede tener opcionalmente un modo de retención y un período de retención predeterminados. La configuración predeterminada se aplica solo a los objetos que se agregan al depósito sin su propia configuración de retención.



Modos de retención

La función de bloqueo de objetos StorageGRID S3 admite dos modos de retención para aplicar diferentes niveles de protección a los objetos. Estos modos son equivalentes a los modos de retención de Amazon S3.

- En modo de cumplimiento:
  - El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta.
  - La fecha de retención del objeto se puede aumentar, pero no se puede reducir.
  - No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha.
- En modo de gobierno:
  - Los usuarios con permiso especial pueden utilizar un encabezado de omisión en las solicitudes para modificar ciertos valores de retención.
  - Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha.
  - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

Configuración de retención para versiones de objetos

Si se crea un depósito con S3 Object Lock habilitado, los usuarios pueden utilizar la aplicación cliente S3 para especificar opcionalmente los siguientes valores de retención para cada objeto que se agregue al depósito:

- **Modo de retención**: Ya sea cumplimiento o gobierno.
- **Retain-until-date**: Si la fecha de retención de una versión de objeto está en el futuro, el objeto se puede recuperar, pero no se puede eliminar.
- **Retención legal**: La aplicación de una retención legal a una versión de objeto bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesite poner una retención legal en un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, pero permanece en su lugar hasta que se elimina explícitamente. La retención legal es independiente de la retención hasta la fecha.

Si un objeto se encuentra bajo una conservación legal, nadie puede eliminarlo, independientemente de su modo de retención.

Para obtener más información sobre la configuración del objeto, consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3".

Valor de retención predeterminado para los depósitos

Si se crea un depósito con S3 Object Lock habilitado, los usuarios pueden especificar opcionalmente los siguientes ajustes predeterminados para el bloque:

- **Modo de retención predeterminado**: Ya sea cumplimiento o gobierno.
- **Período de retención predeterminado**: Cuánto tiempo deben conservarse las nuevas versiones de objetos añadidas a este depósito, a partir del día en que se agregan.

La configuración de bloque predeterminada se aplica solo a objetos nuevos que no tienen su propia configuración de retención. Los objetos de cubo existentes no se ven afectados al agregar o cambiar estos valores predeterminados.

Consulte "Cree un bloque de S3" y.. "Actualizar S3 Retención predeterminada de bloqueo de objetos".

Comparación del bloqueo de objetos de S3 con el cumplimiento de normativas heredado

El bloqueo de objetos de S3 sustituye la función de cumplimiento de normativas que estaba disponible en versiones anteriores de StorageGRID. Debido a que la función Bloqueo de objetos de S3 cumple con los requisitos de Amazon S3, deja en obsoletos la característica de cumplimiento de normativas de StorageGRID, que ahora se conoce como “Cumplimiento de normativas heredado”.

La configuración de cumplimiento global está anticuada. Si ha habilitado esta configuración con una versión anterior de StorageGRID, la configuración Bloqueo de objetos S3 se activa automáticamente. Puede seguir usando StorageGRID para gestionar la configuración de los buckets compatibles existentes; sin embargo, no puede crear nuevos buckets compatibles. Para obtener más información, consulte "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5".

Si ha utilizado la función de cumplimiento de normativas heredada en una versión anterior de StorageGRID, consulte la siguiente tabla para saber cómo se compara con la función de bloqueo de objetos S3 de StorageGRID.

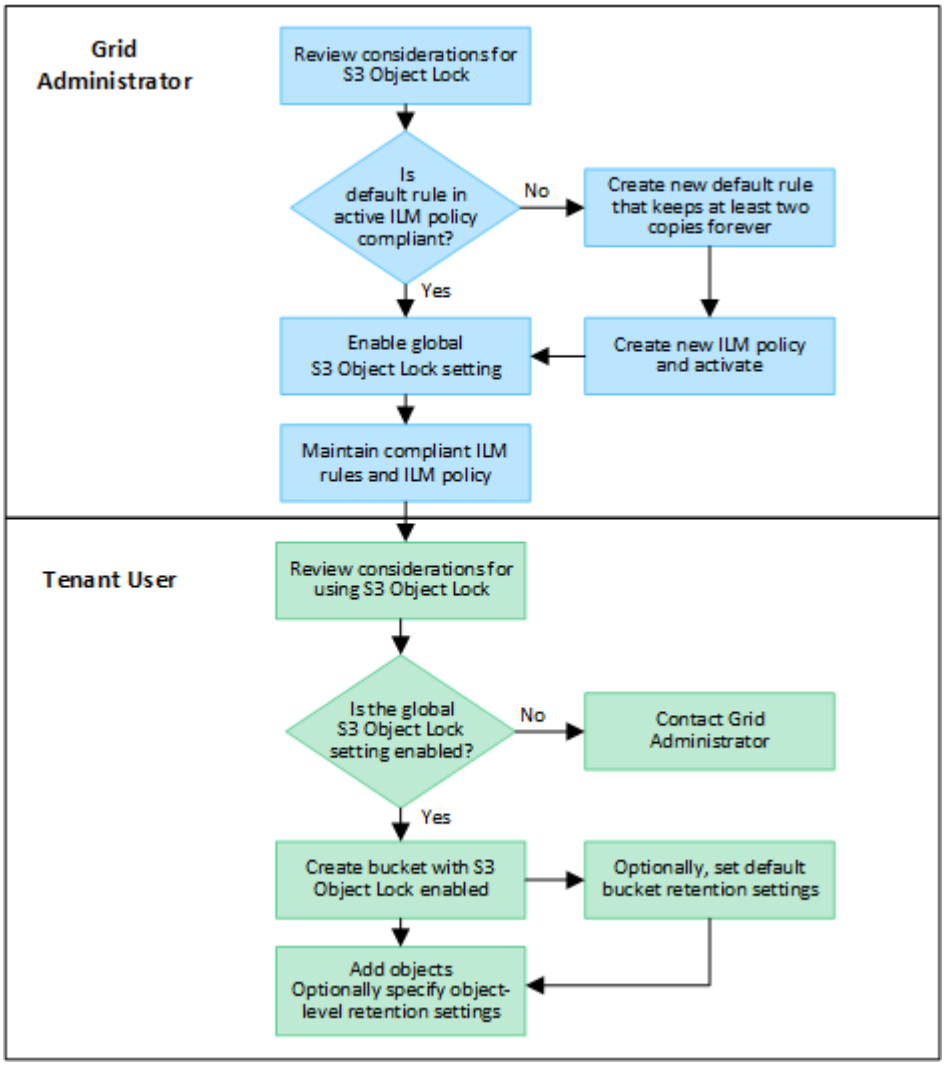
	Bloqueo de objetos de S3	Cumplimiento (heredado)
¿Cómo se habilita la función a nivel global?	En Grid Manager, seleccione **CONFIGURACIÓN** > **sistema** > **S3 Object Lock**.	Ya no es compatible.
¿Cómo se habilita la función para un bloque?	Los usuarios deben habilitar el bloqueo de objetos S3 al crear un nuevo bloque con el administrador de inquilinos, la API de gestión de inquilinos o la API DE REST de S3.	Ya no es compatible.

	Bloqueo de objetos de S3	Cumplimiento (heredado)
¿Se admite el control de versiones de bloques?	Sí. El versionado de bloques se requiere y se habilita automáticamente si se habilita S3 Object Lock para el bloque.	No
¿Cómo se establece la retención de objetos?	Los usuarios pueden establecer una fecha de retención hasta la fecha para cada versión de objeto, o pueden establecer un período de retención predeterminado para cada bloque.	Los usuarios deben establecer un período de retención para todo el segmento. El período de retención se aplica a todos los objetos del bloque.
¿Se puede cambiar el período de retención?	• En el modo de cumplimiento de normativas, se puede aumentar la fecha de retención de una versión de objeto, pero nunca disminuir. • En el modo de gobierno, los usuarios con permisos especiales pueden disminuir o incluso eliminar la configuración de retención de un objeto.	El período de retención de un depósito se puede aumentar, pero nunca disminuir.
¿Dónde se controla la conservación legal?	Los usuarios pueden poner una retención legal o levantar una retención legal para cualquier versión de objeto en el cubo.	Se coloca una retención legal en el cubo y afecta a todos los objetos del cucharón.
¿Cuándo se pueden eliminar los objetos?	• En el modo de cumplimiento, se puede suprimir una versión de objeto después de alcanzar la fecha de retención hasta la fecha, asumiendo que el objeto no está bajo conservación legal. • En el modo de gobierno, los usuarios con permisos especiales pueden eliminar un objeto antes de alcanzar su fecha de retención, asumiendo que el objeto no está bajo retención legal.	Un objeto se puede eliminar después de que caduque el período de retención, suponiendo que el segmento no esté en retención legal. Los objetos se pueden eliminar de forma automática o manual.
¿Se admite la configuración del ciclo de vida de bloques?	Sí	No

Flujo de trabajo para bloqueo de objetos de S3

Como administrador de grid, debe coordinar estrechamente con los usuarios inquilinos a fin de asegurarse de que los objetos estén protegidos de forma que cumplan sus requisitos de retención.

En el diagrama de flujo de trabajo, se muestran los pasos de alto nivel para usar el bloqueo de objetos de S3. Estos pasos los realiza el administrador de grid y los usuarios inquilinos.



Tareas del administrador de grid

Tal y como se muestra en el diagrama de flujo de trabajo, un administrador de grid debe ejecutar dos tareas de alto nivel para que los usuarios de inquilinos S3 puedan usar el bloqueo de objetos S3:

1. Cree al menos una regla de ILM compatible y haga que rija la regla predeterminada en una política de ILM activa.
2. Habilite el valor global de Object Lock para todo el sistema StorageGRID.

Tareas del usuario inquilino

Una vez habilitada la configuración global de bloqueo de objetos S3, los inquilinos pueden realizar estas tareas:

1. Cree bloques con el bloqueo de objetos de S3 habilitado.
2. Opcionalmente, especifique la configuración de retención predeterminada para el bloque. Cualquier configuración de bloque predeterminada se aplica solo a objetos nuevos que no tienen su propia configuración de retención.
3. Agregue objetos a esos bloques y, opcionalmente, especifique los períodos de retención a nivel de objeto y la configuración de retención legal.
4. Según sea necesario, actualice la retención predeterminada del depósito o actualice el período de retención o la configuración de retención legal para un objeto individual.

Requisitos para el bloqueo de objetos de S3

Debe revisar los requisitos para habilitar la configuración global de bloqueo de objetos de S3, los requisitos para crear reglas de ILM y políticas de ILM conformes con la normativa, y las restricciones que StorageGRID coloca en bloques y objetos que usan el bloqueo de objetos S3.

Requisitos para usar el valor global de bloqueo de objetos S3

- Debe habilitar la configuración global de Object Lock mediante el administrador de grid o la API de gestión de grid antes de que cualquier inquilino de S3 pueda crear un bucket con el bloqueo de objetos S3 habilitado.
- Al habilitar el ajuste global de Object Lock, todas las cuentas de inquilinos S3 pueden crear bloques con el bloqueo de objetos S3 habilitado.
- Después de habilitar la configuración global S3 Object Lock, no puede desactivar la configuración.
- No puede activar el bloqueo de objetos S3 global a menos que la regla predeterminada en todas las políticas de ILM activas sea *compliant* (es decir, la regla predeterminada debe cumplir con los requisitos de los bloques con bloqueo de objetos S3 habilitado).
- Cuando se habilita la configuración global S3 Object Lock, no se puede crear una nueva política de ILM ni activar una política de ILM existente a menos que la regla predeterminada de la política sea compatible. Una vez habilitada la configuración global S3 Object Lock, las reglas de ILM y las páginas de políticas de ILM indican qué reglas de ILM cumplen.

Requisitos para las reglas de ILM que cumplen con las normativas

Si desea habilitar la configuración global Bloqueo de objetos S3, debe asegurarse de que la regla predeterminada de todas las políticas de ILM activas sea compatible. Una regla conforme a las normativas satisface los requisitos de ambos bloques con el bloqueo de objetos S3 habilitado y de cualquier bloque existente con el cumplimiento de normativas heredado habilitado:

- Debe crear al menos dos copias de objetos replicados o una copia con código de borrado.
- Estas copias deben existir en los nodos de almacenamiento durante todo el tiempo que dure cada línea en las instrucciones de colocación.
- Las copias de objetos no se pueden guardar en un pool de almacenamiento en la nube.
- Las copias de objetos no se pueden guardar en los nodos de archivado.
- Al menos una línea de las instrucciones de colocación debe comenzar en el día 0, usando **tiempo de ingesta** como tiempo de referencia.
- Al menos una línea de las instrucciones de colocación debe ser “Para siempre”.

Requisitos para las políticas de ILM

Cuando se habilita la configuración global Bloqueo de objetos S3, las políticas de ILM activas e inactivas pueden incluir reglas que cumplen y no cumplen.

- La regla predeterminada de una política de ILM activa o inactiva debe cumplir.
- Las reglas no compatibles solo se aplican a objetos de los depósitos que no tienen activado el bloqueo de objetos S3 o que no tienen activada la función de cumplimiento de normativas heredada.
- Las reglas que cumplen las normativas se pueden aplicar a los objetos de cualquier bloque; no es necesario habilitar el bloqueo de objetos S3 o la conformidad heredada para el bloque.

Una política de ILM compatible puede incluir estas tres reglas:

1. Se trata de una regla que crea copias de los objetos con código de borrado en un bloque específico con el bloqueo de objetos S3 habilitado. Las copias EC se almacenan en nodos de almacenamiento del día 0 al permanente.
2. Una regla no compatible que crea dos copias de objetos replicadas en los nodos de almacenamiento durante un año y, a continuación, mueve una copia de objetos a los nodos de archivado y almacena esa copia para siempre. Esta regla solo se aplica a los depósitos que no tienen activado el bloqueo de objetos S3 o el cumplimiento de normativas heredado porque almacena una sola copia de objeto para siempre y utiliza nodos de archivado.
3. Una regla predeterminada que cumple con las normativas crea dos copias de objetos replicados en los nodos de almacenamiento del día 0 al permanente. Esta regla se aplica a cualquier objeto de cualquier segmento que no haya sido filtrado por las dos primeras reglas.

Requisitos para bloques con bloqueo de objetos de S3 habilitado

- Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, puede usar el administrador de inquilinos, la API de gestión de inquilinos o la API REST de S3 para crear bloques con el bloqueo de objetos S3 habilitado.
- Si planea utilizar el bloqueo de objetos S3, debe habilitar el bloqueo de objetos S3 al crear el bloque. No puede activar el bloqueo de objetos S3 para un depósito existente.
- Cuando se habilita el bloqueo de objetos S3 para un bloque, StorageGRID habilita automáticamente el control de versiones para ese bloque. No puede desactivar el bloqueo de objetos de S3 ni suspender el control de versiones del depósito.
- De manera opcional, puede especificar un modo de retención y un período de retención predeterminados para cada bloque mediante el administrador de inquilinos, la API de gestión de inquilinos o la API DE REST S3. La configuración de retención predeterminada del depósito se aplica solo a los nuevos objetos agregados al depósito que no tienen su propia configuración de retención. Puede anular esta configuración predeterminada especificando un modo de retención y Retain-until-date para cada versión del objeto cuando se cargue.
- Se admite la configuración de ciclo de vida de bloques para los bloques con S3 Object Lock habilitado.
- La replicación de CloudMirror no es compatible para bloques con el bloqueo de objetos S3 habilitado.

Requisitos para objetos en bloques con S3 Object Lock habilitado

- Para proteger una versión de objeto, puede especificar la configuración de retención predeterminada para el bloque, o bien puede especificar la configuración de retención para cada versión de objeto. La configuración de retención a nivel de objeto se puede especificar mediante la aplicación cliente S3 o la API DE REST S3.

- La configuración de retención se aplica a versiones individuales de objetos. Una versión de objeto puede tener una configuración de retención hasta fecha y una retención legal, una pero no la otra, o ninguna. Al especificar una configuración de retención hasta fecha o de retención legal para un objeto, sólo se protege la versión especificada en la solicitud. Puede crear nuevas versiones del objeto, mientras que la versión anterior del objeto permanece bloqueada.

Ciclo de vida de los objetos en bloques con S3 Object Lock habilitado

Cada objeto que se guarda en un depósito con S3 Object Lock habilitado pasa por las siguientes etapas:

1. **Procesamiento de objetos**

   Cuando se agrega una versión de objeto al depósito que tiene S3 Object Lock habilitado, la configuración de retención se aplica de la siguiente manera:

   - Si se especifica la configuración de retención para el objeto, se aplica la configuración de nivel de objeto. Se ignoran todos los valores predeterminados de los depósitos.
   - Si no se especifica ninguna configuración de retención para el objeto, se aplica la configuración de bloque predeterminada, si existe.
   - Si no se especifica ninguna configuración de retención para el objeto o el depósito, el objeto no está protegido por S3 Object Lock.

   Si se aplica una configuración de retención, tanto el objeto como cualquier metadatos definidos por el usuario S3 se protegen.

2. **Retención y eliminación de objetos**

   StorageGRID almacena varias copias de cada objeto protegido durante el período de retención especificado. El número y el tipo exactos de copias de objetos y las ubicaciones de almacenamiento están determinados por las reglas conformes a la normativa de las políticas de ILM activas. Si se puede eliminar un objeto protegido antes de alcanzar su fecha de retención hasta la fecha, depende de su modo de retención.

   - Si un objeto se encuentra bajo una conservación legal, nadie puede eliminarlo, independientemente de su modo de retención.

Información relacionada

- "Cree un bloque de S3"
- "Actualizar S3 Retención predeterminada de bloqueo de objetos"
- "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
- "Ejemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3"

Habilite el bloqueo de objetos de S3 globalmente

Si una cuenta de inquilino de S3 tiene que cumplir con los requisitos de normativa al guardar datos de objetos, debe habilitar el bloqueo de objetos de S3 para todo el sistema StorageGRID. Al habilitar el ajuste global de bloqueo de objetos de S3, cualquier usuario inquilino de S3 puede crear y gestionar bloques y objetos con S3 Object Lock.

Antes de empezar

- Usted tiene la "Permiso de acceso raíz".

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ha revisado el flujo de trabajo de bloqueo de objetos de S3 y comprende las consideraciones.
- Ha confirmado que la regla predeterminada de la política de ILM activa cumple con las normativas. Consulte "Cree una regla de ILM predeterminada" para obtener más detalles.

Acerca de esta tarea

Un administrador de grid debe habilitar la configuración global de bloqueo de objetos S3 para permitir a los usuarios inquilinos crear nuevos bloques con el bloqueo de objetos S3 habilitado. Una vez habilitada esta configuración, no se puede desactivar.

> La configuración de cumplimiento global está anticuada. Si ha habilitado esta configuración con una versión anterior de StorageGRID, la configuración Bloqueo de objetos S3 se activa automáticamente. Puede seguir usando StorageGRID para gestionar la configuración de los buckets compatibles existentes; sin embargo, no puede crear nuevos buckets compatibles. Para obtener más información, consulte "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5".

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **S3 Object Lock**.

   Se muestra la página S3 Object Lock Settings.

2. Seleccione **Activar el bloqueo de objetos S3**.
3. Seleccione **aplicar**.

   Aparece un cuadro de diálogo de confirmación que le recuerda que no puede desactivar el bloqueo de objetos S3 después de que esté habilitado.

4. Si está seguro de que desea activar de forma permanente el bloqueo de objetos S3 para todo el sistema, seleccione **Aceptar**.

   Al seleccionar **Aceptar**:

   - Si la regla predeterminada de la política de ILM activa es compatible, S3 Object Lock ahora está habilitado para toda la cuadrícula y no se puede deshabilitar.
   - Si la regla predeterminada no es compatible, aparece un error. Debe crear y activar una nueva política de ILM que incluya una regla de cumplimiento como regla predeterminada. Seleccione **OK**. A continuación, cree una nueva política, simule y actívela. Consulte "Cree una política de ILM" si desea obtener instrucciones.

Resuelva los errores de coherencia al actualizar la configuración de bloqueo de objetos de S3 o cumplimiento heredado

Si un sitio de centro de datos o varios nodos de almacenamiento de un sitio no están disponibles, es posible que deba ayudar a los usuarios inquilinos S3 a aplicar los cambios en la configuración del bloqueo de objetos S3 o del cumplimiento heredado.

Los usuarios inquilinos que tienen bloques con S3 Object Lock (o Legacy Compliance) habilitado pueden cambiar ciertas opciones. Por ejemplo, es posible que un usuario arrendatario que utilice el bloqueo de objetos S3 deba poner una versión de objeto en retención legal.

Cuando un usuario tenant actualiza la configuración de un bloque de S3 o una versión de objeto,

StorageGRID intenta actualizar inmediatamente los metadatos del objeto o el bloque en el grid. Si el sistema no puede actualizar los metadatos porque no hay disponibles un sitio de centro de datos o varios nodos de almacenamiento, devuelve un error:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Para resolver este error, siga estos pasos:

1. Se debe intentar que todos los nodos o sitios de almacenamiento estén disponibles de nuevo Lo antes posible..
2. Si no puede dejar suficientes nodos de almacenamiento en cada sitio disponible, póngase en contacto con el soporte técnico, que puede ayudarle a recuperar nodos y asegurarse de que los cambios se apliquen de manera coherente en la cuadrícula.
3. Una vez resuelto el problema subyacente, recuerde al usuario inquilino que vuelva a intentar cambiar sus cambios de configuración.

Información relacionada

- "Usar una cuenta de inquilino"
- "USE LA API DE REST DE S3"
- "Recuperación y mantenimiento"

Ejemplo de reglas y políticas de ILM

Ejemplo 1: Reglas de ILM y políticas para el almacenamiento de objetos

Es posible usar las siguientes reglas y políticas de ejemplo como punto de inicio al definir una política de ILM para cumplir con los requisitos de retención y protección de objetos.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

Regla ILM 1 Por ejemplo 1: Copiar datos de objetos en dos sitios

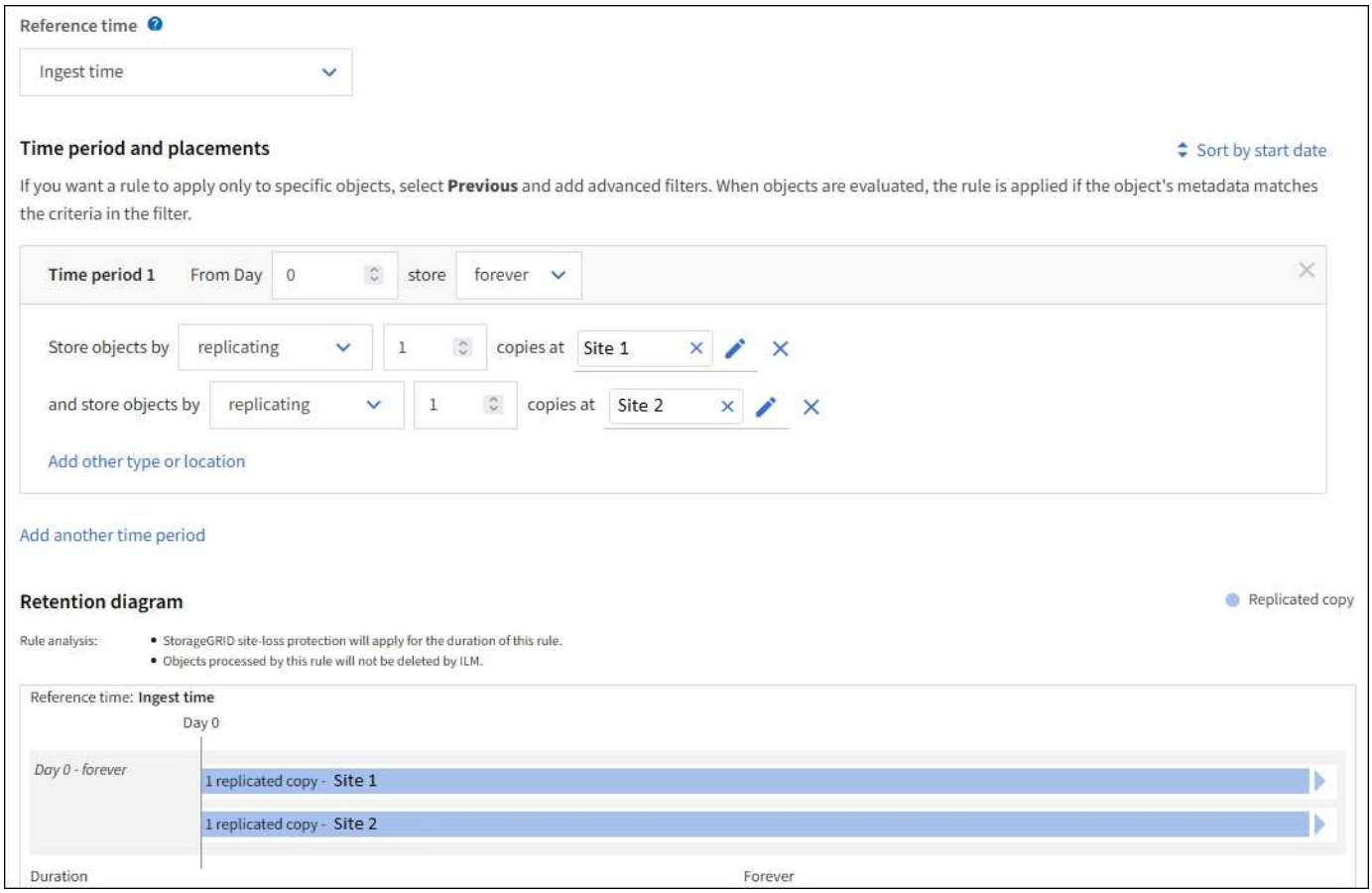
Este ejemplo de regla ILM copia datos de objetos en pools de almacenamiento en dos sitios.

Definición de regla	Valor de ejemplo
Pools de almacenamiento in situ	Dos pools de almacenamiento, cada uno de los cuales contiene sitios diferentes, denominados Sitio 1 y Sitio 2.
Nombre de regla	Dos copias Dos sitios
Tiempo de referencia	Tiempo de ingesta

Definición de regla	Valor de ejemplo
Ubicaciones	En el día 0 hasta siempre, conserve una copia replicada en el sitio 1 y una copia replicada en el sitio 2.

La sección de análisis de reglas del diagrama de retención indica lo siguiente:

- La protección contra pérdida de sitios de StorageGRID se aplicará mientras dure esta regla.
- ILM no eliminará los objetos procesados por esta regla.

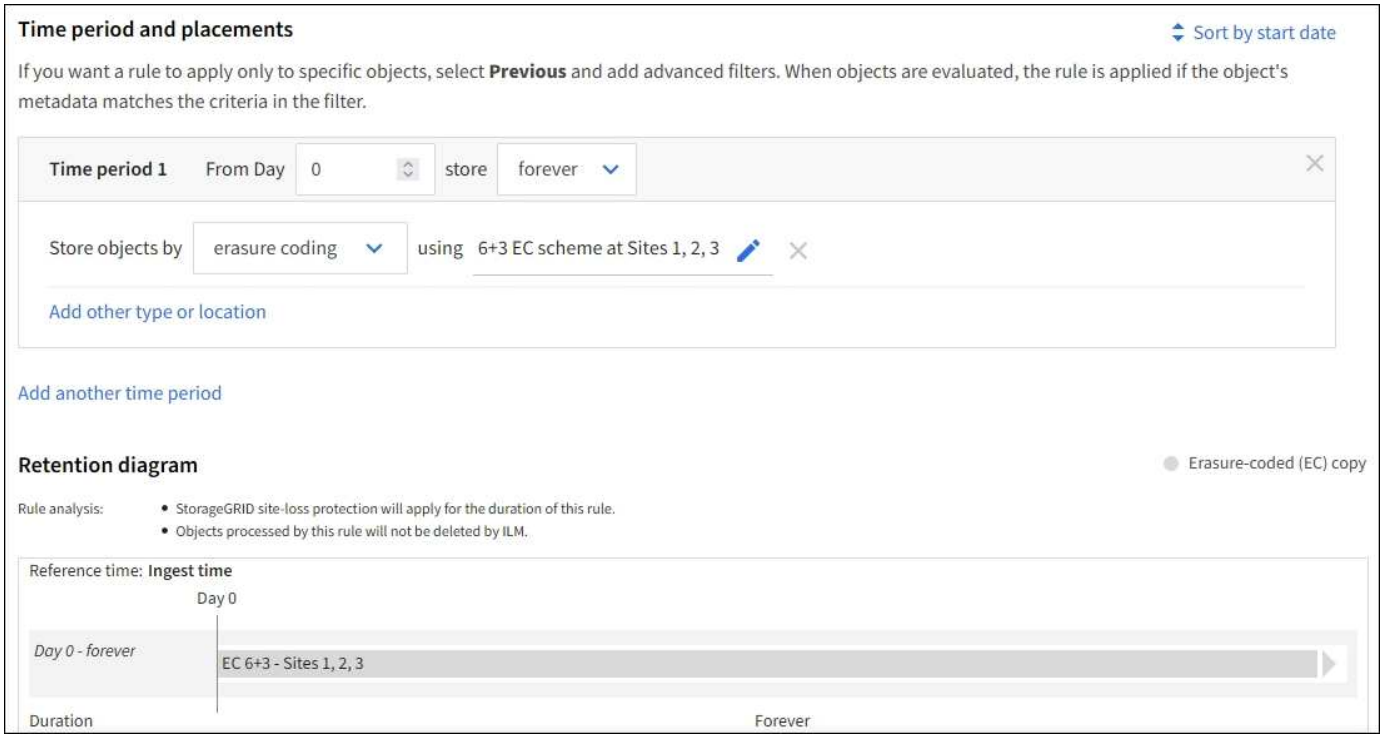


Regla de ILM 2 Por ejemplo 1: Perfil de código de borrado con coincidencia de bloques

En esta regla de ILM de ejemplo se utiliza un perfil de código de borrado y un bloque de S3 para determinar dónde y cuánto tiempo se almacena el objeto.

Definición de regla	Valor de ejemplo
Pool de almacenamiento con múltiples sitios	• Un pool de almacenamiento en tres sitios (sitios 1, 2, 3) • Utilice un esquema de codificación de borrado de 6+3
Nombre de regla	S3 registros financieros del bloque
Tiempo de referencia	Tiempo de ingesta

Definición de regla	Valor de ejemplo
Ubicaciones	Para los objetos del bloque de S3 denominados registros financieros, cree una copia con código de borrado en el pool especificado por el perfil de código de borrado. Guarde esta copia para siempre.



Política de ILM, por ejemplo 1

En la práctica, la mayoría de las políticas de ILM son sencillas, a pesar de que el sistema StorageGRID permite diseñar políticas de ILM sofisticadas y complejas.

Una política de ILM típica para un grid de varios sitios podría incluir reglas de ILM como las siguientes:

- Durante la ingesta, almacene todos los objetos que pertenecen al bloque de S3 denominado `finance-records` en un pool de almacenamiento que contiene tres sitios. Use el código de borrado 6+3.
- Si un objeto no coincide con la primera regla de ILM, utilice la regla de ILM predeterminada de la política, dos copias dos centros de datos, para almacenar una copia de ese objeto en el sitio 1 y una copia en el sitio 2.

Información relacionada

- "Políticas de ILM: Información general"
- "Crear políticas de ILM"

Ejemplo 2: Reglas de ILM y política para el filtrado de tamaño de objetos de EC

Puede usar las siguientes reglas y políticas de ejemplo como puntos de inicio para definir una política de ILM que filtra por tamaño de objeto para cumplir los requisitos de EC recomendados.

Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

Regla de ILM 1 por ejemplo 2: Utilice EC para objetos de más de 1 MB

Este ejemplo codifica los objetos de borrado de regla ILM que tienen más de 1 MB.

El código de borrado se adapta mejor a los objetos de más de 1 MB. No use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

Definición de regla	Valor de ejemplo
Nombre de regla	Objetos sólo EC > 1 MB
Tiempo de referencia	Tiempo de ingesta
Filtro avanzado para Tamaño de objeto	Tamaño de objeto superior a 1 MB
Ubicaciones	Cree una copia codificada con borrado al 2+1 mediante tres ubicaciones

Regla de ILM 2 por ejemplo 2: Dos copias replicadas

Esta regla de ILM de ejemplo crea dos copias replicadas y no filtra por el tamaño del objeto. Esta regla es la regla predeterminada para la directiva. Dado que la primera regla filtra todos los objetos mayores de 1 MB, esta regla sólo se aplica a objetos de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de regla	Dos copias replicadas
Tiempo de referencia	Tiempo de ingesta
Filtro avanzado para Tamaño de objeto	Ninguno
Ubicaciones	En el día 0 hasta siempre, conserve una copia replicada en el sitio 1 y una copia replicada en el sitio 2.

Política de ILM, por ejemplo 2: Usar EC para objetos de más de 1 MB

Este ejemplo de política de ILM incluye dos reglas ILM:

- La primera regla de borrado codifica todos los objetos que sean mayores de 1 MB.
- La segunda regla de ILM (predeterminada) crea dos copias replicadas. Dado que los objetos mayores de 1 MB se han filtrado mediante la regla 1, la regla 2 sólo se aplica a objetos de 1 MB o menos.

Ejemplo 3: Reglas de ILM y política para mejorar la protección de los archivos de imagen

Puede utilizar las siguientes reglas y políticas de ejemplo para asegurarse de que las imágenes de más de 1 MB tengan un código de borrado y que dos copias estén hechas de imágenes más pequeñas.

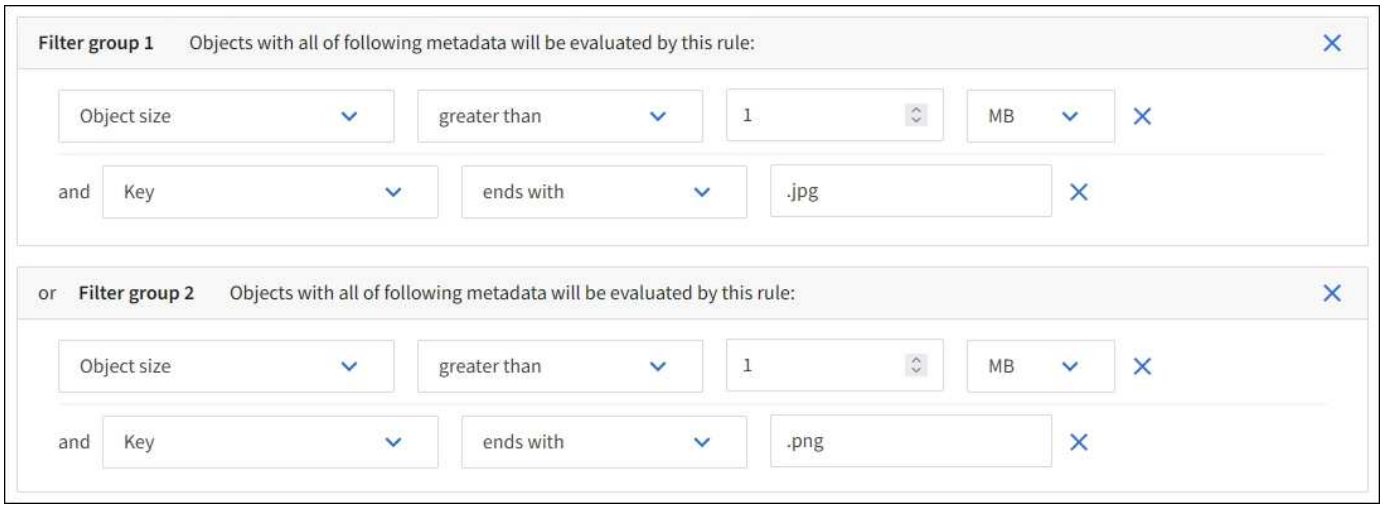
> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

Regla ILM 1 por ejemplo 3: Utilice EC para archivos de imagen superiores a 1 MB

En esta regla de ILM de ejemplo se utiliza un filtrado avanzado para borrar el código de todos los archivos de imagen superiores a 1 MB.

> El código de borrado se adapta mejor a los objetos de más de 1 MB. No use el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos de código de borrado muy pequeños.

Definición de regla	Valor de ejemplo
Nombre de regla	Archivos de imagen EC > 1 MB
Tiempo de referencia	Tiempo de ingesta
Filtro avanzado para Tamaño de objeto	Tamaño de objeto superior a 1 MB
Filtros avanzados para Clave	• Termina en .jpg • Termina en .png
Ubicaciones	Cree una copia codificada con borrado al 2+1 mediante tres ubicaciones



Debido a que esta regla se configura como la primera regla de la directiva, la instrucción de colocación de codificación de borrado solo se aplica a los archivos .jpg y .png que sean mayores de 1 MB.

Regla ILM 2 por ejemplo 3: Cree 2 copias replicadas para todos los archivos de imagen restantes

En este ejemplo, la regla ILM utiliza un filtrado avanzado para especificar que se repliquen los archivos de imagen más pequeños. Dado que la primera regla de la directiva ya coincide con los archivos de imagen superiores a 1 MB, esta regla se aplica a los archivos de imagen de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de regla	2 copias para archivos de imagen
Tiempo de referencia	Tiempo de ingesta
Filtros avanzados para Clave	• Termina en .jpg • Termina en .png
Ubicaciones	Cree 2 copias replicadas en dos pools de almacenamiento

Política de ILM, por ejemplo 3: Mejor protección para los archivos de imagen

Este ejemplo de política de ILM incluye tres reglas:

- La primera regla de borrado codifica todos los archivos de imagen mayores de 1 MB.
- La segunda regla crea dos copias de cualquier archivo de imagen restante (es decir, imágenes de 1 MB o menos).
- La regla predeterminada se aplica a todos los objetos restantes (es decir, cualquier archivo que no sea de imagen).

Ejemplo 4: Reglas de ILM y políticas para objetos con versiones de S3

Si tiene un bucket de S3 con el control de versiones habilitado, puede gestionar las versiones de objetos no corrientes incluyendo reglas en su política de ILM que utilicen la

hora no corriente como tiempo de referencia.

> Si especifica un tiempo de retención limitado para los objetos, esos objetos se suprimirán permanentemente después de alcanzar el período de tiempo. Asegúrese de comprender cuánto tiempo se retendrán los objetos.

Como se muestra en este ejemplo, puede controlar la cantidad de almacenamiento que utilizan los objetos con versiones utilizando instrucciones de colocación diferentes para las versiones de objetos no actuales.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

> Para realizar la simulación de política de ILM en una versión no actual de un objeto, debe conocer el UUID o CBID de la versión del objeto. Para encontrar el UUID y CBID, utilice "búsqueda de metadatos de objetos" mientras el objeto sigue siendo actual.

Información relacionada

- "Cómo se eliminan los objetos"

Regla 1 de ILM, por ejemplo 4: Guarde tres copias durante 10 años

Esta regla de ILM de ejemplo almacena una copia de cada objeto en tres sitios durante 10 años.

Esta regla se aplica a todos los objetos, con o sin versiones.

Definición de regla	Valor de ejemplo
Pools de almacenamiento	Tres pools de almacenamiento, cada uno compuesto por diferentes centros de datos, denominados Sitio 1, Sitio 2 y Sitio 3.
Nombre de regla	Tres copias diez años
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	El día 0, conserve tres copias replicadas durante 10 años (3.652 días), una en el sitio 1, una en el sitio 2 y otra en el sitio 3. Al final de 10 años, elimine todas las copias del objeto.

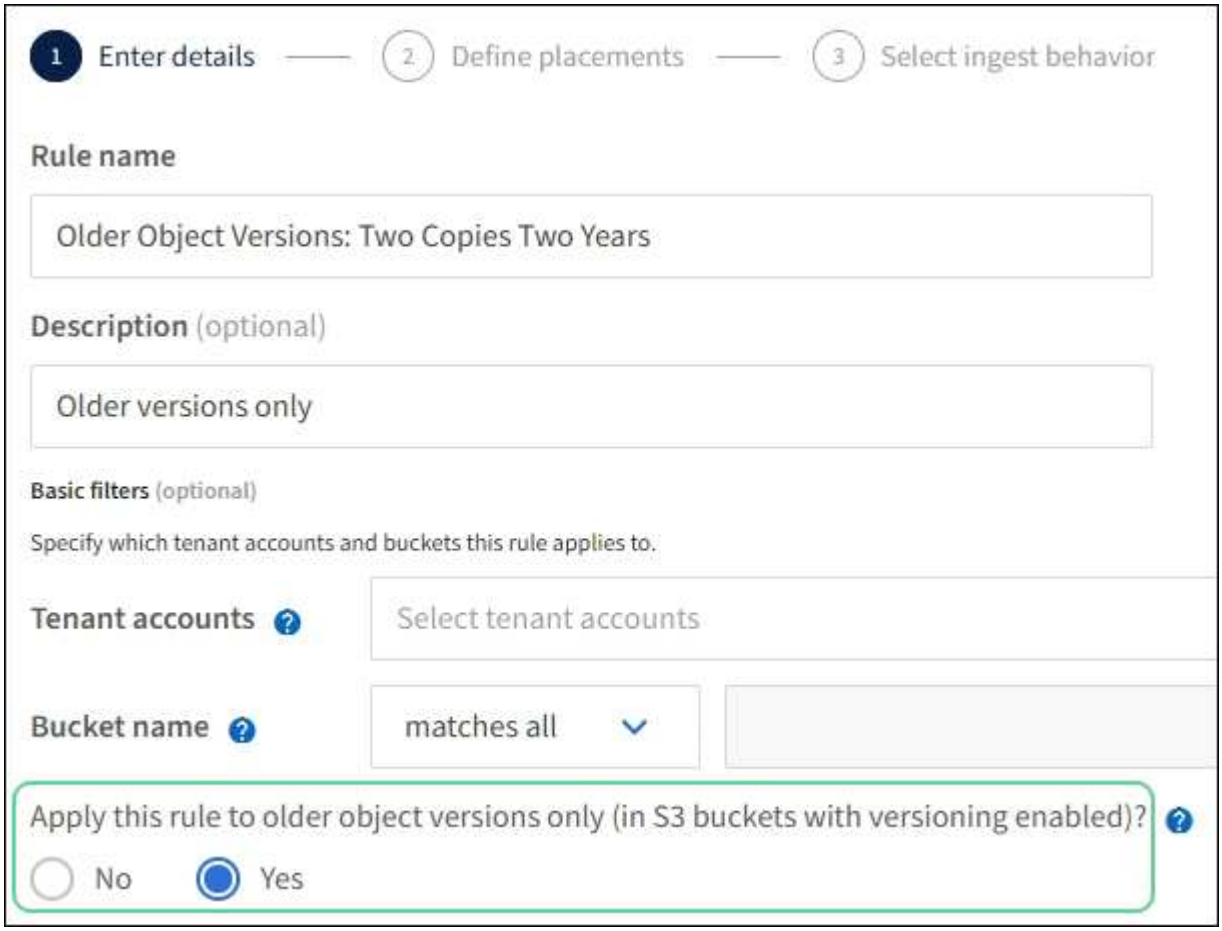
Regla de ILM 2 por ejemplo 4: Guarde dos copias de las versiones no corrientes durante 2 años

Esta regla de ILM de ejemplo almacena dos copias de las versiones no actuales de un objeto con versiones de S3 durante 2 años.

Dado que la regla 1 de ILM se aplica a todas las versiones del objeto, debe crear otra regla para filtrar las versiones no actuales.

Para crear una regla que utilice el tiempo no corriente como tiempo de referencia, seleccione **Sí** para la pregunta, ¿Aplicar esta regla solo a versiones de objetos anteriores (en bloques S3 con control de versiones activado)? En el paso 1 (introduzca detalles) del asistente Create an ILM Rule. Cuando selecciona **Sí**, *Tiempo no corriente* se selecciona automáticamente para el tiempo de referencia y no puede seleccionar un tiempo de

referencia diferente.



En este ejemplo, sólo se almacenan dos copias de las versiones no corrientes, y esas copias se almacenarán durante dos años.

Definición de regla	Valor de ejemplo
Pools de almacenamiento	Dos pools de almacenamiento, cada uno en diferentes centros de datos, Sitio 1 y Sitio 2.
Nombre de regla	Versiones no corrientes: Dos copias dos años
Tiempo de referencia	Hora no corriente Seleccionado automáticamente cuando selecciona **Sí** para la pregunta, ¿Aplicar esta regla solo a versiones de objetos anteriores (en cubos S3 con control de versiones activado)? En el asistente Create an ILM Rule.
Ubicaciones	El día 0 relativo a la hora no corriente (es decir, a partir del día en que la versión del objeto se convierte en la versión no actual), mantenga dos copias replicadas de las versiones del objeto no corriente durante 2 años (730 días), una en el sitio 1 y otra en el sitio 2. Al final de 2 años, elimine las versiones no actuales.

Política de ILM, por ejemplo 4: Objetos con versiones de S3

Si desea administrar versiones anteriores de un objeto de forma distinta a la versión actual, las reglas que utilizan una hora no corriente como tiempo de referencia deben aparecer en la política de ILM antes de las reglas que se aplican a la versión del objeto actual.

Una política de ILM para objetos con versiones de S3 puede incluir reglas de ILM como las siguientes:

- Mantenga las versiones antiguas (no actuales) de cada objeto durante 2 años, a partir del día en que la versión se volvió no actual.

> Las reglas de hora no corriente deben aparecer en la política antes de las reglas que se aplican a la versión del objeto actual. De lo contrario, las versiones del objeto no corriente nunca coincidirán con la regla de hora no corriente.

- Al ingerir, cree tres copias replicadas y almacene una copia en cada uno de tres sitios. Guarde copias de la versión actual del objeto durante 10 años.

Al simular la directiva de ejemplo, se esperaría que los objetos de prueba se evaluaran de la siguiente manera:

- Cualquier versión de objeto no actual se haría coincidir con la primera regla. Si una versión de objeto no actual tiene más de 2 años, ILM lo elimina de forma permanente (todas las copias de la versión no actual se eliminan de la cuadrícula).
- La versión actual del objeto coincidiría con la segunda regla. Cuando la versión actual del objeto se ha almacenado durante 10 años, el proceso de ILM añade un marcador de eliminación como la versión actual del objeto y hace que la versión del objeto anterior sea «no actual». La próxima vez que se produzca una evaluación de ILM, esta versión no actual coincide con la primera regla. Como resultado, la copia en el sitio 3 se purga y las dos copias en el sitio 1 y el sitio 2 se almacenan durante 2 años más.

Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto

Puede usar un filtro de ubicación y el comportamiento de ingesta estricto de una regla para evitar que los objetos se guarden en una ubicación de centro de datos en particular.

En este ejemplo, un inquilino con sede en París no quiere almacenar algunos objetos fuera de la UE debido a preocupaciones regulatorias. Otros objetos, incluidos todos los objetos de otras cuentas de inquilino, pueden almacenarse en el centro de datos de París o en el centro de datos de EE. UU.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

Información relacionada

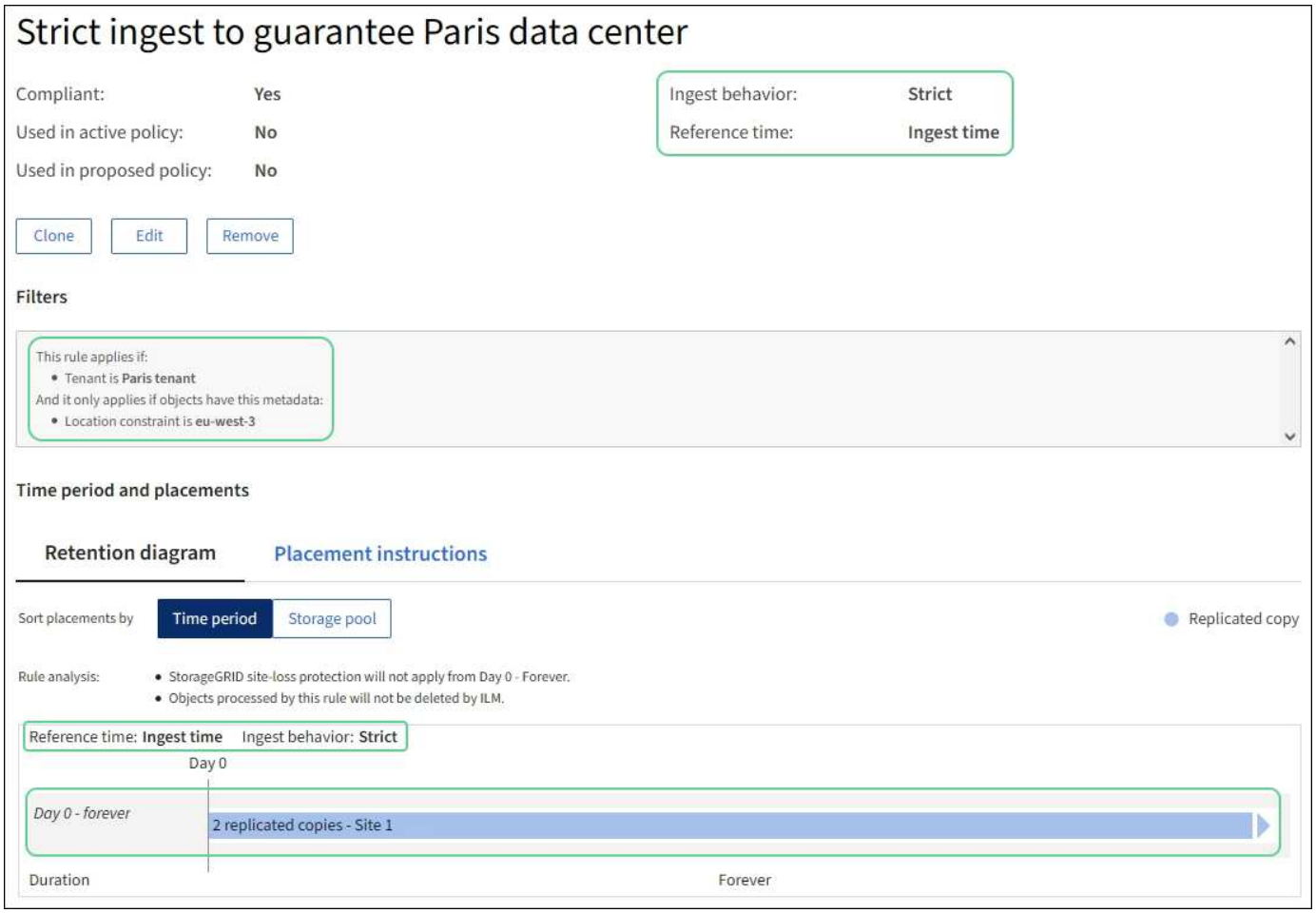
- "Opciones de procesamiento"
- "Create ILM rule: Seleccione el comportamiento de ingesta"

Regla 1 de ILM, por ejemplo 5: Ingesta estricta para garantizar el centro de datos de París

Esta regla de ILM de ejemplo usa el comportamiento de ingesta estricto para garantizar que los objetos que ha ahorrado un inquilino basado en París en cubos S3 con la región establecida en la región eu-West-3 (París) nunca se almacenen en el centro de datos de EE. UU.

Esta regla se aplica a objetos que pertenecen al arrendatario de París y que tienen la región de cubo S3 establecida en eu-West-3 (París).

Definición de regla	Valor de ejemplo
Cuenta de inquilino	Inquilino de París
Filtro avanzado	La restricción de ubicación es igual a eu-west-3
Pools de almacenamiento	Sitio 1 (París)
Nombre de regla	Ingesta estricta para garantizar el centro de datos París
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	El día 0, mantenga dos copias replicadas para siempre en el sitio 1 (París)
Comportamiento de ingesta	Estricto. Utilice siempre las colocaciones de esta regla durante el procesamiento. La ingesta falla si no es posible almacenar dos copias del objeto en el centro de datos de París.



Regla 2 de ILM, por ejemplo 5: Ingesta equilibrada de otros objetos

Esta regla de ILM de ejemplo utiliza el comportamiento de ingesta equilibrada para proporcionar una eficiencia de ILM óptima para cualquier objeto que no sea coincidente con la primera regla. Se almacenarán dos copias de todos los objetos compatibles con esta regla: Una en el centro de datos estadounidense y una en el centro de datos de París. Si la regla no se puede cumplir inmediatamente, las copias provisionales se almacenan en cualquier ubicación disponible.

Esta regla se aplica a objetos que pertenecen a cualquier arrendatario y a cualquier región.

Definición de regla	Valor de ejemplo
Cuenta de inquilino	Ignorar
Filtro avanzado	*No especificado*
Pools de almacenamiento	Sitio 1 (París) y Sitio 2 (EE.UU.)
Nombre de regla	2 copias 2 centros de datos
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	Desde el día 0, mantenga dos copias replicadas para siempre en dos centros de datos
Comportamiento de ingesta	Equilibrado. Los objetos que coinciden con esta regla se colocan de acuerdo con las instrucciones de colocación de la regla, si es posible. De lo contrario, las copias provisionales se realizan en cualquier lugar disponible.

Política de ILM, por ejemplo 5: Combinar comportamientos de consumo

La política de ILM de ejemplo incluye dos reglas que tienen comportamientos de consumo diferentes.

Una política de ILM que usa dos comportamientos de consumo diferentes puede incluir reglas de ILM como las siguientes:

- Almacene objetos que pertenecen al inquilino de París y que tienen la región de cubo de S3 establecida en eu-West-3 (París) solo en el centro de datos de París. No se procese correctamente si el centro de datos de París no está disponible.
- Almacenar todos los demás objetos (incluidos los que pertenecen al inquilino de París, pero que tienen una región de bloques diferente) tanto en el centro de datos de EE. UU. Como en el de París. Realice copias provisionales en cualquier ubicación disponible si la instrucción de colocación no se puede satisfacer.

Al simular la directiva de ejemplo, espera que los objetos de prueba se evalúen de la siguiente forma:

- Cualquier objeto que pertenezca al inquilino de París y que tenga la región de bloque de S3 establecida en eu-West-3 se ajusta a la primera regla y se almacena en el centro de datos de París. Como la primera regla usa un procesamiento estricto, estos objetos nunca se almacenan en el centro de datos de EE. UU. Si los nodos de almacenamiento del centro de datos de París no están disponibles, la ingesta falla.

- Todos los demás objetos coinciden con la segunda regla, incluidos los objetos que pertenecen al arrendatario de París y que no tienen la región del cubo S3 establecida en eu-west-3. Se guarda una copia de cada objeto en cada centro de datos. Sin embargo, como la segunda regla utiliza procesamiento equilibrado, si un centro de datos no está disponible, se guardan dos copias provisionales en cualquier ubicación disponible.

Ejemplo 6: Cambiar una política de ILM

Si es necesario cambiar su protección de datos o añadir nuevos sitios, puede crear y activar una nueva política de ILM.

Antes de cambiar una política, debe comprender cómo los cambios en las ubicaciones de ILM pueden afectar temporalmente al rendimiento general de un sistema StorageGRID.

En este ejemplo, se ha agregado un nuevo sitio StorageGRID en una ampliación y se debe implementar una nueva política de gestión del ciclo de vida de la información activa para almacenar los datos en el nuevo sitio. Para implementar una nueva política activa, primero "crear una política". Después, debes hacerlo "simular" y después "activar" la nueva política.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

Cómo el cambio de una política de ILM afecta al rendimiento

Al activar una nueva política de ILM, el rendimiento de su sistema StorageGRID puede verse afectado temporalmente, especialmente si las instrucciones de ubicación de la nueva política requieren que muchos objetos existentes se muevan a nuevas ubicaciones.

Cuando se activa una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, incluidos los existentes y los objetos recién procesados. Antes de activar una nueva política de ILM, revise los cambios que se produzcan en la ubicación de los objetos replicados y los códigos de borrado existentes. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

Para garantizar que una nueva política de ILM no afecte a la ubicación de los objetos existentes replicados y codificados de borrado, puede hacerlo "Cree una regla de ILM con un filtro de tiempo de ingesta". Por ejemplo, **tiempo de ingesta *es el o posterior <date and time>***, de modo que la nueva regla se aplica solo a los objetos ingeridos en o después de la fecha y hora especificadas.

Entre los tipos de cambios en la política de ILM que pueden afectar temporalmente el rendimiento de la StorageGRID se encuentran los siguientes:

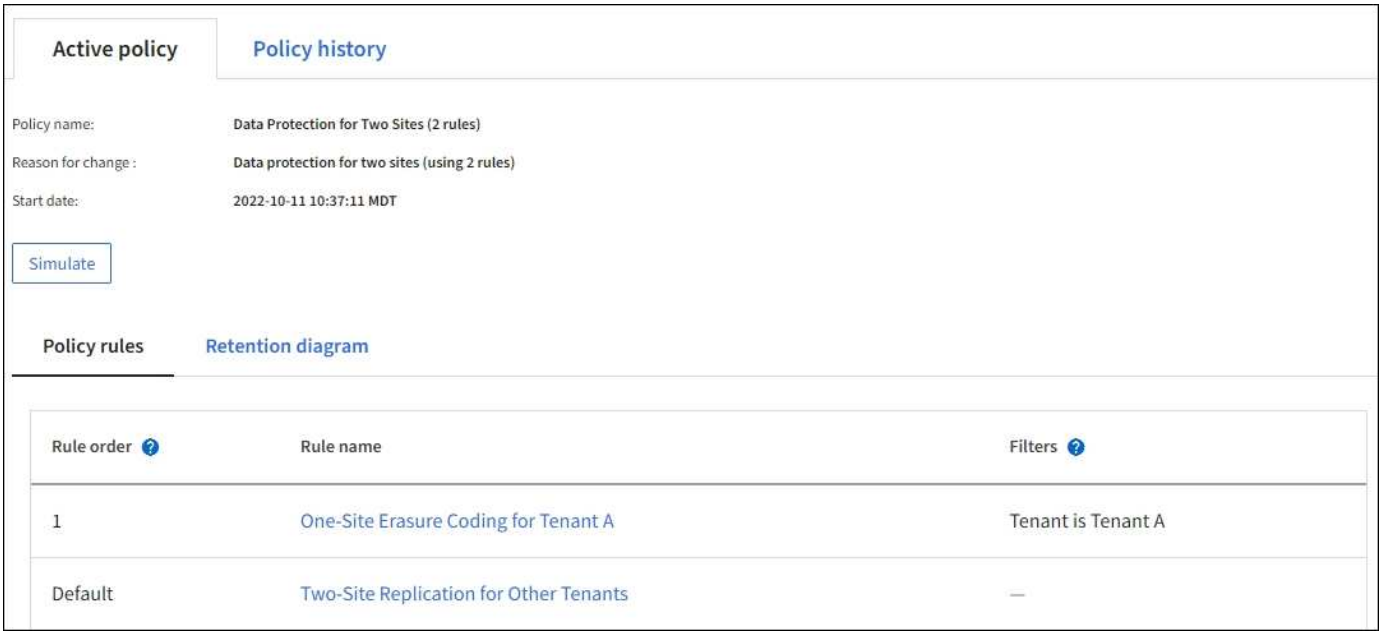
- Aplicar un perfil de código de borrado diferente a los objetos existentes con código de borrado.

  > StorageGRID considera que cada perfil de código de borrado es único y no reutiliza los fragmentos de código de borrado cuando se utiliza un nuevo perfil.

- Cambiar el tipo de copias necesarias para los objetos existentes; por ejemplo, convertir un gran porcentaje de objetos replicados en objetos de código de borrado.
- Mover copias de objetos existentes a una ubicación completamente diferente; por ejemplo, mover un gran número de objetos hacia o desde un pool de almacenamiento en cloud, o desde un sitio remoto.

Política de ILM activa, por ejemplo 6: Protección de datos en dos sitios

En este ejemplo, la activa política de ILM se diseñó inicialmente para un sistema StorageGRID de dos sitios y utiliza dos reglas de ILM.



En esta política de ILM, los objetos del inquilino A están protegidos con codificación de borrado 2+1 en un único sitio, mientras que los objetos que pertenecen al resto de usuarios se protegen en dos sitios mediante replicación de copia.

Regla 1: Codificación de borrado de un sitio para el inquilino A

Definición de regla	Valor de ejemplo
Nombre de regla	Codificación de borrado de un sitio para el inquilino A
Cuenta de inquilino	Inquilinoa
Pool de almacenamiento	Sitio 1
Ubicaciones	Código de borrado 2+1 en el Sitio 1 desde el día 0 hasta siempre

Regla 2: Replicación de dos sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de regla	Replicación de dos sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Pools de almacenamiento	Sitio 1 y sitio 2

Definición de regla	Valor de ejemplo
Ubicaciones	Dos copias replicadas desde el día 0 hasta siempre: Una copia en el sitio 1 y una copia en el sitio 2.

Política de ILM por ejemplo 6: Protección de datos en tres sitios

En este ejemplo, la política de ILM se está reemplazando por una nueva política para un sistema StorageGRID de tres sitios.

Después de realizar una expansión para agregar el nuevo sitio, el administrador de grid creó dos nuevos pools de almacenamiento: Un pool de almacenamiento para el sitio 3 y un pool de almacenamiento que contiene los tres sitios (no el mismo que el pool de almacenamiento predeterminado de todos los nodos de almacenamiento). A continuación, el administrador creó dos nuevas reglas de ILM y una nueva política de ILM, que ha sido diseñada para proteger los datos de los tres sitios.

Cuando se activa esta nueva política de ILM, los objetos que pertenecen al inquilino A se protegerán mediante codificación de borrado 2+1 en tres sitios, mientras que los objetos que pertenecen a otros clientes (y objetos más pequeños que pertenecen al inquilino A) se protegerán en tres sitios usando replicación de 3 copias.

Regla 1: Codificación de borrado a tres ubicaciones para el inquilino A

Definición de regla	Valor de ejemplo
Nombre de regla	Codificación de borrado de tres sitios para el inquilino A
Cuenta de inquilino	Inquilinoa
Pool de almacenamiento	Todos los sitios 3 (incluye el sitio 1, el sitio 2 y el sitio 3)
Ubicaciones	Código de borrado 2+1 en todos los sitios 3 desde el día 0 hasta siempre

Regla 2: Replicación de tres sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de regla	Replicación de tres sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Pools de almacenamiento	Sitio 1, Sitio 2 y Sitio 3
Ubicaciones	Tres copias replicadas desde el día 0 hasta siempre: Una copia en el sitio 1, una copia en el sitio 2 y una copia en el sitio 3.

Activar la política de ILM por ejemplo 6

Al activar una nueva política de ILM, los objetos existentes se pueden mover a ubicaciones nuevas o se

pueden crear copias de objetos nuevas para los objetos existentes, según las instrucciones de ubicación de cualquier regla nueva o actualizada.

> Los errores de un política de ILM pueden provocar la pérdida de datos irrecuperable. Revise y simule cuidadosamente la directiva antes de activarla para confirmar que funcionará según lo previsto.

> Cuando se activa una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, incluidos los existentes y los objetos recién procesados. Antes de activar una nueva política de ILM, revise los cambios que se produzcan en la ubicación de los objetos replicados y los códigos de borrado existentes. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

Lo que ocurre al cambiar las instrucciones de codificación de borrado

En la política de ILM actualmente activa en este ejemplo, los objetos que pertenecen al inquilino A se protegen con el código de borrado 2+1 en el sitio 1. En la nueva política de ILM, los objetos pertenecientes al inquilino A se protegerán con el código de borrado 2+1 en los sitios 1, 2 y 3.

Cuando se activa la nueva política de ILM, se producen las siguientes operaciones de ILM:

- Los objetos nuevos procesados por el inquilino A se dividen en dos fragmentos de datos y se añade un fragmento de paridad. Entonces, cada uno de los tres fragmentos se almacena en un sitio diferente.
- Los objetos existentes que pertenecen al inquilino A se reevalúan durante el proceso de análisis de ILM en curso. Dado que las instrucciones de colocación de ILM usan un nuevo perfil de código de borrado, se crean y distribuyen fragmentos con código de borrado totalmente nuevos en los tres sitios.

> Los fragmentos 2+1 existentes en el Sitio 1 no se reutilizan. StorageGRID considera que cada perfil de código de borrado es único y no reutiliza los fragmentos de código de borrado cuando se utiliza un nuevo perfil.

Qué ocurre cuando cambian las instrucciones de replicación

En la política de ILM actualmente activa en este ejemplo, los objetos que pertenecen a otros inquilinos se protegen usando dos copias replicadas en los pools de almacenamiento de los sitios 1 y 2. En la nueva política de ILM, los objetos que pertenezcan a otros clientes se protegerán usando tres copias replicadas en pools de almacenamiento de los sitios 1, 2 y 3.

Cuando se activa la nueva política de ILM, se producen las siguientes operaciones de ILM:

- Cuando cualquier inquilino que no sea el inquilino A procesa un objeto nuevo, StorageGRID crea tres copias y guarda una copia en cada sitio.
- Los objetos existentes que pertenecen a estos otros inquilinos se reevalúan durante el proceso de análisis de ILM en curso. Como las copias de objetos existentes en el Sitio 1 y el Sitio 2 siguen satisfaciendo los requisitos de replicación de la nueva regla de ILM, StorageGRID solo tiene que crear una nueva copia del objeto para el sitio 3.

Impacto en el rendimiento de la activación de esta política

Cuando se activa la política de ILM en este ejemplo, el rendimiento general de este sistema StorageGRID se verá afectado temporalmente. Se necesitarán niveles superiores a los normales de recursos de grid para crear

nuevos fragmentos con código de borrado para los objetos existentes del inquilino A y nuevas copias replicadas en el sitio 3 para los objetos existentes de otros inquilinos.

Como resultado del cambio en la política de ILM, es posible que las solicitudes de lectura y escritura del cliente experimenten temporalmente más latencias normales. Las latencias volverán a los niveles normales una vez que se implementen por completo las instrucciones de colocación en el grid.

Para evitar problemas de recursos al activar una nueva política de ILM, puede utilizar el filtro avanzado de tiempo de procesamiento en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de procesamiento en mayor o igual que el tiempo aproximado en el que la nueva política entrará en vigor para garantizar que los objetos existentes no se muevan innecesariamente.

> Si necesita ralentizar o aumentar la velocidad a la que se procesan los objetos después de un cambio de la política de ILM, póngase en contacto con el soporte técnico.

Ejemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3

Puede usar el bloque de S3, las reglas de ILM y la política de ILM en este ejemplo como un punto de partida para definir una política de ILM para cumplir con los requisitos de retención y protección de objetos para los objetos en bloques con el bloqueo de objetos S3 habilitado.

> Si ha utilizado la función de cumplimiento de normativas anterior en versiones de StorageGRID anteriores, también puede utilizar este ejemplo para ayudar a gestionar los bloques existentes que tengan habilitada la función de cumplimiento de normativas heredadas.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida.

Información relacionada

- "Gestione objetos con S3 Object Lock"
- "Cree una política de ILM"

Ejemplo de bloque y objetos para S3 Object Lock

En este ejemplo, una cuenta de inquilino de S3 llamada Bank of ABC ha utilizado el administrador de inquilinos para crear un bloque con el bloqueo de objetos S3 habilitado para almacenar registros bancarios críticos.

Definición de bloque	Valor de ejemplo
Nombre de cuenta de inquilino	Banco de ABC
Nombre del bloque	registros bancarios
Región de bloque	us-east-1 (predeterminado)

Cada objeto y versión de objeto que se agrega al bloque de registros bancarios utilizará los siguientes valores para `retain-until-date` y.. `legal hold` configuración.

Configuración para cada objeto	Valor de ejemplo
`retain-until-date`	“2030-12-30T23:59:59Z” (30 de diciembre de 2030) Cada versión de objeto tiene su propia `retain-until-date` ajuste. Este ajuste se puede aumentar, pero no disminuir.
`legal hold`	APAGADO (no vigente) Se puede colocar o levantar una retención legal en cualquier versión del objeto en cualquier momento durante el período de retención. Si un objeto está sujeto a una conservación legal, dicho objeto no se puede eliminar ni siquiera si el `retain-until-date` se ha alcanzado.

Regla de ILM 1 para S3 Object Lock Ejemplo: Perfil de codificación de borrado con coincidencia de bloques

Esta regla de ILM de ejemplo se aplica solo a la cuenta de inquilino de S3 llamada Bank of ABC. Coincide con cualquier objeto de `bank-records` Bucket y, a continuación, utiliza código de borrado para almacenar el objeto en los nodos de almacenamiento en tres sitios de centros de datos mediante un perfil de código de borrado 6+3. Esta regla satisface los requisitos de los buckets con S3 Object Lock activado: Se mantiene una copia en los nodos de almacenamiento desde el día 0 hasta siempre, utilizando el tiempo de ingesta como tiempo de referencia.

Definición de regla	Valor de ejemplo
Nombre de regla	Regla compatible: Objetos EC en el depósito de registros bancarios - Banco de ABC
Cuenta de inquilino	Banco de ABC
Nombre del bloque	`bank-records`
Filtro avanzado	Tamaño de objeto (MB) mayor que 1 **Nota:** este filtro garantiza que la codificación de borrado no se utilice para objetos de 1 MB o menores.

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	Desde el día 0 almacenar para siempre
Perfil de código de borrado	• Cree una copia codificada con borrado en los nodos de almacenamiento en tres centros de datos • Utiliza un esquema de codificación de borrado de 6+3

Ejemplo de regla ILM 2 para bloqueo de objetos S3: Regla no conforme a las normativas

Esta regla de ILM de ejemplo almacena inicialmente dos copias de objetos replicadas en nodos de almacenamiento. Después de un año, se almacena una copia en un pool de almacenamiento en cloud para siempre. Como esta regla utiliza un pool de almacenamiento en cloud, no es compatible y no se aplica a los objetos en bloques con el bloqueo de objetos S3 habilitado.

Definición de regla	Valor de ejemplo
Nombre de regla	Regla no conforme a las normativas: Use Cloud Storage Pool
Cuentas de inquilino	No especificado
Nombre del bloque	No se especifica, pero solo se aplica a los depósitos que no tienen S3 Object Lock (o la función de cumplimiento de normativas heredada) activada.
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	• El día 0, conserve dos copias replicadas en los nodos de almacenamiento en el centro de datos 1 y en el centro de datos 2 durante 365 días • Después de 1 año, mantenga siempre una copia replicada en un pool de almacenamiento en cloud

Ejemplo de regla ILM 3 para bloqueo de objetos S3: Regla predeterminada

Esta regla de ILM de ejemplo copia los datos de objetos en dos pools de almacenamiento en dos centros de datos. Esta regla de cumplimiento está diseñada para ser la regla predeterminada de la política de ILM. No incluye ningún filtro, no utiliza el tiempo de referencia no corriente y satisface los requisitos de los bloques con el bloqueo de objetos S3 habilitado: Se mantienen dos copias de objetos en los nodos de almacenamiento del día 0 al permanente, utilizando procesamiento como tiempo de referencia.

Definición de regla	Valor de ejemplo
Nombre de regla	Regla de conformidad predeterminada: Dos copias Dos centros de datos
Cuenta de inquilino	No especificado
Nombre del bloque	No especificado
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	De día 0 a siempre, conserve dos copias replicadas (una en los nodos de almacenamiento en el centro de datos 1 y otra en los nodos de almacenamiento en el centro de datos 2).

Ejemplo de política de ILM conforme a la normativa para el bloqueo de objetos S3

Para crear una política de ILM que proteja de manera efectiva todos los objetos del sistema, incluidos los que están en bloques con el bloqueo de objetos S3 habilitado, debe seleccionar reglas de ILM que cumplan con los requisitos de almacenamiento para todos los objetos. A continuación, debe simular y activar la política.

Añada reglas a la política

En este ejemplo, la política de ILM incluye tres reglas de ILM, en el siguiente orden:

1. Regla de conformidad que utiliza la codificación de borrado para proteger objetos de más de 1 MB en un bloque específico con el bloqueo de objetos S3 habilitado. Los objetos se almacenan en nodos de almacenamiento del día 0 al permanente.
2. Una regla no conforme a las normativas que crea dos copias de objetos replicados en los nodos de almacenamiento durante un año y, a continuación, mueve una copia de objetos a un Cloud Storage Pool de forma permanente. Esta regla no se aplica a bloques con el bloqueo de objetos S3 habilitado porque utiliza un pool de almacenamiento en cloud.
3. La regla de cumplimiento predeterminada que crea dos copias de objetos replicados en los nodos de almacenamiento desde el día 0 hasta siempre.

Simule la política

Después de agregar reglas a la política, elegir una regla compatible predeterminada y organizar las demás reglas, debe simular la política probando objetos del depósito con S3 Object Lock activado y desde otros depósitos. Por ejemplo, al simular la directiva de ejemplo, debería esperar que los objetos de prueba se evaluaran de la siguiente manera:

- La primera regla sólo coincidirán con los objetos de prueba que son superiores a 1 MB en los registros bancarios de bloque para el inquilino Banco de ABC.
- La segunda regla coincidirán con todos los objetos de todos los segmentos no compatibles para todas las demás cuentas de arrendatario.
- La regla predeterminada coincidirán con estos objetos:
  - Objetos de 1 MB o menos en los registros bancarios del bloque para el inquilino del Banco de ABC.
  - Objetos de cualquier otro bloque que tenga habilitado el bloqueo de objetos S3 para todas las demás cuentas de inquilino.

Activar la política

Cuando esté completamente satisfecho de que la nueva política protege los datos del objeto según lo esperado, puede activarlo.

Ejemplo 8: Prioridades para el ciclo de vida del bloque de S3 y política de ILM

Según la configuración del ciclo de vida, los objetos siguen los ajustes de retención del ciclo de vida de bloques de S3 o una política de ILM.

Ejemplo de ciclo de vida del bloque que tiene prioridad sobre la política de ILM

Política de ILM

- Regla basada en referencia de tiempo no corriente: En el día 0, mantenga X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminado): En el día 0, mantenga X copias durante 50 días

Ciclo de vida del cucharón

- `Filter: {Prefix: "docs/"}, Expiration: Days: 100, NoncurrentVersionExpiration: Days: 5`

Resultado

- Se ingiere un objeto denominado «docs/text». Coincide con el filtro de ciclo de vida del cucharón del prefijo «docs/».
  - Transcurridos 100 días, se crea un marcador de borrado y los documentos/texto dejan de ser actuales.
  - Transcurridos 5 días, se elimina el término «docs/text» durante un total de 105 días desde la ingesta.
- Se ingiere un objeto llamado «vídeo/película». No coincide con el filtro y utiliza la política de retención de ILM.
  - Después de 50 días, se crea un marcador de borrado y el mensaje «vídeo o película» deja de ser actual.
  - Transcurridos 20 días, se eliminará el «vídeo/película» durante un total de 70 días desde la ingesta.

Ejemplo de ciclo de vida del segmento que se mantiene implícitamente para siempre

Política de ILM

- Regla basada en referencia de tiempo no corriente: En el día 0, mantenga X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminado): En el día 0, mantenga X copias durante 50 días

Ciclo de vida del cucharón

- `Filter: {Prefix: "docs/"}, Expiration: ExpiredObjectDeleteMarker: true`

Resultado

- Se ingiere un objeto denominado «docs/text». Coincide con el filtro de ciclo de vida del cucharón del prefijo «docs/».

  La `Expiration` la acción solo se aplica a los marcadores de borrado caducados, lo que implica mantener todo lo demás para siempre (empezando por «docs/»).

  Los marcadores de borrado que comienzan con «docs/» se eliminan cuando caducan.

- Se ingiere un objeto llamado «vídeo/película». No coincide con el filtro y utiliza la política de retención de ILM.

- Después de 50 días, se crea un marcador de borrado y el mensaje «vídeo o película» deja de ser actual.
- Transcurridos 20 días, se eliminará el «vídeo/película» durante un total de 70 días desde la ingesta.

Ejemplo de uso del ciclo de vida de bloque para duplicar ILM y borrar los marcadores de eliminación vencidos

Política de ILM

- Regla basada en referencia de tiempo no corriente: En el día 0, mantenga X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminado): En el día 0, mantenga X copias durante 50 días

Ciclo de vida del cucharón

- `Filter: {}, Expiration: Days: 50, NoncurrentVersionExpiration: Days: 20`

Resultado

- La política de ILM se duplica en el ciclo de vida del bloque.
- Se ha ingerido un objeto. Ningún filtro significa que el ciclo de vida del bloque se aplica a todos los objetos y anula la configuración de retención de ILM.
  - Después de 50 días, se crea un marcador de borrado y el objeto pasa a ser no actual.
  - Una vez transcurridos 20 días, un total de 70 días desde la ingesta, el objeto no actual se elimina y el marcador de borrado pasa a caducar.
  - Transcurridos 30 días, un total de 100 días desde la ingesta, se elimina el marcador de borrado caducado.

Endurecimiento del sistema

Refuerzo del sistema: Descripción general

El endurecimiento del sistema es el proceso de eliminar tantos riesgos de seguridad como sea posible a través de un sistema StorageGRID.

Este documento proporciona una descripción general de las directrices generales específicas de StorageGRID. Estas directrices complementan las mejores prácticas estándar del sector para el endurecimiento del sistema. Por ejemplo, estas directrices asumen que utiliza contraseñas seguras para StorageGRID, utiliza HTTPS en lugar de HTTP y habilite la autenticación basada en certificados cuando esté disponible.

Al instalar y configurar StorageGRID, puede usar estas directrices para ayudarle a cumplir los objetivos de seguridad prescritos para la confidencialidad, la integridad y la disponibilidad del sistema de información.

StorageGRID sigue el "Política de gestión de vulnerabilidades de NetApp". Las vulnerabilidades notificadas se verifican y se tratan de acuerdo con el proceso de respuesta a incidentes de seguridad del producto.

Consideraciones generales sobre el refuerzo de los sistemas StorageGRID

Al reforzar un sistema StorageGRID, debe tener en cuenta lo siguiente:

- ¿Cuál de las tres redes StorageGRID que ha implementado? Todos los sistemas StorageGRID deben utilizar la red de cuadrícula, pero también puede utilizar la red de administración, la red de cliente o ambas. Cada red tiene diferentes consideraciones de seguridad.

- El tipo de plataformas que utiliza para los nodos individuales del sistema StorageGRID. Los nodos StorageGRID se pueden implementar en máquinas virtuales de VMware, en un motor de contenedores en hosts Linux o como dispositivos de hardware dedicados. Cada tipo de plataforma tiene su propio conjunto de mejores prácticas de optimización.
- Qué confianza tienen las cuentas de inquilino. Si es un proveedor de servicios con cuentas de inquilino que no son de confianza, tendrá problemas de seguridad diferentes a si solo utiliza clientes internos de confianza.
- Los requisitos y convenciones de seguridad que siguen su organización. Es posible que deba cumplir requisitos normativos o corporativos específicos.

Directrices de refuerzo para las actualizaciones de software

Debe mantener su sistema StorageGRID y los servicios relacionados actualizados para defender los ataques.

Actualice al software StorageGRID

Siempre que sea posible, debe actualizar el software StorageGRID a la versión principal más reciente o a la versión principal anterior. Mantener la StorageGRID actualizada ayuda a reducir la cantidad de tiempo que las vulnerabilidades conocidas están activas y reduce el área general de la superficie de ataque. Además, las versiones más recientes de StorageGRID a menudo contienen funciones de refuerzo de la seguridad que no se incluyen en versiones anteriores.

Consulte la "Herramienta de matriz de interoperabilidad de NetApp" (IMT) Para determinar qué versión del software StorageGRID debería utilizar. Cuando se necesita una corrección, NetApp prioriza la creación de actualizaciones para las versiones más recientes. Es posible que algunos parches no sean compatibles con versiones anteriores.

- Para descargar las versiones y correcciones urgentes de StorageGRID más recientes, vaya a. "Descargas de NetApp: StorageGRID".
- Para actualizar el software StorageGRID, consulte "instrucciones de actualización".
- Para aplicar una revisión, consulte "Procedimiento de revisión de StorageGRID".

Actualizaciones a servicios externos

Los servicios externos pueden tener vulnerabilidades que afectan indirectamente a StorageGRID. Debe asegurarse de que los servicios de los que depende StorageGRID se mantengan actualizados. Estos servicios incluyen LDAP, KMS (servidor KMIP o KMS), DNS y NTP.

Para obtener una lista de las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Actualizaciones a hipervisores

Si los nodos de StorageGRID se ejecutan en VMware u otro hipervisor, debe asegurarse de que el software y el firmware del hipervisor estén actualizados.

Para obtener una lista de las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Actualizaciones a nodos Linux

Si los nodos de StorageGRID utilizan plataformas host Linux, debe asegurarse de que las actualizaciones de seguridad y del kernel se apliquen al sistema operativo host. Además, debe aplicar actualizaciones de firmware al hardware vulnerable cuando estas actualizaciones estén disponibles.

Para obtener una lista de las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Directrices de refuerzo para redes de StorageGRID

El sistema StorageGRID admite hasta tres interfaces de red por nodo de grid, lo que permite configurar las redes para cada nodo de grid individual de modo que se ajusten a sus requisitos de seguridad y acceso.

Para obtener información detallada sobre las redes StorageGRID, consulte "Tipos de red StorageGRID".

Directrices para la red Grid

Debe configurar una red de red para todo el tráfico interno de StorageGRID. Todos los nodos de grid se encuentran en Grid Network, por lo que deben poder hablar con el resto de nodos.

Al configurar Grid Network, siga estas directrices:

- Asegúrese de que la red está protegida de clientes que no son de confianza, como los que están en Internet abierto.
- Cuando sea posible, utilice la red de red exclusiva para el tráfico interno. Tanto la red de administración como la red de cliente tienen restricciones de firewall adicionales que bloquean el tráfico externo a los servicios internos. Se admite el uso de Grid Network para el tráfico de clientes externos, pero este uso ofrece menos capas de protección.
- Si la implementación de StorageGRID abarca varios centros de datos, utilice una red privada virtual (VPN) o equivalente en la red de Grid para proporcionar protección adicional para el tráfico interno.
- Algunos procedimientos de mantenimiento requieren un acceso de shell seguro (SSH) en el puerto 22 entre el nodo de administrador principal y todos los demás nodos de grid. Use un firewall externo para restringir el acceso SSH a clientes de confianza.

Directrices para la red administrativa

La red de administración suele utilizarse para tareas administrativas (empleados de confianza que utilizan Grid Manager o SSH) y para comunicarse con otros servicios de confianza como LDAP, DNS, NTP o KMS (o servidor KMIP). Sin embargo, StorageGRID no exige este uso interno.

Si utiliza la red de administración, siga estas directrices:

- Bloquee todos los puertos de tráfico internos en la red administrativa. Consulte "lista de puertos internos".
- Si los clientes que no son de confianza pueden acceder a la red de administración, bloquee el acceso a StorageGRID en la red de administración con un firewall externo.

Directrices para la red de clientes

La red de cliente suele utilizarse para los inquilinos y para comunicarse con servicios externos, como el servicio de replicación de CloudMirror o otro servicio de la plataforma. Sin embargo, StorageGRID no exige

este uso interno.

Si está utilizando la red cliente, siga estas directrices:

- Bloquee todos los puertos de tráfico internos de la red cliente. Consulte "lista de puertos internos".
- Acepte tráfico de cliente entrante sólo en puntos finales configurados explícitamente. Consulte la información acerca de "gestión de controles de firewall".

Directrices de refuerzo para nodos de StorageGRID

Los nodos StorageGRID se pueden implementar en máquinas virtuales de VMware, en un motor de contenedores en hosts Linux o como dispositivos de hardware dedicados. Cada tipo de plataforma y cada tipo de nodo tiene su propio conjunto de prácticas recomendadas de endurecimiento.

Controle el acceso remoto de IPMI a BMC

Es posible habilitar o deshabilitar el acceso IPMI remoto para todos los dispositivos que contengan un BMC. La interfaz de IPMI remota permite que cualquier persona que tenga una cuenta y una contraseña de BMC acceda al hardware de bajo nivel a sus dispositivos StorageGRID. Si no necesita acceso IPMI remoto a BMC, deshabilite esta opción.

- Para controlar el acceso remoto de IPMI a BMC en Grid Manager, vaya a **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD** > **Electrodomésticos**:
  - Desactive la casilla de verificación **Enable remote IPMI access** para desactivar el acceso IPMI a BMC.
  - Seleccione la casilla de verificación **Enable remote IPMI access** para habilitar el acceso de IPMI a BMC.

Configuración del firewall

Como parte del proceso de endurecimiento del sistema, debe revisar las configuraciones de firewall externo y modificarlas para que el tráfico se acepte solo de las direcciones IP y en los puertos de los que se necesite estrictamente.

StorageGRID incluye un firewall interno en cada nodo que mejora la seguridad del grid al permitirle controlar el acceso de red al nodo. Usted debe "gestionar los controles internos del firewall" para evitar el acceso a la red en todos los puertos, excepto los necesarios para su implementación de grid específica. Los cambios de configuración que realice en la página de control del firewall se despliegan en cada nodo.

Específicamente, puede gestionar estas áreas:

- **Direcciones privilegiadas**: Puede permitir que las direcciones IP o subredes seleccionadas accedan a los puertos que están cerrados por la configuración en la pestaña Administrar acceso externo.
- **Administrar el acceso externo**: Puede cerrar los puertos que están abiertos por defecto, o reabrir los puertos previamente cerrados.
- **Red cliente no confiable**: Puede especificar si un nodo confía en el tráfico entrante de la red cliente, así como en los puertos adicionales que desea abrir cuando la red cliente no confiable está configurada.

Aunque este firewall interno proporciona una capa adicional de protección contra algunas amenazas comunes, no elimina la necesidad de un firewall externo.

Para obtener una lista de todos los puertos internos y externos utilizados por StorageGRID, consulte "Referencia de puerto de red".

Desactive los servicios no utilizados

Para todos los nodos StorageGRID, debe deshabilitar o bloquear el acceso a los servicios que no se utilizan. Por ejemplo, si no está planeando configurar el acceso de cliente a los recursos compartidos de auditoría para NFS, bloquee o deshabilite el acceso a estos servicios.

Virtualización, contenedores y hardware compartido

Para todos los nodos de StorageGRID, evite ejecutar StorageGRID en el mismo hardware físico que el software que no es de confianza. No asuma que las protecciones del hipervisor evitarán que el malware acceda a los datos protegidos por StorageGRID si el StorageGRID y el malware existen en el mismo hardware físico. Por ejemplo, los ataques Meltdown y Spectre aprovechan vulnerabilidades críticas en los procesadores modernos y permiten a los programas robar datos en memoria en el mismo equipo.

Proteja los nodos durante la instalación

No permita que usuarios que no sean de confianza accedan a los nodos StorageGRID a través de la red cuando se van a instalar los nodos. Los nodos no son totalmente seguros hasta que se han unido a la cuadrícula.

Directrices para los nodos de administrador

Los nodos de administración, que proporcionan servicios de gestión como configuración, supervisión y registro del sistema. Cuando inicia sesión en el administrador de grid o en el administrador de inquilinos, se conecta a un nodo de administración.

Siga estas directrices para proteger los nodos de administrador en el sistema StorageGRID:

- Proteja todos los nodos de administrador de clientes que no son de confianza, como los que están en Internet abierto. Asegúrese de que ningún cliente que no sea de confianza puede acceder a un nodo de administración en la red de grid, la red de administración o la red de cliente.
- Los grupos StorageGRID controlan el acceso a las funciones de administrador de grid y administrador de inquilinos. Otorgue a cada grupo de usuarios los permisos mínimos necesarios para su función y utilice el modo de acceso de sólo lectura para evitar que los usuarios cambien la configuración.
- Cuando se utilizan extremos de equilibrador de carga de StorageGRID, use nodos de puerta de enlace en lugar de nodos de administrador para el tráfico de cliente que no es de confianza.
- Si tiene inquilinos que no son de confianza, no permita que tengan acceso directo al administrador de inquilinos o a la API de gestión de inquilinos. En su lugar, para que los inquilinos que no son de confianza utilicen un portal de inquilinos o un sistema de gestión de inquilinos externo, que interactúa con la API de gestión de inquilinos.
- Opcionalmente, utilice un proxy de administrador para tener más control sobre la comunicación de AutoSupport de los nodos de administración a Soporte de NetApp. Consulte los pasos para "creando un proxy de administración".
- Opcionalmente, utilice los puertos restringidos 8443 y 9443 para separar las comunicaciones de Grid Manager y de arrendatario Manager. Bloquee el puerto compartido 443 y limite las solicitudes de inquilinos al puerto 9443 para obtener una protección adicional.
- De manera opcional, utilice nodos de administrador separados para los administradores de grid y los usuarios inquilinos.

Para obtener más información, consulte las instrucciones de "Administración de StorageGRID".

Directrices para nodos de almacenamiento

Los nodos de almacenamiento gestionan y almacenan metadatos y datos de objetos. Siga estas directrices para proteger los nodos de almacenamiento en el sistema StorageGRID.

- No permita que los clientes que no son de confianza se conecten directamente con los nodos de almacenamiento. Utilice un punto final de equilibrio de carga servido por un nodo de gateway o un equilibrador de carga de terceros.
- No habilite los servicios de salida para inquilinos que no son de confianza. Por ejemplo, al crear la cuenta para un inquilino que no sea de confianza, no permita que el inquilino utilice su propia fuente de identidad y no permita el uso de servicios de plataforma. Consulte los pasos para "crear una cuenta de inquilino".
- Utilice un equilibrador de carga de terceros para el tráfico de clientes que no sea de confianza. El equilibrio de carga de terceros ofrece más control y niveles adicionales de protección frente a ataques.
- Opcionalmente, utilice un proxy de almacenamiento para tener un mayor control sobre la comunicación de los pools de Cloud Storage y los servicios de plataforma de los nodos de almacenamiento a los servicios externos. Consulte los pasos para "creación de un proxy de almacenamiento".
- Opcionalmente, conéctese a servicios externos mediante la red cliente. A continuación, seleccione **CONFIGURACIÓN** > **Seguridad** > **Control de firewall** > **Redes de clientes sin confianza** e indique que la red cliente del nodo de almacenamiento no es de confianza. El nodo de almacenamiento ya no acepta tráfico entrante en la red cliente, pero sigue permitiendo solicitudes salientes para los servicios de plataforma.

Directrices para los nodos de puerta de enlace

Los nodos de puerta de enlace proporcionan una interfaz opcional de equilibrio de carga que las aplicaciones cliente pueden utilizar para conectarse a StorageGRID. Siga estas directrices para proteger cualquier nodo de puerta de enlace en el sistema StorageGRID:

- Configurar y utilizar puntos finales del equilibrador de carga. Consulte "Consideraciones que tener en cuenta al equilibrio de carga".
- Utilice un equilibrador de carga de terceros entre el cliente y los nodos de puerta de enlace o de almacenamiento para buscar tráfico de cliente que no sea de confianza. El equilibrio de carga de terceros ofrece más control y niveles adicionales de protección frente a ataques. Si utiliza un equilibrador de carga de terceros, se puede configurar opcionalmente el tráfico de red para que pase por un extremo de equilibrador de carga interno o se envíe directamente a nodos de almacenamiento.
- Si utiliza puntos finales de equilibrador de carga, haga que los clientes se conecten a través de la red de cliente de forma opcional. A continuación, seleccione **CONFIGURACIÓN** > **Seguridad** > **Control de firewall** > **Redes de clientes sin confianza** e indique que la red cliente del nodo de gateway no es de confianza. El nodo Gateway sólo acepta tráfico entrante en los puertos configurados explícitamente como extremos equilibradores de carga.

Directrices para los nodos de dispositivos de hardware

Los dispositivos de hardware StorageGRID están especialmente diseñados para su uso en un sistema StorageGRID. Algunos dispositivos se pueden usar como nodos de almacenamiento. Otros dispositivos se pueden usar como nodos de administrador o nodos de puerta de enlace. Puede combinar nodos de dispositivos con nodos basados en software o poner en marcha grids totalmente diseñados para todos los dispositivos.

Siga estas directrices para proteger cualquier nodo de dispositivo de hardware en el sistema StorageGRID:

- Si el dispositivo utiliza System Manager de SANtricity para la gestión de la controladora de almacenamiento, evite que los clientes que no son de confianza accedan a System Manager de SANtricity a través de la red.
- Si el dispositivo tiene un controlador de administración de placa base (BMC), tenga en cuenta que el puerto de administración del BMC permite un acceso bajo al hardware. Conecte el puerto de gestión de BMC sólo a una red de gestión interna segura y de confianza. Si no existe dicha red disponible, deje el puerto de administración del BMC desconectado o bloqueado, a menos que el soporte técnico solicite una conexión al BMC.
- Si el dispositivo admite la administración remota del hardware de la controladora a través de Ethernet mediante el estándar de interfaz de gestión de plataforma inteligente (IPMI), bloquee el tráfico que no sea de confianza en el puerto 623.

> Es posible habilitar o deshabilitar el acceso IPMI remoto para todos los dispositivos que contengan un BMC. La interfaz de IPMI remota permite que cualquier persona que tenga una cuenta y una contraseña de BMC acceda al hardware de bajo nivel a sus dispositivos StorageGRID. Si no necesita acceso remoto de IPMI a BMC, deshabilite esta opción mediante uno de los siguientes métodos:
> En Grid Manager, vaya a **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD** > **Electrodomésticos** y desactive la casilla de verificación **Habilitar acceso remoto a IPMI**.
> En la API de administración de grid, utilice el extremo privado: `PUT /private/bmc`.

- En el caso de los modelos de dispositivos que contienen unidades SED, FDE o FIPS NL-SAS que gestiona con el administrador del sistema de SANtricity, "Habilite y configure SANtricity Drive Security".
- Para los modelos de dispositivos que contienen SSD NVMe SED o FIPS que administra mediante el instalador del dispositivo StorageGRID y Grid Manager, "Habilite y configure el cifrado de unidades StorageGRID".
- En el caso de dispositivos sin unidades SED, FDE o FIPS, habilite y configure el cifrado de nodos de software de StorageGRID "Uso de un servidor de gestión de claves (KMS)".

Directrices de refuerzo para TLS y SSH

Debe reemplazar los certificados predeterminados creados durante la instalación y seleccionar la política de seguridad adecuada para las conexiones TLS y SSH.

Directrices de refuerzo para los certificados

Debe sustituir los certificados predeterminados creados durante la instalación por sus propios certificados personalizados.

Para muchas organizaciones, el certificado digital autofirmado para el acceso web StorageGRID no cumple con sus políticas de seguridad de la información. En los sistemas de producción, debe instalar un certificado digital firmado por CA para utilizarlo en la autenticación de StorageGRID.

Específicamente, debe utilizar certificados de servidor personalizados en lugar de los siguientes certificados predeterminados:

- **Certificado de interfaz de administración**: Se utiliza para asegurar el acceso a Grid Manager, al arrendatario Manager, a la API de gestión de grid y a la API de administración de inquilinos.
- **Certificado API S3 y Swift**: Se utiliza para garantizar el acceso seguro a los nodos de almacenamiento y los nodos de puerta de enlace, que las aplicaciones cliente S3 y Swift utilizan para cargar y descargar

datos de objetos.

Consulte "Gestionar certificados de seguridad" para obtener detalles e instrucciones.

> StorageGRID gestiona los certificados utilizados para los extremos del equilibrador de carga por separado. Para configurar los certificados del equilibrador de carga, consulte "Configurar puntos finales del equilibrador de carga".

Cuando utilice certificados de servidor personalizados, siga estas directrices:

- Los certificados deben tener un `subjectAltName` Que coincida con las entradas de DNS para StorageGRID. Para obtener más información, consulte la sección 4,2.1,6, «Nombre alternativo del asunto», en la "RFC 5280: Certificado PKIX y perfil CRL".
- Cuando sea posible, evite el uso de certificados comodín. Una excepción a esta directriz es el certificado para un punto final de estilo alojado virtual S3, que requiere el uso de un comodín si los nombres de depósito no se conocen por adelantado.
- Cuando debe utilizar comodines en los certificados, debe tomar medidas adicionales para reducir los riesgos. Utilice un patrón comodín como `*.s3.example.com`, y no utilice el `s3.example.com` sufijo para otras aplicaciones. Este patrón también funciona con acceso S3 de estilo de ruta como, por ejemplo `dc1-s1.s3.example.com/mybucket`.
- Establezca los tiempos de caducidad del certificado como cortos (por ejemplo, 2 meses) y utilice la API de gestión de grid para automatizar la rotación del certificado. Esto es especialmente importante para los certificados con caracteres comodín.

Además, los clientes deben usar una comprobación estricta del nombre de host al comunicarse con StorageGRID.

Directrices de endurecimiento para las políticas TLS y SSH

Es posible seleccionar una política de seguridad para determinar qué protocolos y cifrados se usan para establecer conexiones TLS seguras con aplicaciones cliente y conexiones SSH seguras a servicios StorageGRID internos.

La directiva de seguridad controla cómo TLS y SSH cifran los datos en movimiento. Como práctica recomendada, debe desactivar las opciones de cifrado que no son necesarias para la compatibilidad de aplicaciones. Utilice la directiva Modern predeterminada, a menos que el sistema deba cumplir con Common Criteria o que necesite utilizar otros cifrados.

Consulte "Gestione la política TLS y SSH" para obtener detalles e instrucciones.

Otras directrices de endurecimiento

Además de seguir las directrices de refuerzo para redes y nodos de StorageGRID, debe seguir las directrices de refuerzo para otras áreas del sistema StorageGRID.

Registros y mensajes de auditoría

Proteja siempre los registros de StorageGRID y los resultados de mensajes de auditoría de forma segura. Los registros y mensajes de auditoría de StorageGRID proporcionan información de gran valor desde el punto de vista del soporte y la disponibilidad del sistema. Además, la información y los detalles que contienen los registros de StorageGRID y el resultado de un mensaje de auditoría suelen ser confidenciales.

Configure StorageGRID para que envíe eventos de seguridad a un servidor de syslog externo. Si utiliza la exportación de syslog, seleccione TLS y RELP/TLS para los protocolos de transporte.

Consulte "Referencia de archivos de registro" Para obtener más información acerca de los registros de StorageGRID. Consulte "Auditar mensajes" Para obtener más información acerca de los mensajes de auditoría de StorageGRID.

AutoSupport de NetApp

La función AutoSupport de StorageGRID permite supervisar de forma proactiva el estado del sistema y enviar automáticamente paquetes al sitio de soporte de NetApp, al equipo de soporte interno de su organización o a un partner de soporte. De manera predeterminada, el envío de paquetes AutoSupport a NetApp se habilita cuando StorageGRID se configura por primera vez.

Es posible deshabilitar la función AutoSupport. Sin embargo, NetApp recomienda habilitarlo porque AutoSupport ayuda a acelerar la identificación y resolución de problemas en caso de que se produzca un problema en su sistema StorageGRID.

AutoSupport admite HTTPS, HTTP y SMTP para los protocolos de transporte. Debido a la naturaleza confidencial de los paquetes de AutoSupport, NetApp recomienda encarecidamente usar HTTPS como protocolo de transporte predeterminado para enviar paquetes de AutoSupport a NetApp.

Uso compartido de recursos de origen cruzado (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un depósito de S3 si desea que las aplicaciones web de otros dominios puedan acceder a ese depósito y a los objetos de ese depósito. En general, no active CORS a menos que sea necesario. Si se requiere CORS, restringirlo a orígenes de confianza.

Consulte los pasos para "Configuración del uso compartido de recursos de origen cruzado (CORS)".

Dispositivos de seguridad externos

Una solución completa de consolidación debe abordar los mecanismos de seguridad fuera de StorageGRID. El uso de dispositivos de infraestructura adicionales para filtrar y limitar el acceso a StorageGRID es una forma efectiva de establecer y mantener una política de seguridad estricta. Estos dispositivos de seguridad externos incluyen firewalls, sistemas de prevención de intrusiones (IPS) y otros dispositivos de seguridad.

Se recomienda un equilibrador de carga de terceros para el tráfico de clientes que no sea de confianza. El equilibrio de carga de terceros ofrece más control y niveles adicionales de protección frente a ataques.

Mitigación de ransomware

Ayuda a proteger los datos de objetos frente a ataques de ransomware siguiendo las recomendaciones de "Defensa contra ransomware con StorageGRID".

Configure StorageGRID para FabricPool

Configure StorageGRID para FabricPool: Información general

Si utiliza el software ONTAP de NetApp, puede utilizar FabricPool de NetApp para organizar en niveles los datos inactivos en un sistema de almacenamiento de objetos de StorageGRID de NetApp.

Utilice estas instrucciones para:

- Conozca las consideraciones y las prácticas recomendadas para configurar StorageGRID para una carga de trabajo FabricPool.
- Aprenda a configurar un sistema de almacenamiento de objetos StorageGRID para su uso con FabricPool.
- Aprenda a proporcionar los valores necesarios a ONTAP al añadir StorageGRID como nivel de cloud de FabricPool.

Inicio rápido para configurar StorageGRID para FabricPool

Planificación de la configuración

- Decidir qué política de organización en niveles de volúmenes de FabricPool utilizará para organizar los datos de ONTAP inactivos en StorageGRID.
- Planificar e instalar un sistema StorageGRID para satisfacer sus necesidades de rendimiento y capacidad de almacenamiento.
- Familiarícese con el software del sistema StorageGRID, incluido el "Administrador de grid" y la "Administrador de inquilinos".
- Consulte las prácticas recomendadas de FabricPool para "Grupos DE ALTA disponibilidad", "balanceo de carga", "ILM", y. "más".
- Revise estos recursos adicionales, que ofrecen detalles sobre el uso y la configuración de ONTAP y FabricPool:

  "TR-4598: Prácticas recomendadas de FabricPool en ONTAP"

  "ONTAP 9: Información general de gestión de niveles de FabricPool con System Manager"

Realizar tareas de requisitos previos

Obtenga el "Información necesaria para adjuntar StorageGRID como nivel de nube", incluyendo:

- Direcciones IP
- Nombres de dominio
- Certificado SSL

Opcionalmente, configure "federación de identidades" y.. "inicio de sesión único".

Configure los ajustes de StorageGRID

Utilice StorageGRID para obtener los valores que ONTAP necesita para conectarse a la cuadrícula.

Con el "Asistente de configuración de FabricPool" es la forma recomendada y la más rápida de configurar todos los elementos, pero también puede configurar cada entidad manualmente, si es necesario.

Configure ONTAP y DNS

Utilice ONTAP para "añada un nivel de cloud" Que utiliza los valores de StorageGRID. A continuación,

"Configurar entradas DNS" Para asociar direcciones IP a cualquier nombre de dominio que desee utilizar.

5 **Supervisar y gestionar**

Cuando el sistema esté activo, lleve a cabo tareas continuas en ONTAP y StorageGRID para gestionar y supervisar la organización en niveles de los datos de FabricPool a lo largo del tiempo.

¿Qué es FabricPool?

FabricPool es una solución de almacenamiento híbrido de ONTAP que utiliza un agregado flash de alto rendimiento como nivel de rendimiento y un almacén de objetos como nivel del cloud. El uso de agregados habilitados para FabricPool le ayuda a reducir el coste del almacenamiento sin comprometer el rendimiento, la eficiencia o la protección.

FabricPool asocia un nivel de cloud (un almacén de objetos externo, como StorageGRID) con un nivel local (un agregado de almacenamiento de ONTAP) para crear una colección de discos compuesta. A continuación, los volúmenes del FabricPool pueden aprovechar la organización en niveles porque mantienen los datos activos (calientes) en un almacenamiento de alto rendimiento (el nivel local) y organizan en niveles los datos inactivos (fríos) en el almacén de objetos externo (el nivel de cloud).

No se necesitan cambios de arquitectura y puede continuar gestionando sus datos y entorno de aplicaciones desde el sistema de almacenamiento de ONTAP central.

¿Qué es StorageGRID?

StorageGRID de NetApp es una arquitectura de almacenamiento que gestiona los datos como objetos, frente a otras arquitecturas de almacenamiento, como almacenamiento de archivos o bloques. Los objetos se mantienen dentro de un único contenedor (como un depósito) y no se anidan como archivos dentro de un directorio dentro de otros directorios. Aunque el almacenamiento de objetos por lo general proporciona un rendimiento menor que el almacenamiento de archivos o bloques, es mucho más escalable. Los bloques de StorageGRID pueden alojar petabytes de datos y miles de millones de objetos.

¿Por qué usar StorageGRID como nivel de cloud de FabricPool?

FabricPool puede organizar en niveles los datos de ONTAP en diversos proveedores de almacenamiento de objetos, incluidos StorageGRID. A diferencia de los clouds públicos que podrían establecer un número máximo de operaciones de entrada/salida por segundo (IOPS) admitidas a nivel de bloque o contenedor, el rendimiento de StorageGRID se escala con el número de nodos de un sistema. Usar StorageGRID como nivel de cloud de FabricPool le permite mantener sus datos fríos en su propio cloud privado para obtener el máximo rendimiento y un control total sobre sus datos.

Además, no hace falta una licencia de FabricPool cuando utiliza StorageGRID como nivel de cloud.

Información necesaria para adjuntar StorageGRID como nivel de cloud

Para poder asociar StorageGRID como nivel de nube para FabricPool, debe realizar pasos de configuración en StorageGRID y obtener determinados valores para utilizarlos en ONTAP.

¿Qué valores necesito?

La siguiente tabla muestra los valores que debe configurar en StorageGRID y cómo los utiliza ONTAP y el servidor DNS.

Valor	Donde se configura el valor	Donde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	Entrada DNS
Puerto	StorageGRID > Punto final del equilibrador de carga	System Manager de ONTAP > Agregar nivel de cloud
Certificado SSL	StorageGRID > Punto final del equilibrador de carga	System Manager de ONTAP > Agregar nivel de cloud
Nombre del servidor (FQDN)	StorageGRID > Punto final del equilibrador de carga	Entrada DNS
ID de clave de acceso y clave de acceso secreta	StorageGRID > inquilino y bloque	System Manager de ONTAP > Agregar nivel de cloud
Nombre de cubo/contenedor	StorageGRID > inquilino y bloque	System Manager de ONTAP > Agregar nivel de cloud

¿Cómo obtengo estos valores?

Dependiendo de sus requisitos, puede hacer cualquiera de los siguientes pasos para obtener la información que necesita:

- Utilice la "Asistente de configuración de FabricPool". El asistente de configuración de FabricPool ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera un archivo que puede utilizar para configurar System Manager de ONTAP. El asistente le guiará por los pasos necesarios y le ayudará a garantizar que la configuración cumple las prácticas recomendadas de StorageGRID y FabricPool.
- Configure cada elemento manualmente. A continuación, introduzca los valores en ONTAP System Manager o en la CLI de ONTAP. Siga estos pasos:
  a. "Configure un grupo de alta disponibilidad para FabricPool".
  b. "Cree un extremo de equilibrador de carga para FabricPool".
  c. "Cree una cuenta de inquilino para FabricPool".
  d. Inicie sesión en la cuenta de inquilino, y. "cree el bloque y las claves de acceso para el usuario raíz".
  e. Crear una regla de ILM para los datos de FabricPool y añadirla a sus políticas de ILM activas. Consulte "Configurar ILM para los datos de FabricPool".
  f. Opcionalmente, "Cree una política de clasificación del tráfico para FabricPool".

Use el asistente de configuración de FabricPool

Use el asistente de configuración de FabricPool: Consideraciones y requisitos

Puede usar el asistente de configuración de FabricPool para configurar StorageGRID como el sistema de almacenamiento de objetos para un nivel de cloud de FabricPool. Después de completar el asistente de configuración, puede introducir los detalles necesarios en ONTAP System Manager.

Cuándo utilizar el asistente de configuración de FabricPool

El asistente de configuración de FabricPool lo guiará a través de cada paso de configuración de StorageGRID para su uso con FabricPool y configurará automáticamente ciertas entidades para usted, como ILM y las políticas de clasificación de tráfico. Como parte de completar el asistente, descargará un archivo que podrá utilizar para introducir valores en ONTAP System Manager. Utilice el asistente para configurar su sistema con mayor rapidez y asegurarse de que su configuración cumple las prácticas recomendadas de StorageGRID y FabricPool.

Suponiendo que dispone de permiso de acceso de raíz, puede completar el asistente de configuración de FabricPool cuando comience a utilizar el Administrador de grid de StorageGRID, o bien puede acceder al asistente y completarlo en cualquier momento posterior. En función de los requisitos, también puede configurar algunos o todos los elementos necesarios manualmente y, a continuación, utilizar el asistente para ensamblar los valores que ONTAP necesita en un único archivo.

Use el asistente de configuración de FabricPool a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

Antes de utilizar el asistente

Confirme que ha completado estos pasos de requisitos previos.

Revise las prácticas recomendadas

- Usted tiene una comprensión general de "Información necesaria para adjuntar StorageGRID como nivel de nube".
- Ha revisado las prácticas recomendadas de FabricPool para:
  - "Grupos de alta disponibilidad"
  - "Balanceo de carga"
  - "Reglas y políticas de ILM"

Obtenga direcciones IP y configure interfaces VLAN

Si va a configurar un grupo de alta disponibilidad, sabrá a qué nodos se conectará ONTAP y a qué red StorageGRID se usará. También sabe qué valores introducir para la subred CIDR, la dirección IP de la puerta de enlace y las direcciones IP virtuales (VIP).

Si planea utilizar una LAN virtual para segregar el tráfico de FabricPool, ya habrá configurado la interfaz de VLAN. Consulte "Configure las interfaces VLAN".

Configurar la federación de identidades y SSO

Si tiene pensado utilizar la federación de identidades o el inicio de sesión único (SSO) para el sistema StorageGRID, tiene activadas estas funciones. También sabe qué grupo federado debe tener acceso raíz para la cuenta de inquilino que utilizará ONTAP. Consulte "Usar la federación de identidades" y.. "Configurar el inicio de sesión único".

Obtener y configurar nombres de dominio

- Sabe qué nombre de dominio completo (FQDN) debe utilizar para StorageGRID. Las entradas del servidor de nombres de dominio (DNS) asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo de alta disponibilidad que cree con el asistente. Consulte "Configure el servidor DNS".

- Si tiene pensado utilizar S3 solicitudes virtuales de estilo hospedado, tiene "Nombres de dominio de punto final S3 configurados". ONTAP utiliza URL de estilo de ruta de forma predeterminada, pero se recomienda el uso de solicitudes virtuales de estilo hospedado.

Revisión de los requisitos del equilibrio de carga y del certificado de seguridad

Si tiene pensado utilizar el equilibrador de carga StorageGRID, ha revisado el general "consideraciones que tener en cuenta al equilibrio de carga". Tiene los certificados que cargará o los valores necesarios para generar un certificado.

Si planea utilizar un punto final de equilibrio de carga externo (de terceros), tiene el nombre de dominio completo (FQDN), el puerto y el certificado para ese equilibrador de carga.

Confirmar la configuración del pool de almacenamiento ILM

Si instaló inicialmente StorageGRID 11,6 o una versión anterior, configuró el pool de almacenamiento que utilizará. En general, debe crear un pool de almacenamiento para cada sitio de StorageGRID que utilizará para almacenar los datos de ONTAP.

> Este requisito no se aplica si instaló inicialmente StorageGRID 11,7 o 11,8. Cuando instala cualquiera de estas versiones inicialmente, se crean automáticamente pools de almacenamiento para cada sitio.

Relación entre ONTAP y el nivel de cloud de StorageGRID

El asistente de FabricPool lo guiará por el proceso de creación de un único nivel de cloud de StorageGRID que incluye un inquilino de StorageGRID, un conjunto de claves de acceso y un bloque de StorageGRID. Puede asociar este nivel de cloud de StorageGRID a uno o más niveles locales de ONTAP.

La práctica recomendada general es asociar un solo nivel cloud a varios niveles locales en un clúster. Sin embargo, según sus requisitos, es posible que desee utilizar más de un bloque o incluso más de un inquilino StorageGRID para los niveles locales en un único clúster. El uso de diferentes bloques e inquilinos permite aislar el acceso a los datos y los datos entre las capas locales de ONTAP, pero resulta más complejo de configurar y gestionar.

NetApp no recomienda vincular un único nivel de cloud a niveles locales en varios clústeres.

> Para conocer las prácticas recomendadas para usar StorageGRID con NetApp MetroCluster™ y FabricPool Mirror, consulte "TR-4598: Prácticas recomendadas de FabricPool en ONTAP".

Opcional: Use un bloque diferente para cada nivel local

Para utilizar más de un bloque para los niveles locales de un clúster de ONTAP, añada más de un nivel de cloud de StorageGRID en ONTAP. Cada nivel de cloud comparte el mismo grupo de alta disponibilidad, extremo de balanceador de carga, inquilino y claves de acceso, pero utiliza un contenedor diferente (bloque de StorageGRID). Siga estos pasos generales:

1. En Grid Manager de StorageGRID, complete el asistente de configuración de FabricPool para el primer nivel de cloud.
2. En ONTAP System Manager, añada un nivel de cloud y utilice el archivo que ha descargado desde StorageGRID para proporcionar los valores necesarios.
3. En el Administrador de inquilinos de StorageGRID, inicie sesión en el inquilino que creó el asistente y cree un segundo bloque.

4. Vuelva a completar el asistente FabricPool. Seleccione el grupo de alta disponibilidad existente, el extremo del equilibrador de carga y el inquilino. A continuación, seleccione el nuevo bloque que creó manualmente. Cree una regla de ILM nueva para el nuevo bloque y active una política de ILM para incluir esa regla.
5. En ONTAP, añada un segundo nivel de cloud, pero proporcione el nuevo nombre del bloque.

Opcional: Use un inquilino y un depósito diferentes para cada nivel local

Para usar más de un inquilino y conjuntos diferentes de claves de acceso para los niveles locales de un clúster de ONTAP, añada más de un nivel de cloud de StorageGRID en ONTAP. Cada nivel de cloud comparte el mismo grupo de alta disponibilidad, extremo de balanceador de carga, pero utiliza un inquilino, claves de acceso y contenedor (bloque de StorageGRID) diferentes. Siga estos pasos generales:

1. En Grid Manager de StorageGRID, complete el asistente de configuración de FabricPool para el primer nivel de cloud.
2. En ONTAP System Manager, añada un nivel de cloud y utilice el archivo que ha descargado desde StorageGRID para proporcionar los valores necesarios.
3. Vuelva a completar el asistente FabricPool. Seleccione el grupo de alta disponibilidad existente y el extremo del equilibrador de carga. Cree un inquilino y un bloque nuevos. Cree una regla de ILM nueva para el nuevo bloque y active una política de ILM para incluir esa regla.
4. En ONTAP, añada un segundo nivel de cloud pero proporcione la nueva clave de acceso, la clave secreta y el nombre del bloque.

Acceda al asistente de configuración de FabricPool y complete este

Puede usar el asistente de configuración de FabricPool para configurar StorageGRID como el sistema de almacenamiento de objetos para un nivel de cloud de FabricPool.

Antes de empezar

- Ha revisado el "consideraciones y requisitos" Para utilizar el asistente de configuración de FabricPool.

> Si desea configurar StorageGRID para utilizarlo con cualquier otra aplicación cliente S3, vaya a. "Utilice el asistente de configuración de S3".

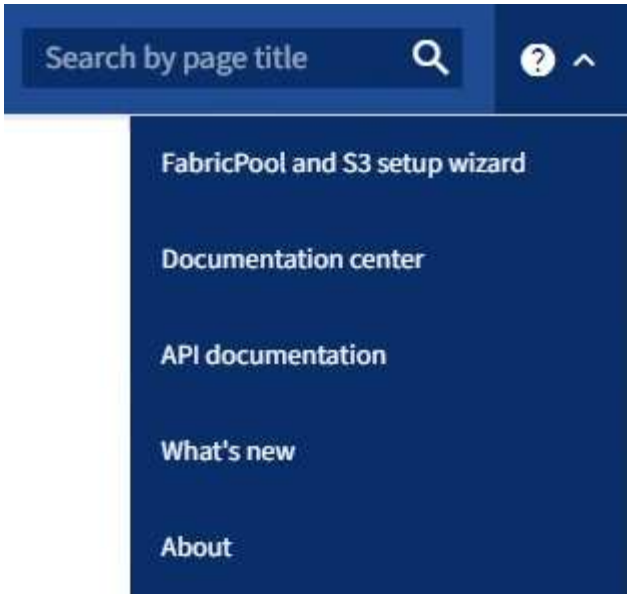
- Usted tiene la "Permiso de acceso raíz".

Acceda al asistente

Puede completar el asistente de configuración de FabricPool cuando empiece a usar el Administrador de grid de StorageGRID, o bien puede acceder al asistente y completarlo en cualquier momento posterior.

Pasos

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Si el banner del asistente de configuración **FabricPool y S3** aparece en el panel de control, seleccione el enlace en el banner. Si el banner ya no aparece, seleccione el icono de ayuda en la barra de encabezado del Administrador de cuadrículas y seleccione **FabricPool y el asistente de configuración S3**.



3. En la sección FabricPool de la página del asistente de configuración de FabricPool y S3, seleccione **Configurar ahora**.

   Paso 1 de 9: Aparece CONFIGURAR GRUPO HA.

Paso 1 de 9: Configurar el grupo de alta disponibilidad

Un grupo de alta disponibilidad es una colección de nodos que contienen el servicio de equilibrador de carga de StorageGRID. Un grupo de alta disponibilidad puede contener nodos de pasarela, nodos de administración o ambos.

Puede usar un grupo de alta disponibilidad para ayudar a mantener disponibles las conexiones de datos FabricPool. Un grupo de alta disponibilidad utiliza direcciones IP virtuales (VIP) para proporcionar acceso de alta disponibilidad al servicio Load Balancer. Si falla la interfaz activa en el grupo HA, una interfaz de backup puede gestionar la carga de trabajo con poco impacto en las operaciones de FabricPool

Para obtener más detalles sobre esta tarea, consulte "Gestión de grupos de alta disponibilidad" y.. "Mejores prácticas para grupos de alta disponibilidad".

Pasos

1. Si va a utilizar un equilibrador de carga externo, no es necesario crear un grupo de alta disponibilidad. Seleccione **Omitir este paso** y vaya a. Paso 2 de 9: Configurar punto final de equilibrio de carga.
2. Para usar el balanceador de carga de StorageGRID, cree un grupo de alta disponibilidad nuevo o use un grupo de alta disponibilidad existente.

Crear grupo de alta disponibilidad

a. Para crear un nuevo grupo HA, selecciona **Crear grupo HA**.

b. Para el paso **Enter details**, complete los siguientes campos.

Campo	Descripción
Nombre del GRUPO HA	Un nombre mostrado exclusivo para este grupo HA.
Descripción (opcional)	La descripción de este grupo de alta disponibilidad.

c. Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo HA.

Utilice los encabezados de columna para ordenar las filas o introduzca un término de búsqueda para localizar las interfaces más rápidamente.

Puede seleccionar uno o varios nodos, pero solo puede seleccionar una interfaz para cada nodo.

d. Para el paso **Priorize interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo HA.

Arrastre las filas para cambiar los valores en la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.

Si el grupo de alta disponibilidad incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si falla esa interfaz, las direcciones VIP pasan a la siguiente interfaz de respaldo, etc. Cuando se resuelven los fallos, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

e. Para el paso **Introducir direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de subred	La dirección de la subred VIP en CIDR notation—Una dirección IPv4 seguida de una barra diagonal y la longitud de subred (0-32). La dirección de red no debe tener ningún bit de host configurado. Por ejemplo: `192.16.0.0/22`.
Dirección IP de la puerta de enlace (opcional)	Opcional. Si las direcciones IP de ONTAP utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID, introduzca la dirección IP de la puerta de enlace local VIP de StorageGRID. La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.

Campo	Descripción
Dirección IP virtual	Introduzca al menos una y como máximo diez direcciones VIP para la interfaz activa en el grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP y todas estarán activas al mismo tiempo en la interfaz activa. Al menos una dirección debe ser IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

f. Seleccione **Crear grupo HA** y luego seleccione **Finalizar** para volver al asistente de configuración de FabricPool.

g. Seleccione **Continuar** para ir al paso del equilibrador de carga.

Use el grupo de alta disponibilidad existente

a. Para usar un grupo HA existente, seleccione el nombre del grupo HA en la lista desplegable **Select an HA group**.

b. Seleccione **Continuar** para ir al paso del equilibrador de carga.

Paso 2 de 9: Configurar punto final de equilibrio de carga

StorageGRID utiliza un balanceador de carga para gestionar la carga de trabajo desde aplicaciones cliente, como FabricPool. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en varios nodos de almacenamiento.

Puede usar el servicio de equilibrador de carga de StorageGRID, que existe en todos los nodos de administración y puerta de enlace, o puede conectarse a un equilibrador de carga externo (de terceros). Se recomienda utilizar el equilibrador de carga de StorageGRID.

Para obtener detalles sobre esta tarea, consulte la sección general "consideraciones que tener en cuenta al equilibrio de carga" y la "Prácticas recomendadas para el equilibrio de carga para FabricPool".

Pasos

1. Seleccione o cree un extremo de equilibrador de carga de StorageGRID o utilice un equilibrador de carga externo.

Crear punto final

a. Seleccione **Crear punto final**.

b. Para el paso **Introducir detalles de punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Nombre descriptivo para el punto final.
Puerto	El puerto StorageGRID que desea usar para el equilibrio de carga. Este campo se establece por defecto en 10433 para el primer punto final que cree, pero puede introducir cualquier puerto externo no utilizado. Si introduce 80 o 443, el punto final se configura sólo en los nodos de Gateway, ya que estos puertos están reservados en los nodos de Admin. **Nota:** Los puertos utilizados por otros servicios de red no están permitidos. Consulte "Referencia de puerto de red".
Tipo de cliente	Debe ser **S3**.
Protocolo de red	Seleccione **HTTPS**. **Nota**: La comunicación con StorageGRID sin cifrado TLS es compatible, pero no se recomienda.

c. Para el paso **Select Binding mode**, especifique el modo de encuadernación. El modo de enlace controla cómo se accede al punto final mediante cualquier dirección IP o mediante direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final mediante la dirección IP de cualquier nodo de gateway o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice el ajuste **Global** (predeterminado) a menos que necesite restringir la accesibilidad de este extremo.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad para acceder a este extremo. Los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que seleccione para los puntos finales no se superpongan.

Modo	Descripción
Interfaces de nodos	Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo	En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este extremo.

d. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir todos los inquilinos (predeterminado)	Todas las cuentas de inquilino pueden usar este extremo para acceder a sus bloques. **Permitir a todos los inquilinos** es casi siempre la opción apropiada para el punto final del equilibrador de carga utilizado para FabricPool. Debe seleccionar esta opción si está utilizando el asistente de configuración de FabricPool para un sistema de StorageGRID nuevo y todavía no ha creado ninguna cuenta de inquilino.
Permitir arrendatarios seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este extremo para acceder a sus bloques.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este punto final para acceder a sus bloques. Todos los demás inquilinos pueden usar este extremo.

e. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Cargar certificado (recomendado)	Use esta opción para cargar un certificado de servidor firmado por CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Use esta opción para generar un certificado autofirmado. Consulte "Configurar puntos finales del equilibrador de carga" para obtener detalles sobre lo que se debe introducir.
Usar certificado StorageGRID S3 y Swift	Esta opción solo está disponible si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID. Consulte "Configure los certificados API S3 y Swift" para obtener más detalles.

f. Seleccione **Finalizar** para volver al asistente de configuración de FabricPool.

g. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Los cambios en el certificado de extremo pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Utilizar punto final de equilibrio de carga existente

a. Seleccione el nombre de un punto final existente de la lista desplegable **Select a load balancer endpoint**.

b. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Utilizar equilibrador de carga externo

a. Complete los siguientes campos para el equilibrador de carga externo.

Campo	Descripción
FQDN	Nombre de dominio completo (FQDN) del equilibrador de carga externo.
Puerto	Número de puerto que FabricPool utilizará para conectar al equilibrador de carga externo.
Certificado	Copie el certificado del servidor para el equilibrador de carga externo y péguelo en este campo.

b. Seleccione **Continuar** para ir al paso del inquilino y del cubo.

Paso 3 de 9: Inquilino y cubo

Un inquilino es una entidad que puede utilizar aplicaciones S3 para almacenar y recuperar objetos en StorageGRID. Cada inquilino tiene sus propios usuarios, claves de acceso, bloques, objetos y un conjunto específico de funcionalidades. Debe crear un inquilino de StorageGRID antes de poder crear el bloque que utilizará FabricPool.

Un bucket es un contenedor que se usa para almacenar los objetos y los metadatos de objetos de un inquilino. Aunque es posible que algunos inquilinos tengan muchos buckets, el asistente le permite crear o seleccionar solo un inquilino y un bucket a la vez. Puede utilizar el Gestor de inquilinos más adelante para agregar los depósitos adicionales que necesite.

Puede crear un inquilino y un bloque nuevos para uso de FabricPool, o puede seleccionar un inquilino y un bloque existentes. Si crea un inquilino nuevo, el sistema crea automáticamente el ID de clave de acceso y la clave de acceso secreta para el usuario raíz del inquilino.

Para obtener más detalles sobre esta tarea, consulte "Cree una cuenta de inquilino para FabricPool" y.. "Cree un bloque de S3 y obtenga una clave de acceso".

Pasos

Cree un nuevo arrendatario y un bloque o seleccione un arrendatario existente.

Inquilino y bloque nuevos

1. Para crear un nuevo inquilino y depósito, introduzca un **Nombre del inquilino**. Por ejemplo: `FabricPool tenant`.
2. Defina el acceso raíz para la cuenta de inquilino en función de si utiliza el sistema StorageGRID "federación de identidades", "Inicio de sesión único (SSO)", o ambos.

Opción	Haga esto
Si la federación de identidades no está activada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidades está activada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si se activan tanto la federación de identidades como el inicio de sesión único (SSO)	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

3. Para **Nombre del cubo**, ingrese el nombre del cubo que FabricPool usará para almacenar datos de ONTAP. Por ejemplo: `fabricpool-bucket`.

   No puede cambiar el nombre del bloque después de crear el bloque.

4. Seleccione la **Región** para este cubo.

   Utilice la región predeterminada (`us-east-1`) A menos que espere utilizar ILM en el futuro para filtrar objetos en función de la región del bloque.

5. Seleccione **Crear y continuar** para crear el inquilino y el depósito y para ir al paso de datos de descarga

Seleccione tenant and bucket

La cuenta de inquilino existente debe tener al menos un depósito que no tenga el control de versiones activado. No puede seleccionar una cuenta de arrendatario existente si no existe ningún depósito para ese arrendatario.

1. Seleccione el arrendatario existente de la lista desplegable **Nombre del arrendatario**.
2. Seleccione el cubo existente de la lista desplegable **Nombre del cubo**.

   FabricPool no admite el control de versiones de objetos, por lo que no se muestran los bloques que tienen el control de versiones activado.

   No seleccione un depósito que tenga S3 Object Lock habilitado para su uso con FabricPool.

3. Seleccione **Continuar** para ir al paso de datos de descarga.

Paso 4 de 9: Descargar la configuración de ONTAP

Durante este paso, debe descargar un archivo que puede usar para introducir valores en ONTAP System Manager.

Pasos

1. Si lo desea, seleccione el icono de copia ( ) Para copiar el ID de clave de acceso y la clave de acceso secreta en el portapapeles.

   Estos valores están incluidos en el archivo de descarga, pero es posible que desee guardarlos por separado.

2. Selecciona **Descargar configuración de ONTAP** para descargar un archivo de texto que contenga los valores que has introducido hasta ahora.

   La `ONTAP_FabricPool_settings_bucketname.txt` En el archivo se incluye la información que necesita configurar StorageGRID como sistema de almacenamiento de objetos para un nivel de cloud de FabricPool, lo que incluye:

   - Detalles de conexión del balanceador de carga, incluido el nombre del servidor (FQDN), el puerto y el certificado
   - Nombre del bloque
   - El ID de clave de acceso y la clave de acceso secreta para el usuario raíz de la cuenta de inquilino

3. Guarde las claves copiadas y el archivo descargado en una ubicación segura.

   > No cierre esta página hasta que haya copiado ambas claves de acceso, descargado la configuración de ONTAP o ambas. Las teclas no estarán disponibles después de cerrar esta página. Asegúrese de guardar esta información en una ubicación segura, ya que se puede utilizar para obtener datos de su sistema StorageGRID.

4. Seleccione la casilla de verificación para confirmar que ha descargado o copiado el ID de clave de acceso y la clave de acceso secreta.
5. Seleccione **Continuar** para ir al paso del pool de almacenamiento ILM.

Paso 5 de 9: Seleccione un pool de almacenamiento

Un pool de almacenamiento es un grupo de nodos de almacenamiento. Cuando se selecciona un pool de almacenamiento, se determina qué nodos StorageGRID utilizará para almacenar los datos organizados en niveles de ONTAP.

Para obtener más información sobre este paso, consulte "Cree un pool de almacenamiento".

Pasos

1. En la lista desplegable **Sitio**, selecciona el sitio StorageGRID que deseas usar para los datos organizados en niveles desde ONTAP.
2. En la lista desplegable **Pool de almacenamiento**, seleccione el grupo de almacenamiento para ese sitio.

   El pool de almacenamiento para un sitio incluye todos los nodos de almacenamiento en ese sitio.

3. Seleccione **Continuar** para ir al paso de la regla ILM.

Paso 6 de 9: Revise la regla de gestión de la vida útil de la información para FabricPool

Las reglas de gestión de la vida útil de la información controlan la ubicación, la duración y el comportamiento de procesamiento de todos los objetos del sistema StorageGRID.

El asistente de configuración de FabricPool crea automáticamente la regla de ILM recomendada para su uso en FabricPool. Esta regla se aplica sólo al bloque especificado. Utiliza código de borrado 2+1 en un único sitio para almacenar los datos organizados en niveles de ONTAP.

Para obtener más información sobre este paso, consulte "Cree la regla de ILM" y.. "Prácticas recomendadas para usar ILM con datos de FabricPool".

Pasos

1. Revise los detalles de la regla.

Campo	Descripción
Nombre de regla	Se genera automáticamente y no se puede cambiar
Descripción	Se genera automáticamente y no se puede cambiar
Filtro	El nombre del cubo Esta regla sólo se aplica a los objetos guardados en el depósito especificado.
Tiempo de referencia	Tiempo de ingesta La instrucción de colocación comienza cuando los objetos se guardan inicialmente en el depósito.
Instrucción de colocación	Use el código de borrado 2+1

2. Ordena el diagrama de retención por **periodo de tiempo** y **Grupo de almacenamiento** para confirmar la instrucción de colocación.
   - El **período de tiempo** para la regla es **Día 0 - Para siempre**. **Día 0** significa que la regla se aplica cuando los datos se almacenan en niveles desde ONTAP. **Forever** significa que StorageGRID ILM no eliminará los datos que se han organizado en niveles desde ONTAP.
   - El **Pool de almacenamiento** para la regla es el pool de almacenamiento seleccionado. **EC 2+1** significa que los datos se almacenarán utilizando la codificación de borrado 2+1. Cada objeto se guardará como dos fragmentos de datos y un fragmento de paridad. Los tres fragmentos para cada objeto se guardarán en nodos de almacenamiento diferentes en un único sitio.
3. Seleccione **Crear y continuar** para crear esta regla y para ir al paso de la política de ILM.

Paso 7 de 9: Revisar y activar la política de ILM

Una vez que el asistente de configuración de FabricPool crea la regla de ILM para su uso en FabricPool, crea una política de ILM. Debe simular y revisar cuidadosamente esta política antes de activarla.

Para obtener más información sobre este paso, consulte "Cree una política de ILM" y.. "Prácticas

recomendadas para usar ILM con datos de FabricPool".

> Al activar una nueva política de ILM, StorageGRID utiliza esa política para gestionar la ubicación, la duración y la protección de datos de todos los objetos del grid, incluidos los objetos existentes y los objetos recién procesados. En algunos casos, la activación de una nueva política puede provocar que los objetos existentes se muevan a nuevas ubicaciones.

> Para evitar la pérdida de datos, no use una regla de ILM que caduque o elimine los datos del nivel de cloud de FabricPool. Establezca el período de retención en **Forever** para asegurarse de que los objetos FabricPool no sean eliminados por StorageGRID ILM.

Pasos

1. Opcionalmente, actualice el **Policy name** generado por el sistema. De forma predeterminada, el sistema agrega «+ FabricPool» al nombre de su política activa o inactiva, pero puede proporcionar su propio nombre.
2. Revise la lista de reglas de la política inactiva.
   - Si el grid no tiene una política de ILM inactiva, el asistente crea una política inactiva clonando la política activa y agregando la nueva regla a la parte superior.
   - Si el grid ya tiene una política de ILM inactiva y esa política utiliza las mismas reglas y el mismo orden que la política de ILM activa, el asistente agrega la nueva regla a la parte superior de la política inactiva.
   - Si la política inactiva contiene reglas diferentes o un orden diferente al de la política activa, el asistente crea una nueva política inactiva clonando la política activa y agregando la nueva regla a la parte superior.
3. Revise el orden de las reglas en la nueva política inactiva.

   Puesto que la regla FabricPool es la primera regla, los objetos del depósito de FabricPool se colocan antes de que se evalúen las demás reglas de la política. Los objetos de cualquier otro depósito se colocan por reglas posteriores de la política.

4. Revise el diagrama de retención para saber cómo se retendrán los diferentes objetos.
   a. Seleccione **Expandir todo** para ver un diagrama de retención para cada regla en la política inactiva.
   b. Seleccione **Período de tiempo** y **Grupo de almacenamiento** para revisar el diagrama de retención. Confirme que cualquier regla que se aplique al depósito o inquilino de FabricPool retenga objetos **para siempre**.
5. Cuando haya revisado la política inactiva, seleccione **Activar y continuar** para activar la directiva y vaya al paso de clasificación de tráfico.

> Los errores en una política de ILM pueden provocar una pérdida de datos irreparable. Revise la política detenidamente antes de activarla.

Paso 8 de 9: Crear política de clasificación de tráfico

Como opción, el asistente de configuración de FabricPool puede crear una política de clasificación del tráfico que puede utilizar para supervisar la carga de trabajo de FabricPool. La política creada por el sistema utiliza una regla de coincidencia para identificar todo el tráfico de red relacionado con el bloque que ha creado. Esta política supervisa únicamente el tráfico; no limita el tráfico de FabricPool ni de otros clientes.

Para obtener más información sobre este paso, consulte "Cree una directiva de clasificación del tráfico para

FabricPool".

Pasos

1. Revise la política.
2. Si desea crear esta política de clasificación de tráfico, seleccione **Crear y continuar**.

   Tan pronto como FabricPool empiece a organizar los datos en niveles en StorageGRID, puede ir a la página Directivas de clasificación del tráfico para ver las métricas del tráfico de red para esta directiva. Posteriormente, también puede agregar reglas para limitar otras cargas de trabajo y asegurarse de que la carga de trabajo de la FabricPool tenga la mayor parte del ancho de banda.

3. De lo contrario, selecciona **Omitir este paso**.

Paso 9 de 9: Resumen de la revisión

El resumen proporciona detalles sobre los elementos configurados, incluidos el nombre del equilibrador de carga, el inquilino y el bloque, la política de clasificación de tráfico y la política de ILM activa.

Pasos

1. Revise el resumen.
2. Seleccione **Finalizar**.

Siguientes pasos

Después de completar el asistente FabricPool, realice estos pasos adicionales.

Pasos

1. Vaya a. "Configure System Manager de ONTAP" Para introducir los valores guardados y completar el lado ONTAP de la conexión. Debe añadir StorageGRID como nivel de cloud, adjuntar el nivel de cloud a un nivel local para crear una FabricPool y establecer las políticas de organización en niveles de los volúmenes.
2. Vaya a. "Configure el servidor DNS" Y asegúrese de que el DNS incluye un registro para asociar el nombre del servidor StorageGRID (nombre de dominio completo) a cada dirección IP de StorageGRID que utilizará.
3. Vaya a. "Otras prácticas recomendadas para StorageGRID y FabricPool" Para conocer las mejores prácticas para los registros de auditoría de StorageGRID y otras opciones de configuración global.

Configure StorageGRID manualmente

Crear un grupo de alta disponibilidad para FabricPool

Al configurar StorageGRID para su uso con FabricPool, puede opcionalmente crear uno o varios grupos de alta disponibilidad (ha).
Un grupo de alta disponibilidad es una colección de nodos que contiene cada uno de ellos el servicio de equilibrador de carga de StorageGRID. Un grupo de alta disponibilidad puede contener nodos de pasarela, nodos de administración o ambos.

Puede usar un grupo de alta disponibilidad para ayudar a mantener disponibles las conexiones de datos FabricPool. Un grupo de alta disponibilidad utiliza direcciones IP virtuales (VIP) para proporcionar acceso de alta disponibilidad al servicio Load Balancer. Si falla la interfaz activa en el grupo HA, una interfaz de backup puede gestionar la carga de trabajo con poco impacto en las operaciones de FabricPool.

Para obtener más detalles sobre esta tarea, consulte "Gestión de grupos de alta disponibilidad". Para utilizar el asistente de configuración de FabricPool y completar esta tarea, vaya a. "Acceda al asistente de configuración de FabricPool y complete este".

Antes de empezar

- Ha revisado el "prácticas recomendadas para grupos de alta disponibilidad".
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".
- Si planea utilizar una VLAN, ha creado la interfaz VLAN. Consulte "Configure las interfaces VLAN".

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
2. Seleccione **Crear**.
3. Para el paso **Enter details**, complete los siguientes campos.

Campo	Descripción
Nombre del GRUPO HA	Un nombre mostrado exclusivo para este grupo HA.
Descripción (opcional)	La descripción de este grupo de alta disponibilidad.

4. Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo HA.

   Utilice los encabezados de columna para ordenar las filas o introduzca un término de búsqueda para localizar las interfaces más rápidamente.

   Puede seleccionar uno o varios nodos, pero solo puede seleccionar una interfaz para cada nodo.

5. Para el paso **Priorize interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo HA.

   Arrastre las filas para cambiar los valores en la columna **Orden de prioridad**.

   La primera interfaz de la lista es la interfaz principal. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.

   Si el grupo de alta disponibilidad incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si falla esa interfaz, las direcciones VIP pasan a la siguiente interfaz de respaldo, etc. Cuando se resuelven los fallos, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

6. Para el paso **Introducir direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de subred	La dirección de la subred VIP en CIDR notation—Una dirección IPv4 seguida de una barra diagonal y la longitud de subred (0-32). La dirección de red no debe tener ningún bit de host configurado. Por ejemplo: `192.16.0.0/22`.

Campo	Descripción
Dirección IP de la puerta de enlace (opcional)	Opcional. Si las direcciones IP de ONTAP utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID, introduzca la dirección IP de la puerta de enlace local VIP de StorageGRID. La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.
Dirección IP virtual	Introduzca al menos una y como máximo diez direcciones VIP para la interfaz activa en el grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP. Al menos una dirección debe ser IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

7. Seleccione **Crear grupo ha** y, a continuación, seleccione **Finalizar**.

Cree un extremo de equilibrador de carga para FabricPool

StorageGRID utiliza un balanceador de carga para gestionar la carga de trabajo desde aplicaciones cliente, como FabricPool. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en varios nodos de almacenamiento.

Al configurar StorageGRID para su uso con FabricPool, debe configurar un extremo de equilibrador de carga y cargar o generar un certificado de extremo de equilibrador de carga, que se utiliza para proteger la conexión entre ONTAP y StorageGRID.

Para utilizar el asistente de configuración de FabricPool y completar esta tarea, vaya a. "Acceda al asistente de configuración de FabricPool y complete este".

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".
- Ha revisado el general "consideraciones que tener en cuenta al equilibrio de carga" así como la "Prácticas recomendadas para el equilibrio de carga para FabricPool".

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**.
2. Seleccione **Crear**.
3. Para el paso **Introducir detalles de punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Nombre descriptivo para el punto final.

Campo	Descripción
Puerto	El puerto StorageGRID que desea usar para el equilibrio de carga. Este campo se establece por defecto en 10433 para el primer punto final que cree, pero puede introducir cualquier puerto externo no utilizado. Si introduce 80 o 443, el punto final se configura sólo en los nodos de Gateway. Estos puertos están reservados en los nodos de administrador. **Nota:** Los puertos utilizados por otros servicios de red no están permitidos. Consulte "Referencia de puerto de red". Proporcionará este número a ONTAP cuando adjunte StorageGRID como nivel de cloud de FabricPool.
Tipo de cliente	Selecciona **S3**.
Protocolo de red	Seleccione **HTTPS**. **Nota**: La comunicación con StorageGRID sin cifrado TLS es compatible, pero no se recomienda.

4. Para el paso **Select Binding mode**, especifique el modo de encuadernación. El modo de enlace controla cómo se accede al punto final mediante cualquier dirección IP o mediante direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final mediante la dirección IP de cualquier nodo de gateway o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice el ajuste **Global** (predeterminado) a menos que necesite restringir la accesibilidad de este extremo.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o el FQDN correspondiente) de un grupo de alta disponibilidad para acceder a este extremo. Los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que seleccione para los puntos finales no se superpongan.
Interfaces de nodos	Los clientes deben usar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo	En función del tipo de nodo que seleccione, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o el FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este extremo.

5. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir todos los inquilinos (predeterminado)	Todas las cuentas de inquilino pueden usar este extremo para acceder a sus bloques. **Permitir a todos los inquilinos** es casi siempre la opción apropiada para el punto final del equilibrador de carga utilizado para FabricPool. Debe seleccionar esta opción si aún no ha creado ninguna cuenta de arrendatario.
Permitir arrendatarios seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este extremo para acceder a sus bloques.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este punto final para acceder a sus bloques. Todos los demás inquilinos pueden usar este extremo.

6. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Cargar certificado (recomendado)	Use esta opción para cargar un certificado de servidor firmado por CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Use esta opción para generar un certificado autofirmado. Consulte "Configurar puntos finales del equilibrador de carga" para obtener detalles sobre lo que se debe introducir.
Usar certificado StorageGRID S3 y Swift	Esta opción solo está disponible si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID. Consulte "Configure los certificados API S3 y Swift" para obtener más detalles.

7. Seleccione **Crear**.

> Los cambios en el certificado de extremo pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Cree una cuenta de inquilino para FabricPool

Debe crear una cuenta de inquilino en el Gestor de grid para uso de FabricPool.

Las cuentas de inquilino permiten a las aplicaciones cliente almacenar y recuperar objetos en StorageGRID. Cada cuenta de inquilino tiene su propio ID de cuenta, grupos y usuarios autorizados, bloques y objetos.

Para obtener más detalles sobre esta tarea, consulte "Cree una cuenta de inquilino". Para utilizar el asistente de configuración de FabricPool y completar esta tarea, vaya a. "Acceda al asistente de configuración de FabricPool y complete este".

Antes de empezar

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

Pasos

1. Seleccione **ARRENDATARIOS**.
2. Seleccione **Crear**.
3. Para los pasos Enter details, introduzca la siguiente información.

Campo	Descripción
Nombre	Un nombre para la cuenta de inquilino. Los nombres de inquilinos no necesitan ser únicos. Cuando se crea la cuenta de arrendatario, recibe un ID de cuenta numérico único.
Descripción (opcional)	Descripción para ayudar a identificar al inquilino.
Tipo de cliente	Debe ser **S3** para FabricPool.
Cuota de almacenamiento (opcional)	Deje este campo en blanco para FabricPool.

4. Para el paso Seleccionar permisos:
   a. No seleccione **Permitir servicios de plataforma**.

      Normalmente, los inquilinos de FabricPool no necesitan usar servicios de plataforma, como la replicación de CloudMirror.

   b. Opcionalmente, selecciona **Usar fuente de identidad propia**.
   c. No seleccione **Permitir selección S3**.

      Los inquilinos de FabricPool no suelen utilizar S3 Select.

   d. Opcionalmente, seleccione **Usar conexión de federación de grid** para permitir que el inquilino utilice a. "conexión de federación de grid" para el clon de cuentas y la replicación entre grid. A continuación, seleccione la conexión de federación de cuadrícula que desea utilizar.
5. Para el paso Definir acceso root, especifique qué usuario tendrá el permiso de acceso root inicial para la cuenta de tenant, en función de si utiliza el sistema StorageGRID "federación de identidades", "Inicio de sesión único (SSO)", o ambos.

Opción	Haga esto
Si la federación de identidades no está activada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.

Opción	Haga esto
Si la federación de identidades está activada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si se activan tanto la federación de identidades como el inicio de sesión único (SSO)	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

6. Seleccione **Crear arrendatario**.

Cree un cubo S3 y obtenga claves de acceso

Antes de usar StorageGRID con una carga de trabajo de FabricPool, debe crear un bucket de S3 para sus datos de FabricPool. También debe obtener una clave de acceso y una clave de acceso secreta para la cuenta de inquilino que utilizará para FabricPool.

Para obtener más detalles sobre esta tarea, consulte "Crear bloque de S3" y.. "Cree sus propias claves de acceso S3". Para utilizar el asistente de configuración de FabricPool y completar esta tarea, vaya a. "Acceda al asistente de configuración de FabricPool y complete este".

Antes de empezar

- Creó una cuenta de inquilino para uso de FabricPool.
- Tiene acceso raíz a la cuenta de inquilino.

Pasos

1. Inicie sesión en el Administrador de inquilinos.

   Puede realizar una de las siguientes acciones:

   - En la página Cuentas de arrendatarios de Grid Manager, seleccione el enlace **Iniciar sesión** para el arrendatario e introduzca sus credenciales.
   - Introduzca la URL para la cuenta de inquilino en un navegador web e introduzca sus credenciales.

2. Cree un bloque de S3 para datos de FabricPool.

   Debe crear un bloque único para cada clúster de ONTAP que vaya a utilizar.

   a. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
   b. Seleccione **Crear cucharón**.
   c. Introduzca el nombre del bucket de StorageGRID que desee usar con FabricPool. Por ejemplo: `fabricpool-bucket`.

      No puede cambiar el nombre del bloque después de crear el bloque.

   d. Seleccione la región para este segmento.

      De forma predeterminada, todos los bloques se crean en la `us-east-1` región.

e. Seleccione **continuar**.

f. Seleccione **Crear cucharón**.

> No seleccione **Activar control de versiones de objetos** para el depósito de FabricPool. Del mismo modo, no edite un bucket de FabricPool para usar **available** o una consistencia no predeterminada. La consistencia de cucharón recomendada para los depósitos de FabricPool es **Leer después de-nuevo-escribir**, que es la consistencia predeterminada para un nuevo depósito.

3. Cree una clave de acceso y una clave de acceso secreta.

a. Seleccione **ALMACENAMIENTO (S3)** > **Mis claves de acceso**.

b. Seleccione **Crear clave**.

c. Seleccione **Crear clave de acceso**.

d. Copie el ID de la clave de acceso y la clave de acceso secreta a una ubicación segura, o seleccione **Descargar .csv** para guardar un archivo de hoja de cálculo que contenga el ID de clave de acceso y la clave de acceso secreta.

   Estos valores se introducirán en ONTAP cuando configure StorageGRID como un nivel de cloud de FabricPool.

> Si genera una nueva clave de acceso y una clave de acceso secreta en StorageGRID en el futuro, introduzca las nuevas claves en ONTAP antes de eliminar los valores anteriores de StorageGRID. De lo contrario, ONTAP podría perder temporalmente su acceso a StorageGRID.

Configurar ILM para los datos de FabricPool

Puede usar esta política de ejemplo sencillo como punto de inicio para sus propias reglas y política de ILM.

Este ejemplo asume que está diseñando las reglas del ILM y una política de ILM para un sistema StorageGRID que tiene cuatro nodos de almacenamiento en un único centro de datos en Denver, Colorado. Los datos de FabricPool en este ejemplo utilizan un bloque llamado `fabricpool-bucket`.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva política, simule para confirmar que funcionará según lo previsto para proteger el contenido de la pérdida. Para obtener más información, consulte "Gestión de objetos con ILM".

> Para evitar la pérdida de datos, no use una regla de ILM que caduque o elimine los datos del nivel de cloud de FabricPool. Establezca el período de retención en **Forever** para asegurarse de que los objetos FabricPool no sean eliminados por StorageGRID ILM.

Antes de empezar

- Ha revisado el "Prácticas recomendadas para usar ILM con datos de FabricPool".
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso de ILM o raíz".

- Si actualizó a StorageGRID 11,8 desde una versión anterior de StorageGRID, configuró el pool de almacenamiento que usará. En general, debe crear un pool de almacenamiento para cada sitio de StorageGRID que utilizará para almacenar datos.

> Este requisito no se aplica si instaló inicialmente StorageGRID 11,7 o 11,8. Cuando instala cualquiera de estas versiones inicialmente, se crean automáticamente pools de almacenamiento para cada sitio.

Pasos

1. Cree una regla de ILM que se aplique solo a los datos de `fabricpool-bucket`. En este ejemplo, se crean copias con código de borrado.

Definición de regla	Valor de ejemplo
Nombre de regla	Código de borrado 2 + 1 para datos de FabricPool
Nombre del bloque	`fabricpool-bucket` También puede filtrar en la cuenta de inquilino de FabricPool.
Filtros avanzados	Tamaño de objeto superior a 0,2 MB. **Nota:** FabricPool solo escribe objetos de 4 MB, pero debe agregar un filtro de tamaño de objeto porque esta regla utiliza codificación de borrado.
Tiempo de referencia	Tiempo de ingesta
Período de tiempo y colocaciones	Desde la tienda del día 0 para siempre Almacene objetos mediante la codificación de borrado usando el esquema EC 2+1 en Denver y conserve esos objetos en StorageGRID para siempre. Para evitar la pérdida de datos, no use una regla de ILM que caduque o elimine los datos del nivel de cloud de FabricPool.
Comportamiento de ingesta	Equilibrado

2. Cree una regla de ILM predeterminada que creará dos copias replicadas de todos los objetos que no coincidan con la primera regla. No seleccione un filtro básico (cuenta de inquilino o nombre de depósito) ni ningún filtro avanzado.

Definición de regla	Valor de ejemplo
Nombre de regla	Dos copias replicadas

Definición de regla	Valor de ejemplo
Nombre del bloque	*none*
Filtros avanzados	*none*
Tiempo de referencia	Tiempo de ingesta
Período de tiempo y colocaciones	Desde la tienda del día 0 para siempre Almacene objetos replicando 2 copias en Denver.
Comportamiento de ingesta	Equilibrado

3. Cree una política de ILM y seleccione las dos reglas. Como la regla de replicación no utiliza ningún filtro, puede ser la regla predeterminada (última) de la directiva.
4. Ingesta de objetos de prueba en el grid.
5. Simule la directiva con los objetos de prueba para verificar el comportamiento.
6. Activar la política.

Cuando se activa esta política, StorageGRID coloca los datos de objetos de la siguiente manera:

- Los datos se organizan en niveles desde FabricPool en `fabricpool-bucket` se codificará para borrado mediante el esquema de código de borrado 2+1. Se colocarán dos fragmentos de datos y un fragmento de paridad en tres nodos de almacenamiento diferentes.
- Se replicarán todos los objetos de todos los demás bloques. Se crearán dos copias y se colocarán en dos nodos de almacenamiento diferentes.
- Las copias se mantendrán en StorageGRID para siempre. Gestión de la vida útil de la información de StorageGRID no eliminará estos objetos.

Cree una directiva de clasificación del tráfico para FabricPool

Opcionalmente, puede diseñar una normativa de clasificación del tráfico StorageGRID para optimizar la calidad del servicio para la carga de trabajo de FabricPool.

Para obtener más detalles sobre esta tarea, consulte "Administrar directivas de clasificación de tráfico". Para utilizar el asistente de configuración de FabricPool y completar esta tarea, vaya a. "Acceda al asistente de configuración de FabricPool y complete este".

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

Acerca de esta tarea

Las prácticas recomendadas para crear una política de clasificación del tráfico para FabricPool dependen de la carga de trabajo de la siguiente manera:

- Si planea organizar en niveles los datos de la carga de trabajo principal de FabricPool en StorageGRID,

debe asegurarse de que la carga de trabajo de FabricPool tenga la mayor parte de ancho de banda. Puede crear una política de clasificación del tráfico para limitar el resto de cargas de trabajo.

> En general, es más importante priorizar las operaciones de lectura de FabricPool que las operaciones de escritura.

Por ejemplo, si otros clientes S3 utilizan este sistema StorageGRID, deberá crear una directiva de clasificación del tráfico. Puede limitar el tráfico de red para los demás bloques, inquilinos, subredes IP o puntos finales de equilibrador de carga.

*Por lo general, no debe imponer límites de calidad de servicio a ninguna carga de trabajo de FabricPool; solo debe limitar las demás cargas de trabajo.

- Los límites puestos en otras cargas de trabajo deben tener en cuenta el comportamiento de estas cargas de trabajo. Los límites impuestos también varían en función del tamaño y las funcionalidades de la cuadrícula y del grado de utilización previsto.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.
2. Seleccione **Crear**.
3. Introduzca un nombre y una descripción (opcional) para la política y seleccione **Continuar**.
4. Para el paso Agregar reglas coincidentes, agregue al menos una regla.
   a. Seleccione **Añadir regla**
   b. En Tipo, seleccione **Punto final de equilibrio de carga** y seleccione el punto final de equilibrio de carga que creó para FabricPool.

      También puede seleccionar la cuenta de inquilino o el bloque de FabricPool.

   c. Si desea que esta política de tráfico limite el tráfico para los otros puntos finales, seleccione **Coincidencia inversa**.
5. Opcionalmente, agregue uno o más límites para controlar el tráfico de red que coincide con la regla.

   > StorageGRID recopila métricas incluso si no agrega ningún límite, para que pueda comprender las tendencias del tráfico.

   a. Selecciona **Añadir un límite**.
   b. Seleccione el tipo de tráfico que desea limitar y el límite que desea aplicar.
6. Seleccione **continuar**.
7. Lea y revise la política de clasificación de tráfico. Utilice el botón **Anterior** para volver atrás y realizar los cambios necesarios. Cuando esté satisfecho con la política, seleccione **Guardar y continuar**.

Después de tu acabado

"Ver las métricas de tráfico de red" para verificar que las políticas están aplicando los límites de tráfico que espera.

Configure System Manager de ONTAP

Una vez que haya obtenido la información de StorageGRID necesaria, puede ir a ONTAP

para añadir StorageGRID como nivel de cloud.

Antes de empezar

- Si completó el asistente de configuración de FabricPool, tiene el `ONTAP_FabricPool_settings_bucketname.txt` archivo descargado.
- Si configuró StorageGRID manualmente, tiene el nombre de dominio completo (FQDN) que utiliza para StorageGRID o la dirección IP virtual (VIP) para el grupo HA de StorageGRID, el número de puerto para el extremo del equilibrador de carga, el certificado del equilibrador de carga y el certificado del equilibrador de carga. El ID de clave de acceso y la clave secreta para el usuario raíz de la cuenta de inquilino, y el nombre de la ONTAP de bloque que usará en ese inquilino.

Acceda a Administrador del sistema de ONTAP

Estas instrucciones describen cómo usar el Administrador del sistema de ONTAP para añadir StorageGRID como nivel de cloud. Puede completar la misma configuración con la CLI de ONTAP. Para obtener instrucciones, vaya a. "ONTAP 9: Gestión de niveles de FabricPool con la interfaz de línea de comandos".

Pasos

1. Acceda a System Manager para el clúster ONTAP que desea organizar en niveles en StorageGRID.
2. Inicie sesión como administrador para el clúster.
3. Navegue hasta **STORAGE** > **Tiers** > **Add Cloud Tier**.
4. Seleccione **StorageGRID** de la lista de proveedores de almacenes de objetos.

Introduzca los valores de StorageGRID

Consulte "ONTAP 9: Información general de gestión de niveles de FabricPool con System Manager" si quiere más información.

Pasos

1. Complete el formulario Agregar nivel de nube, mediante `ONTAP_FabricPool_settings_bucketname.txt` archivo o los valores obtenidos manualmente.

Campo	Descripción
Nombre	Introduzca un nombre único para este nivel de cloud. Puede aceptar el valor predeterminado.
Estilo de URL	Si usted "Nombres de dominio de punto final S3 configurados", Seleccione **Virtual Hosted-Style URL**. **URL de estilo de ruta** es el valor predeterminado para ONTAP, pero se recomienda usar solicitudes de estilo hospedado virtual para StorageGRID. Debe usar **URL de estilo de ruta** si proporciona una dirección IP en lugar de un nombre de dominio para el campo **Nombre de servidor (FQDN)**.

Campo	Descripción
Nombre del servidor (FQDN)	Introduzca el nombre de dominio completo (FQDN) que utiliza para StorageGRID o la dirección IP virtual (VIP) del grupo de alta disponibilidad de StorageGRID. Por ejemplo: `s3.storagegrid.company.com`. Tenga en cuenta lo siguiente: • La dirección IP o el nombre de dominio que especifique aquí deben coincidir con el certificado que haya cargado o generado para el punto final del equilibrador de carga de StorageGRID. • Si proporciona un nombre de dominio, el registro DNS debe asignar a cada dirección IP que utilizará para conectarse a StorageGRID. Consulte "Configure el servidor DNS".
SSL	Activado (predeterminado).
Certificado de almacén de objetos	Pegue el PEM del certificado que está utilizando para el punto final del equilibrador de carga de StorageGRID, que incluye: `-----BEGIN CERTIFICATE-----` y.. `-----END CERTIFICATE-----`. **Nota:** Si una CA intermedia emitió el certificado StorageGRID, debe proporcionar el certificado de CA intermedio. Si la CA raíz emitió directamente el certificado StorageGRID, debe proporcionar el certificado de CA raíz.
Puerto	Introduzca el puerto utilizado por el punto final del equilibrador de carga de StorageGRID. ONTAP utilizará este puerto cuando se conecte a StorageGRID. Por ejemplo, 10433.
Clave de acceso y clave secreta	Introduzca el ID de clave de acceso y la clave de acceso secreta para el usuario raíz de la cuenta de inquilino de StorageGRID. **Consejo**: Si generas una nueva clave de acceso y una clave de acceso secreta en StorageGRID en el futuro, introduce las nuevas claves en ONTAP antes de eliminar los valores antiguos de StorageGRID. De lo contrario, ONTAP podría perder temporalmente su acceso a StorageGRID.
Nombre del contenedor	Introduzca el nombre del bucket de StorageGRID que ha creado para su uso con este nivel de ONTAP.

2. Complete la configuración final de FabricPool en ONTAP.
   a. Adjunte uno o más agregados al nivel de cloud.
   b. Opcionalmente, cree una política de organización en niveles de volúmenes.

Configure el servidor DNS

Después de configurar grupos de alta disponibilidad, puntos finales de equilibrio de carga y nombres de dominio de punto final S3, debe asegurarse de que el DNS incluya las entradas necesarias para StorageGRID. Debe incluir una entrada DNS para cada

nombre del certificado de seguridad y para cada dirección IP que pueda utilizar.

Consulte "Consideraciones que tener en cuenta al equilibrio de carga".

Entradas DNS para el nombre del servidor StorageGRID

Agregue entradas DNS para asociar el nombre del servidor StorageGRID (nombre de dominio completo) a cada dirección IP de StorageGRID que utilice.
Las direcciones IP que introduzca en el DNS dependen de si va a utilizar un grupo de alta disponibilidad de nodos de equilibrio de carga:

- Si ha configurado un grupo de alta disponibilidad, ONTAP se conectará a las direcciones IP virtuales de dicho grupo de alta disponibilidad.
- Si no está utilizando un grupo de alta disponibilidad, ONTAP puede conectarse al servicio de equilibrador de carga de StorageGRID mediante la dirección IP de cualquier nodo de puerta de enlace o nodo de administración.
- Si el nombre del servidor resuelve más de una dirección IP, ONTAP establece conexiones de cliente con todas las direcciones IP (hasta un máximo de 16 direcciones IP). Las direcciones IP se recogen en un método round-robin cuando se establecen conexiones.

Entradas DNS para solicitudes virtuales de estilo alojado

Si ha definido "Nombres de dominio de punto final S3" Y utilizará solicitudes virtuales de estilo hospedado, agregue entradas DNS para todos los nombres de dominio de punto final S3 necesarios, incluidos los nombres de comodín.

Prácticas recomendadas de StorageGRID para FabricPool

Prácticas recomendadas para grupos de alta disponibilidad

Antes de asociar StorageGRID como nivel de cloud de FabricPool, conozca los grupos de alta disponibilidad de StorageGRID y revise las prácticas recomendadas para usar grupos de alta disponibilidad con FabricPool.

¿Qué es un grupo de alta disponibilidad?

Un grupo de alta disponibilidad es una colección de interfaces de varios nodos de puerta de enlace StorageGRID, nodos de administración o ambos. Un grupo de alta disponibilidad ayuda a mantener la disponibilidad de las conexiones de datos de cliente. Si falla la interfaz activa del grupo HA, una interfaz de backup puede gestionar la carga de trabajo con poco impacto en las operaciones de FabricPool.

Cada grupo de alta disponibilidad proporciona acceso de alta disponibilidad a los servicios compartidos en los nodos asociados. Por ejemplo, un grupo de alta disponibilidad que consta de interfaces solo en los nodos de puerta de enlace o en los nodos de administración y de puerta de enlace proporciona un acceso de alta disponibilidad al servicio de equilibrador de carga compartido.

Para obtener más información sobre los grupos de alta disponibilidad, consulte "Gestione grupos de alta disponibilidad".

Usando grupos de alta disponibilidad

Las mejores prácticas para crear un grupo de alta disponibilidad de StorageGRID para FabricPool dependen de la carga de trabajo.

- Si piensa utilizar FabricPool con datos de carga de trabajo principal, debe crear un grupo de alta disponibilidad que incluya al menos dos nodos de equilibrio de carga para evitar la interrupción de la recuperación de datos.
- Si planea utilizar la política de organización en niveles de volúmenes sólo para snapshots de FabricPool o los niveles de rendimiento locales no primarios (por ejemplo, ubicaciones de recuperación ante desastres o destinos de SnapMirror® de NetApp), puede configurar un grupo ha con sólo un nodo.

Estas instrucciones describen cómo configurar un grupo de alta disponibilidad para la alta disponibilidad de Active-Backup (un nodo es activo y uno es backup). Sin embargo, puede que prefiera usar DNS Round Robin o ha activo-activo. Para conocer las ventajas de estas otras configuraciones de alta disponibilidad, consulte "Opciones de configuración para grupos de alta disponibilidad".

Prácticas recomendadas para el equilibrio de carga para FabricPool

Antes de asociar StorageGRID como nivel de cloud de FabricPool, revise las prácticas recomendadas para usar balanceadores de carga con FabricPool.

Para obtener información general sobre el equilibrador de carga StorageGRID y el certificado del equilibrador de carga, consulte "Consideraciones que tener en cuenta al equilibrio de carga".

Prácticas recomendadas para el acceso de inquilinos al extremo del balanceador de carga utilizado para FabricPool

Puede controlar qué inquilinos pueden utilizar un extremo de balanceador de carga específico para acceder a sus bloques. Puede permitir a todos los inquilinos, permitir algunos inquilinos o bloquear algunos inquilinos. Al crear un punto final de equilibrio de carga para el uso de FabricPool, seleccione **Permitir todos los inquilinos**. ONTAP cifra los datos que se almacenan en buckets de StorageGRID, por lo que esta capa de seguridad adicional ofrece poca seguridad adicional.

Prácticas recomendadas para el certificado de seguridad

Cuando se crea un punto final de equilibrio de carga de StorageGRID para uso de FabricPool, se proporciona el certificado de seguridad que permitirá que ONTAP se autentique con StorageGRID.

En la mayoría de los casos, la conexión entre ONTAP y StorageGRID debe utilizar cifrado de seguridad de la capa de transporte (TLS). Pero no es recomendable utilizar FabricPool sin el cifrado TLS. Cuando seleccione el protocolo de red para el punto final del equilibrador de carga StorageGRID, seleccione **HTTPS**. A continuación, proporcione el certificado de seguridad que permitirá la autenticación de ONTAP con StorageGRID.

Para obtener más información acerca del certificado de servidor para un extremo de equilibrio de carga:

- "Gestionar certificados de seguridad"
- "Consideraciones que tener en cuenta al equilibrio de carga"
- "Directrices de refuerzo para certificados de servidor"

Agregar certificado a ONTAP

Al añadir StorageGRID como nivel cloud de FabricPool, debe instalar el mismo certificado en el clúster de ONTAP, incluidos los certificados raíz y todos los certificados de entidad de certificación (CA) subordinados.

Gestionar el vencimiento del certificado

Si el certificado utilizado para proteger la conexión entre ONTAP y StorageGRID caduca, FabricPool dejará de funcionar temporalmente y ONTAP perderá temporalmente el acceso a los datos almacenados en niveles en StorageGRID.

Para evitar problemas de caducidad de certificados, siga las siguientes prácticas recomendadas:

- Monitoree cuidadosamente cualquier alerta que advierta de fechas de vencimiento de certificados que se acercan, como el **Caducidad del certificado de punto final del equilibrador de carga** y **Caducidad del certificado de servidor global para las alertas S3 y Swift API**.
- Mantenga siempre sincronizadas las versiones de StorageGRID y ONTAP del certificado. Si reemplaza o renueva el certificado utilizado para un extremo de balanceador de carga, debe reemplazar o renovar el certificado equivalente utilizado por ONTAP para el nivel de cloud.
- Utilice un certificado de CA firmado públicamente. Si utiliza un certificado firmado por una CA, puede usar la API de gestión de grid para automatizar la rotación de certificados. Esto permite sustituir certificados que pronto caducan de forma no disruptiva.
- Si generó un certificado StorageGRID autofirmado y ese certificado está a punto de caducar, debe sustituir manualmente el certificado tanto en StorageGRID como en ONTAP antes de que caduque el certificado existente. Si ya ha caducado un certificado autofirmado, desactive la validación de certificados en ONTAP para evitar la pérdida de acceso.

  Consulte "Base de conocimientos de NetApp: Cómo configurar un certificado de servidor autofirmado de StorageGRID en una implementación existente de ONTAP FabricPool" si desea obtener instrucciones.

Prácticas recomendadas para usar ILM con datos de FabricPool

Si utiliza FabricPool para organizar los datos en niveles en StorageGRID, debe conocer los requisitos para usar la gestión de la vida útil de la información (ILM) de StorageGRID con los datos de FabricPool.

FabricPool no conoce las reglas ni las políticas de ILM de StorageGRID. Se pueden perder datos si la política de ILM de StorageGRID está mal configurada. Para obtener información detallada, consulte "Cree una regla de ILM: Información general" y.. "Cree una política de ILM: Información general".

Directrices para utilizar ILM con FabricPool

Cuando utiliza el asistente de configuración de FabricPool, el asistente crea automáticamente una nueva regla de ILM para cada bloque de S3 que cree y agrega esa regla a una política inactiva. Se le solicitará que active la política. La regla creada automáticamente sigue las mejores prácticas recomendadas: Utiliza código de borrado 2+1 en un solo sitio.

Si configura StorageGRID manualmente en lugar de usar el asistente de configuración de FabricPool, revise estas directrices para asegurarse de que las reglas de ILM y la política de ILM sean adecuados para los datos de FabricPool y los requisitos del negocio. Es posible que deba crear nuevas reglas y actualizar sus políticas de ILM activas para cumplir con estas directrices.

- Puede utilizar cualquier combinación de reglas de replicación y codificación de borrado para proteger los datos de nivel de cloud.

  La mejor práctica recomendada es utilizar códigos de borrado 2+1 dentro de las instalaciones para una protección de datos rentable. La codificación de borrado utiliza más CPU, pero ofrece mucha menos

capacidad de almacenamiento que la replicación. Los esquemas 4+1 y 6+1 utilizan menos capacidad que el esquema 2+1. Sin embargo, los esquemas 4+1 y 6+1 son menos flexibles si necesita agregar nodos de almacenamiento durante la expansión de la cuadrícula. Para obtener más información, consulte "Añada capacidad de almacenamiento para objetos codificados de borrado".

- Cada regla se aplica a los datos FabricPool debe utilizar código de borrado o bien crear al menos dos copias replicadas.

> Una regla de ILM que crea solo una copia replicada en cualquier periodo de tiempo pone los datos en riesgo de pérdida permanente. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

- Si lo necesita "Eliminar datos de FabricPool de StorageGRID", Use ONTAP para recuperar todos los datos del volumen FabricPool y promocionarlo al nivel de rendimiento.

> Para evitar la pérdida de datos, no use una regla de ILM que caduque o elimine los datos del nivel de cloud de FabricPool. Establezca el período de retención en cada regla de gestión de la vida útil de la información en **forever** para asegurarse de que los objetos de FabricPool no se eliminen mediante gestión de la vida útil de la información de StorageGRID.

- No cree reglas que trasladarán los datos de nivel del cloud de FabricPool fuera del bloque a otra ubicación. No se puede usar un Pool de almacenamiento en cloud para mover datos de FabricPool a otro almacén de objetos. De forma similar, no es posible archivar datos FabricPool en cinta utilizando un nodo de archivado.

> No se puede usar Cloud Storage Pools con FabricPool debido a la latencia añadida de recuperar un objeto del destino de Cloud Storage Pool.

- A partir de ONTAP 9.8, puede crear opcionalmente etiquetas de objeto, con el fin de clasificar y ordenar los datos por niveles para simplificar la gestión. Por ejemplo, puede establecer solo etiquetas en los volúmenes de FabricPool conectados a StorageGRID. A continuación, cuando cree reglas de ILM en StorageGRID, puede utilizar el filtro avanzado etiqueta de objeto para seleccionar y colocar estos datos.

Otras prácticas recomendadas para StorageGRID y FabricPool

Al configurar un sistema StorageGRID para utilizarlo con FabricPool, es posible que deba cambiar otras opciones de StorageGRID. Antes de cambiar una configuración global, considere cómo afectará el cambio a otras aplicaciones S3.

Destinos de registro y mensajes de auditoría

Las cargas de trabajo de FabricPool suelen tener una tasa alta de operaciones de lectura, las que pueden generar un alto volumen de mensajes de auditoría.

- Si no necesita un registro de operaciones de lectura de cliente para FabricPool o cualquier otra aplicación S3, vaya opcionalmente a **CONFIGURACIÓN** > **Monitoreo** > **Servidor de auditoría y syslog**. Cambie la configuración de **Lecturas de cliente** a **Error** para disminuir el número de mensajes de auditoría registrados en el registro de auditoría. Consulte "Configurar los mensajes de auditoría y los destinos de registro" para obtener más detalles.

- Si tiene un grid grande, utilice varios tipos de aplicaciones S3 o desea conservar todos los datos de auditoría, configure un servidor syslog externo y guarde la 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. Consulte "Consideraciones sobre el servidor de syslog externo" para obtener más detalles.

Cifrado de objetos

Al configurar StorageGRID, también puede habilitar el "opción global para el cifrado de objetos almacenados" Si se requiere cifrado de datos para otros clientes StorageGRID. Los datos organizados en niveles desde FabricPool a StorageGRID ya están cifrados, por lo que no es necesario habilitar la configuración de StorageGRID. Las claves de cifrado en el cliente son propiedad de ONTAP.

Compresión de objetos

Al configurar StorageGRID, no habilite el "opción global para comprimir objetos almacenados". Los datos que se organizan en niveles de FabricPool a StorageGRID ya están comprimidos. El uso de la opción StorageGRID no reducirá más el tamaño de un objeto.

Consistencia del cucharón

Para los depósitos de FabricPool, la consistencia del cucharón recomendada es **Read-after-new-write**, que es la consistencia predeterminada para un nuevo cucharón. No edites cubos de FabricPool para usar **available** o **strong-site**.

Organización en niveles de FabricPool

Si un nodo de StorageGRID utiliza almacenamiento asignado desde un sistema ONTAP de NetApp, confirme que el volumen no tiene una política de organización en niveles de FabricPool habilitada. Por ejemplo, si un nodo StorageGRID se ejecuta en un host VMware, asegúrese de que el volumen que realiza el backup del almacén de datos para el nodo StorageGRID no tenga habilitada una política de organización en niveles de FabricPool. Al deshabilitar el almacenamiento en niveles de FabricPool para los volúmenes que se usan con los nodos StorageGRID, se simplifica la solución de problemas y las operaciones de almacenamiento.

> ⚠ No utilice nunca FabricPool para colocar en niveles datos relacionados con StorageGRID en el propio StorageGRID. La organización en niveles de los datos de StorageGRID en StorageGRID aumenta la solución de problemas y la complejidad operativa.

Eliminar datos de FabricPool de StorageGRID

Si necesita eliminar los datos de FabricPool almacenados actualmente en StorageGRID, deberá usar ONTAP para recuperar todos los datos del volumen de FabricPool y promoverlos al nivel de rendimiento.

Antes de empezar

- Ha revisado las instrucciones y consideraciones de "Promocione los datos al nivel de rendimiento".
- Utiliza ONTAP 9,8 o posterior.
- Está utilizando un "navegador web compatible".
- Pertenece a un grupo de usuarios de StorageGRID de la cuenta de inquilino de FabricPool que tiene el "Gestione todos los bloques o permisos de acceso raíz".

Acerca de esta tarea

En estas instrucciones, se explica cómo mover los datos de StorageGRID a FabricPool. Realice este procedimiento con ONTAP y el Administrador de inquilinos de StorageGRID.

Pasos

1. Desde ONTAP, emita el `volume modify` comando.

   Configurado `tiering-policy` para `none` para detener y establecer una nueva organización en niveles `cloud-retrieval-policy` para `promote` Para devolver todos los datos que anteriormente se organizaban en niveles en StorageGRID.

   Consulte "Promocione todos los datos de un volumen de FabricPool al nivel de rendimiento".

2. Espere a que se complete la operación.

   Puede utilizar el `volume object-store` con el `tiering` opción a. "compruebe el estado del ascenso de nivel de rendimiento".

3. Una vez finalizada la operación de promoción, inicie sesión en el Administrador de inquilinos de StorageGRID para la cuenta de inquilino de FabricPool.
4. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
5. Confirme que el bloque de FabricPool está vacío.
6. Si el cucharón está vacío, "elimine el cucharón".

Después de terminar

Al eliminar el bloque, la organización en niveles desde FabricPool hasta StorageGRID ya no puede continuar. Sin embargo, como el nivel local todavía está conectado a la capa de cloud de StorageGRID, System Manager de ONTAP devolverá mensajes de error que indican que no se puede acceder al bloque.

Para evitar estos mensajes de error, realice una de las siguientes acciones:

- Utilice FabricPool Mirror para adjuntar un nivel de cloud diferente al agregado.
- Mueva los datos del agregado de FabricPool a un agregado no compatible con FabricPool y, a continuación, elimine el agregado no utilizado.

Consulte "Documentación de ONTAP para FabricPool" si desea obtener instrucciones.

Utilizar clientes y inquilinos de StorageGRID

Usar una cuenta de inquilino

Usar una cuenta de inquilino: Descripción general

Una cuenta de inquilino permite usar la API DE REST de simple Storage Service (S3) o la API DE REST de Swift para almacenar y recuperar objetos en un sistema StorageGRID.

¿Qué es una cuenta de inquilino?

Cada cuenta de inquilino tiene sus propios grupos locales o federados, usuarios, bloques S3 o contenedores Swift, y objetos.

Las cuentas de arrendatario se pueden utilizar para segregar objetos almacenados por diferentes entidades. Por ejemplo, pueden utilizarse varias cuentas de inquilino en cualquiera de estos casos de uso:

- **Caso de uso empresarial:** Si el sistema StorageGRID se está utilizando dentro de una empresa, el almacenamiento de objetos de la cuadrícula puede estar segregado por los diferentes departamentos de la organización. Por ejemplo, puede haber cuentas de inquilino para el departamento de marketing, el departamento de soporte al cliente, el departamento de recursos humanos, etc.

  > Si utiliza el protocolo cliente S3, también puede utilizar bloques S3 y políticas de bucket para separar objetos entre los departamentos de una empresa. No es necesario crear cuentas de arrendatario independientes. Consulte las instrucciones de implementación "Bloques de S3 y políticas de bloques" si quiere más información.

- **Caso de uso del proveedor de servicios:** Si un proveedor de servicios utiliza el sistema StorageGRID, el almacenamiento de objetos de la cuadrícula puede estar segregado por las diferentes entidades que arriendan el almacenamiento. Por ejemplo, puede que haya cuentas de inquilino para la empresa A, la empresa B, la empresa C, etc.

Cómo crear una cuenta de inquilino

Las cuentas de inquilino se crean mediante una "El administrador de grid de StorageGRID que utiliza Grid Manager". Al crear una cuenta de inquilino, el administrador de grid especifica lo siguiente:

- Información básica, incluido el nombre del inquilino, el tipo de cliente (S3 o Swift) y la cuota de almacenamiento opcional.
- Permisos para la cuenta de inquilino, como si la cuenta de inquilino puede usar los servicios de la plataforma S3, configurar su propio origen de identidad, usar S3 Select o usar una conexión de federación de grid.
- Acceso raíz inicial para el inquilino, basado en si el sistema StorageGRID utiliza usuarios y grupos locales, federación de identidades o inicio de sesión único (SSO).

Además, los administradores de grid pueden habilitar la configuración de bloqueo de objetos de S3 para el sistema StorageGRID si las cuentas de inquilinos S3 necesitan cumplir con los requisitos normativos. Cuando se habilita el bloqueo de objetos S3, todas las cuentas de inquilinos S3 pueden crear y gestionar bloques conforme a la normativa.

Configure los inquilinos S3

Después de un "Se crea la cuenta de inquilino de S3", Puede acceder al Administrador de arrendatarios para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidad se comparta con la cuadrícula)
- Gestionar grupos y usuarios
- Utilice la federación de grid para la clonación de cuentas y la replicación entre grid
- Gestión de claves de acceso de S3
- Cree y gestione bloques de S3
- Utilice los servicios de la plataforma S3
- Utilice S3 Select
- Supervise el uso del almacenamiento

Aunque puede crear y administrar buckets S3 con el Gestor de inquilinos, debe utilizar un "Cliente S3" o. "S3 Consola" para procesar y gestionar objetos.

Configure los inquilinos Swift

Después de un "Se crea la cuenta de inquilino de Swift", Puede acceder al Administrador de arrendatarios para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidad se comparta con la cuadrícula)
- Gestionar grupos y usuarios
- Supervise el uso del almacenamiento

Los usuarios de Swift deben tener el permiso de acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso de acceso raíz no permite que los usuarios se autentiquen en el "API REST de Swift" para crear contenedores y objetos de procesamiento. Los usuarios deben tener el permiso de administrador de Swift para autenticarse en la API DE REST de Swift.

Cómo iniciar sesión y salir

Inicie sesión en el Administrador de inquilinos

Para acceder al Administrador de arrendatarios, introduzca la dirección URL del arrendatario en la barra de direcciones de un "navegador web compatible".

Antes de empezar

- Tiene sus credenciales de inicio de sesión.
- Dispone de una dirección URL para acceder al gestor de inquilinos, tal y como proporciona el administrador de grid. La dirección URL tendrá el aspecto de uno de estos ejemplos:

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/

https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

La URL siempre incluye un nombre de dominio completo (FQDN), la dirección IP de un nodo de administración o la dirección IP virtual de un grupo de alta disponibilidad de nodos de administración. También puede incluir un número de puerto, el ID de cuenta de inquilino de 20 dígitos o ambos.

- Si la URL no incluye el ID de cuenta de 20 dígitos del inquilino, tiene este ID de cuenta.
- Está utilizando un "navegador web compatible".
- Las cookies están habilitadas en su navegador web.
- Pertenece a un grupo de usuarios que tiene "permisos de acceso específicos".

Pasos

1. Inicie un "navegador web compatible".
2. En la barra de dirección del navegador, introduzca la URL para acceder al Administrador de inquilinos.
3. Si se le solicita una alerta de seguridad, instale el certificado con el asistente de instalación del explorador.
4. Inicie sesión en el Administrador de inquilinos.

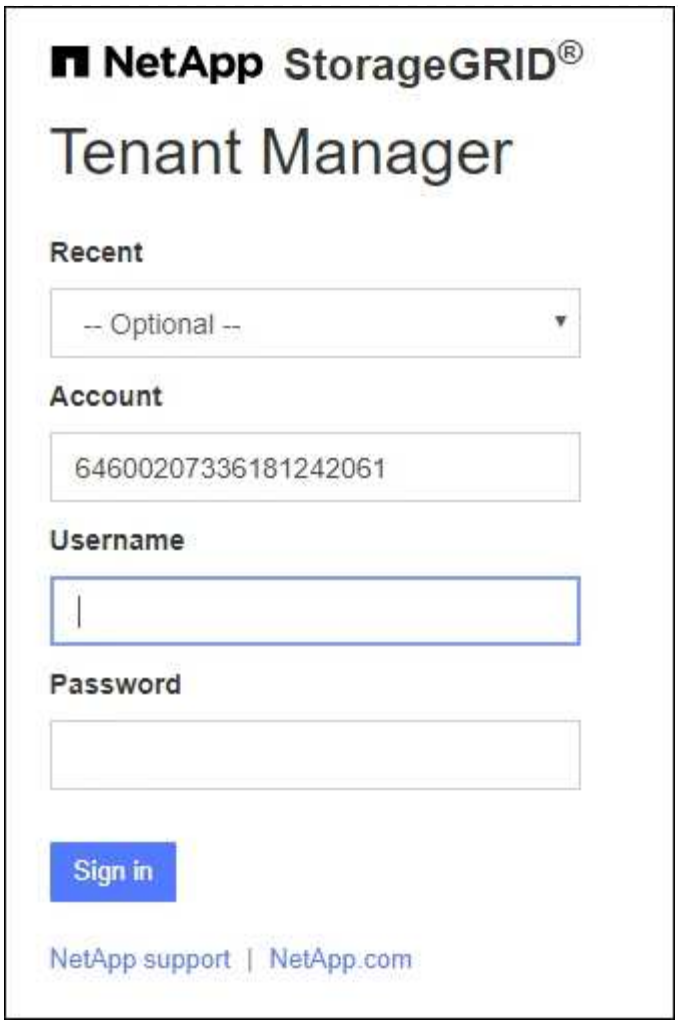
   La pantalla de inicio de sesión que aparece depende de la dirección URL introducida y de si se ha configurado el inicio de sesión único (SSO) para StorageGRID.

No se utiliza SSO

Si StorageGRID no utiliza SSO, aparecerá una de las siguientes pantallas:

- La página de inicio de sesión de Grid Manager. Seleccione el enlace **Inscrito de inquilino**.

- La página de inicio de sesión del administrador de inquilinos. Es posible que el campo **Cuenta** ya esté completado, como se muestra a continuación.



i. Si no se muestra el ID de cuenta de 20 dígitos del arrendatario, seleccione el nombre de la cuenta de arrendatario si aparece en la lista de cuentas recientes o introduzca el ID de cuenta.

ii. Introduzca su nombre de usuario y contraseña.

iii. Seleccione **Iniciar sesión**.

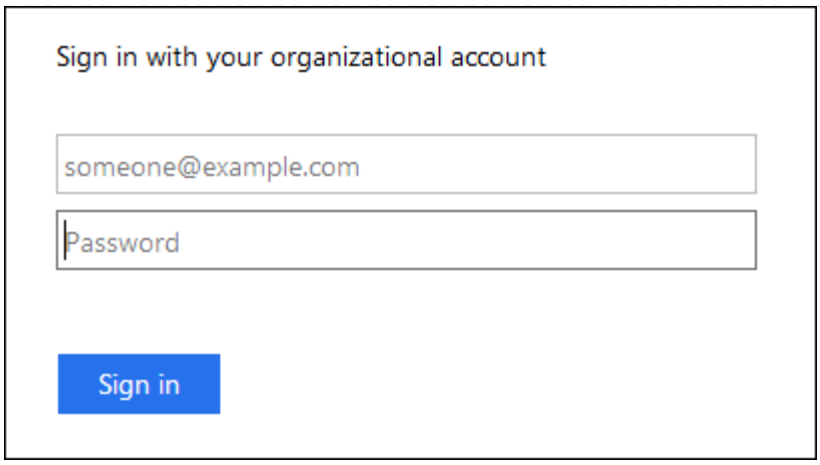
Aparece el panel de control del gestor de inquilinos.

iv. Si recibió una contraseña inicial de otra persona, seleccione ***username*** > **Cambiar contraseña** para proteger su cuenta.

Uso de SSO

Si StorageGRID utiliza SSO, aparece una de las siguientes pantallas:

◦ La página de SSO de su organización. Por ejemplo:



Ingrese sus credenciales estándar de SSO y seleccione **Iniciar sesión**.

- La página de inicio de sesión SSO de inquilino Manager.

i. Si no se muestra el ID de cuenta de 20 dígitos del arrendatario, seleccione el nombre de la cuenta de arrendatario si aparece en la lista de cuentas recientes o introduzca el ID de cuenta.

ii. Seleccione **Iniciar sesión**.

iii. Inicie sesión con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización.

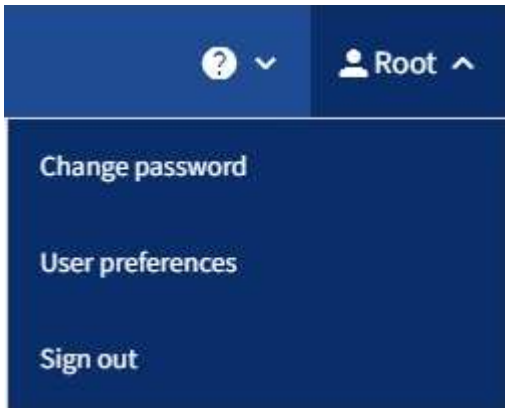
Aparece el panel de control del gestor de inquilinos.

Cierre la sesión del responsable de inquilinos

Cuando haya terminado de trabajar con el Administrador de inquilinos, debe cerrar sesión para asegurarse de que los usuarios no autorizados no puedan acceder al sistema StorageGRID. Es posible que cerrar el navegador no le cierre la sesión del sistema según la configuración de cookies del navegador.

Pasos

1. Busque el menú desplegable username en la esquina superior derecha de la interfaz de usuario.



2. Seleccione el nombre de usuario y luego seleccione **Cerrar sesión**.

   - Si SSO no está en uso:

     Ha cerrado sesión en el nodo de administrador. Se muestra la página de inicio de sesión del administrador de inquilinos.

     Si ha iniciado sesión en más de un nodo de administrador, debe cerrar la sesión de cada nodo.

   - Si SSO está habilitado:

     Inició sesión en todos los nodos de administrador a los que accedían. Aparece la página Inicio de sesión de StorageGRID. El nombre de la cuenta de arrendatario a la que acaba de acceder aparece como el valor predeterminado en el menú desplegable **Cuentas recientes**, y se muestra el **ID de cuenta** del arrendatario.

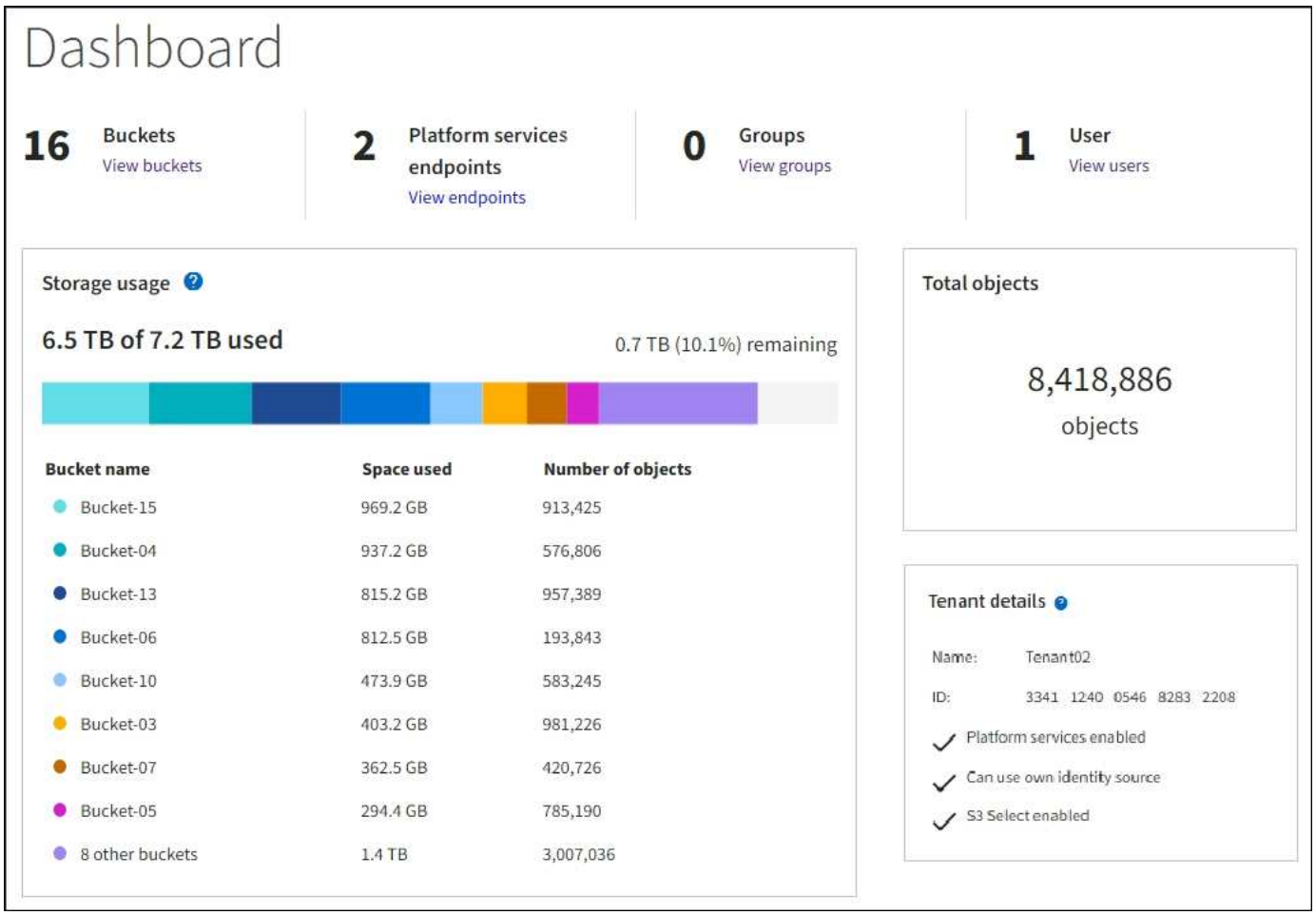
     Si SSO está activado y también ha iniciado sesión en Grid Manager, también debe cerrar sesión en Grid Manager para cerrar sesión en SSO.

Conozca la consola de tenant Manager

La consola de tenant Manager proporciona información general de la configuración de una cuenta de inquilino y la cantidad de espacio que usan los objetos de los bloques del inquilino (S3) o los contenedores (Swift). Si el inquilino tiene una cuota, la consola muestra cuánta cuota se usa y cuánta queda. Si hay algún error relacionado con la cuenta de inquilino, los errores se muestran en el panel de control.

Los valores de espacio utilizado son estimaciones. Estas estimaciones se ven afectadas por el tiempo de los ingests, la conectividad de red y el estado del nodo.

Cuando se han cargado objetos, el panel de control tiene el siguiente ejemplo:



Resumen de la cuenta de inquilino

La parte superior del panel contiene la siguiente información:

- El número de bloques o contenedores, grupos y usuarios configurados
- El número de extremos de servicios de plataforma, si se han configurado alguno

Puede seleccionar los enlaces para ver los detalles.

La parte derecha del panel contiene la siguiente información:

- Número total de objetos para el arrendatario.

  Para una cuenta S3, si no se ha ingerido ningún objeto y tiene el "Permiso de acceso raíz", aparecen las directrices de inicio en lugar del número total de objetos.

- Detalles de inquilinos, incluidos el nombre e ID de la cuenta de inquilino y si este puede usar "servicios de plataforma", "su propia fuente de identidad", "federación de grid", o. "S3 Select" (sólo se muestran los permisos habilitados).

Aprovechamiento del almacenamiento y de la cuota

El panel uso del almacenamiento contiene la siguiente información:

- La cantidad de datos de objeto para el inquilino.

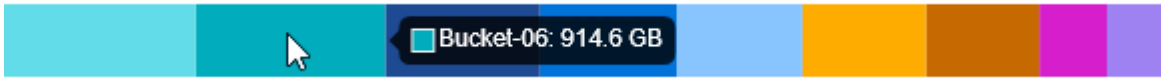
  Este valor indica la cantidad total de datos de objeto cargados y no representa el espacio utilizado para almacenar copias de esos objetos y sus metadatos.

- Si se establece una cuota, la cantidad total de espacio disponible para los datos del objeto y la cantidad y el porcentaje de espacio restante. La cuota limita la cantidad de datos de objetos que se pueden procesar.

  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.

- Un gráfico de barras que representa los tamaños relativos de los cubos o contenedores más grandes.

  Puede colocar el cursor sobre cualquiera de los segmentos del gráfico para ver el espacio total consumido por ese cucharón o contenedor.



- Para corresponder con el gráfico de barras, una lista de los cubos o contenedores más grandes, incluida la cantidad total de datos de objeto y el número de objetos de cada cucharón o contenedor.

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

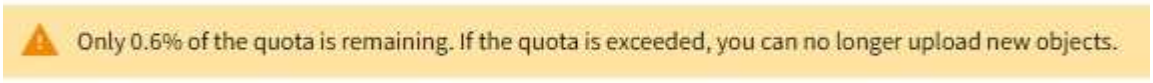
Si el inquilino tiene más de nueve cubos o contenedores, el resto de cubos o contenedores se combinan en una sola entrada al final de la lista.

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

Alertas de uso de cuotas

Si se han habilitado alertas de uso de cuota en Grid Manager, aparecerán en el Gestor de arrendatarios cuando la cuota sea baja o excedida, de la siguiente manera:

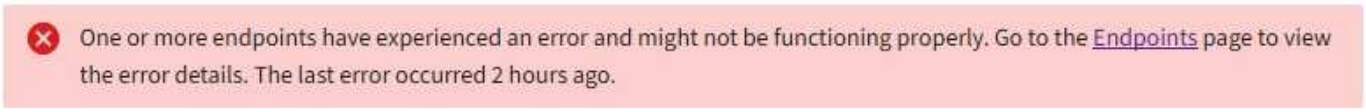
Si se ha utilizado un 90% o más de la cuota de un inquilino, se activa la alerta **uso de cuota de inquilino alto**. Realice las acciones recomendadas para la alerta.



Si excedes tu cuota, no podrás cargar nuevos objetos.

Errores de punto final

Si ha utilizado Grid Manager para configurar uno o más puntos finales para su uso con servicios de plataforma, el panel de control de tenant Manager muestra una alerta si se han producido errores de punto final en los últimos siete días.



Para ver los detalles acerca de "errores de punto final de servicios de plataforma", Seleccione **Endpoints** para mostrar la página Endpoints.

API de gestión de inquilinos

Comprender la API de gestión de inquilinos

Puede realizar tareas de administración del sistema mediante la API REST de gestión de inquilinos en lugar de la interfaz de usuario de inquilino Manager. Por ejemplo, se recomienda utilizar la API para automatizar operaciones o crear varias entidades, como los usuarios, más rápidamente.

API de gestión de inquilinos:

- Utiliza la plataforma API de código abierto de Swagger. Swagger proporciona una interfaz de usuario intuitiva que permite a los desarrolladores y no desarrolladores interactuar con la API. La interfaz de usuario de Swagger proporciona detalles y documentación completos para cada operación de API.

- Utiliza "creación de versiones para dar cabida a actualizaciones no disruptivas".

Para acceder a la documentación de Swagger para la API de gestión de inquilinos:

1. Inicie sesión en el Administrador de inquilinos.
2. En la parte superior del Administrador de inquilinos, selecciona el icono de ayuda y selecciona **Documentación de API**.

Operaciones de API

La API de gestión de inquilinos organiza las operaciones de API disponibles en las siguientes secciones:

- **CUENTA**: Operaciones en la cuenta de inquilino actual, incluida la obtención de información de uso de almacenamiento.
- **AUTH**: Operaciones para realizar la autenticación de sesión de usuario.

  La API de administración de arrendatarios admite el esquema de autenticación de token Bearer. Para el inicio de sesión de un inquilino, debe proporcionar un nombre de usuario, una contraseña y un ID de cuenta en el cuerpo JSON de la solicitud de autenticación (es decir, `POST /api/v3/authorize`). Si el usuario se autentica correctamente, se devuelve un token de seguridad. Este token se debe proporcionar en el encabezado de las posteriores solicitudes de API ("autorización: Token del portador").

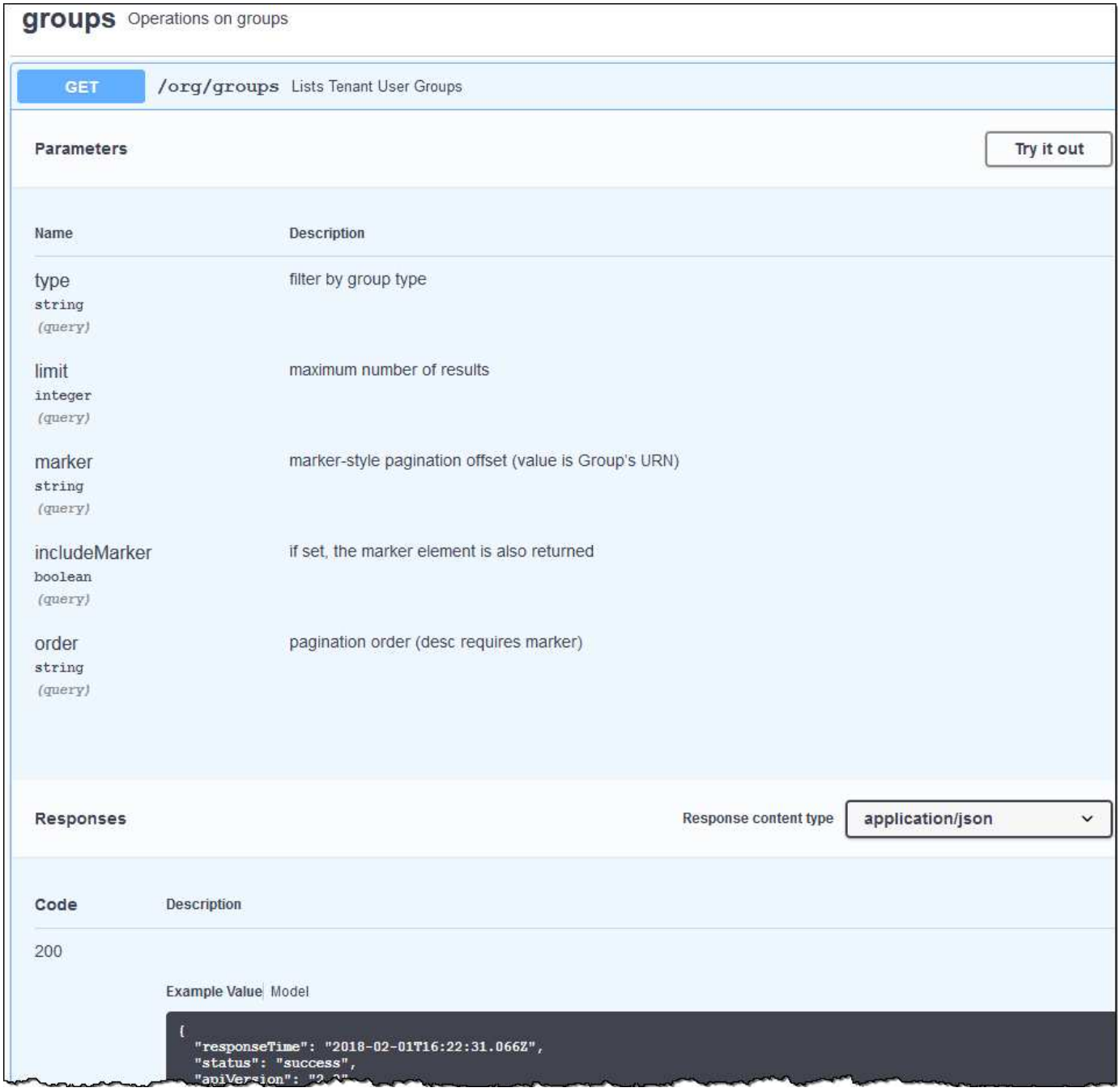
  Para obtener información acerca de cómo mejorar la seguridad de autenticación, consulte "Protección contra falsificación de solicitudes entre sitios".

  > Si está habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, debe realizar diferentes pasos para la autenticación. Consulte "Instrucciones de uso de la API de gestión de grid".

- **Config**: Operaciones relacionadas con el lanzamiento del producto y versiones de la API de Gestión de Inquilinos. Puede mostrar la versión de la versión del producto y las versiones principales de la API que admite esa versión.
- **Contenedores**: Operaciones en S3 cubos o contenedores Swift.
- **Funciones desactivadas**: Operaciones para ver características que podrían haber sido desactivadas.
- **Endpoints**: Operaciones para gestionar un endpoint. Los extremos permiten que un bloque de S3 use un servicio externo para la replicación de CloudMirror de StorageGRID, notificaciones o integración de búsqueda.
- **Grid-federation-connections**: Operaciones en conexiones de federación de grid y replicación entre grid.
- **GRUPOS**: Operaciones para administrar grupos de inquilinos locales y para recuperar grupos de inquilinos federados de una fuente de identidad externa.
- **Identity-source**: Operaciones para configurar una fuente de identidad externa y sincronizar manualmente la información federada del grupo y del usuario.
- **ilm**: Operaciones en la configuración de gestión del ciclo de vida de la información (ILM).
- **REGIONS**: Operaciones para determinar qué regiones se han configurado para el sistema StorageGRID.
- **S3**: Operaciones para administrar las claves de acceso S3 para los usuarios inquilinos.
- **S3-OBJECT-LOCK**: Operaciones en la configuración global de S3 Object Lock, utilizada para apoyar el cumplimiento normativo.
- **Usuarios**: Operaciones para ver y administrar usuarios inquilinos.

Detalles de la operación

Al expandir cada operación de API, puede ver su acción HTTP, su URL de extremo, una lista de cualquier parámetro requerido o opcional, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.



Emita solicitudes API

> Cualquier operación de API que realice mediante la página web de documentos de API es una operación en directo. Tenga cuidado de no crear, actualizar o eliminar datos de configuración u otros datos por error.

Pasos

1. Seleccione la acción HTTP para ver los detalles de la solicitud.

2. Determine si la solicitud requiere parámetros adicionales, como un ID de grupo o de usuario. A continuación, obtenga estos valores. Es posible que primero deba emitir una solicitud de API diferente para obtener la información que necesita.
3. Determine si necesita modificar el cuerpo de solicitud de ejemplo. Si es así, puede seleccionar **Modelo** para conocer los requisitos de cada campo.
4. Seleccione **probar**.
5. Proporcione los parámetros necesarios o modifique el cuerpo de la solicitud según sea necesario.
6. Seleccione **Ejecutar**.
7. Revise el código de respuesta para determinar si la solicitud se ha realizado correctamente.

Creación de versiones de la API de gestión de inquilinos

La API de gestión de inquilinos utiliza versiones para dar cabida a actualizaciones no disruptivas.

Por ejemplo, esta URL de solicitud especifica la versión 4 de la API.

`https://hostname_or_ip_address/api/v4/authorize`

La versión principal de la API se salta cuando se realizan cambios que son *no compatibles* con versiones anteriores. La versión secundaria de la API se salta cuando se realizan cambios que son compatibles con versiones anteriores. Los cambios compatibles incluyen la adición de nuevos extremos o nuevas propiedades.

En el ejemplo siguiente se muestra cómo la versión de API se bONTAP en función del tipo de cambios realizados.

Tipo de cambio en la API	Versión anterior	Nueva versión
Compatible con versiones anteriores	2,1	2,2
No es compatible con versiones anteriores	2,1	3,0

Al instalar el software StorageGRID por primera vez, solo se habilita la versión más reciente de la API. Sin embargo, cuando actualice a una versión de función nueva de StorageGRID, seguirá teniendo acceso a la versión de API anterior para al menos una versión de función de StorageGRID.

> Puede configurar las versiones admitidas. Consulte la sección **config** de la documentación de la API de Swagger para el "API de gestión de grid" si quiere más información. Debe desactivar la compatibilidad con la versión anterior después de actualizar todos los clientes API para que usen la versión más reciente.

Las solicitudes obsoletas se marcan como obsoletas de las siguientes formas:

- El encabezado de la respuesta es "Dedeprecated: True"
- El cuerpo de respuesta JSON incluye "obsoleto": TRUE
- Se agrega una advertencia obsoleta a nms.log. Por ejemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determine qué versiones de API son compatibles con la versión actual

Utilice la `GET /versions` Solicitud de API para devolver una lista de las versiones principales de la API admitidas. Esta solicitud se encuentra en la sección **config** de la documentación de la API de Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Especifique una versión API para una solicitud

Puede especificar la versión de API mediante un parámetro path (`/api/v4`) o un encabezado (`Api-Version: 4`). Si proporciona ambos valores, el valor de encabezado anula el valor de ruta de acceso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protección contra falsificación de solicitudes entre sitios (CSRF)

Puede ayudar a protegerse contra ataques de falsificación de solicitudes entre sitios (CSRF) contra StorageGRID mediante tokens CSRF para mejorar la autenticación que usa cookies. El administrador de grid y el administrador de inquilinos habilitan automáticamente esta característica de seguridad; otros clientes de API pueden elegir si habilitar la función cuando se conectan.

Un atacante que pueda activar una solicitud a un sitio diferente (por ejemplo, con UNA POST de formulario HTTP) puede provocar ciertas solicitudes mediante las cookies del usuario que ha iniciado sesión.

StorageGRID ayuda a proteger contra ataques de CSRF mediante tokens CSRF. Cuando se activa, el contenido de una cookie específica debe coincidir con el contenido de un encabezado específico o de un parámetro DE cuerpo DE POST específico.

Para habilitar la función, configure la `csrfToken` parámetro a. `true` durante la autenticación. El valor predeterminado es `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Cuando es verdadero, un `GridCsrfToken` Cookie se establece con un valor aleatorio para las operaciones de inicio de sesión en Grid Manager y en `AccountCsrfToken` Cookie se establece con un valor aleatorio para las operaciones de inicio de sesión en el Administrador de inquilinos.

Si la cookie está presente, todas las solicitudes que puedan modificar el estado del sistema (POST, PUT, PATCH, DELETE) deben incluir una de las siguientes:

- La `X-Csrf-Token` Encabezado, con el valor del encabezado establecido en el valor de la cookie de token de CSRF.
- Para los extremos que aceptan un cuerpo codificado mediante formulario: A. `csrfToken` parámetro de cuerpo de solicitud codificado mediante formulario.

Para configurar la protección CSRF, utilice "API de gestión de grid" o. "API de gestión de inquilinos".

> Las solicitudes que tienen un conjunto de cookies de token CSRF también aplicarán el encabezado de tipo de contenido: Aplicación/json para cualquier solicitud que espere un cuerpo de solicitud JSON como una protección adicional contra los ataques CSRF.

Utilizar conexiones de federación de grid

Clone los usuarios y los grupos de inquilinos

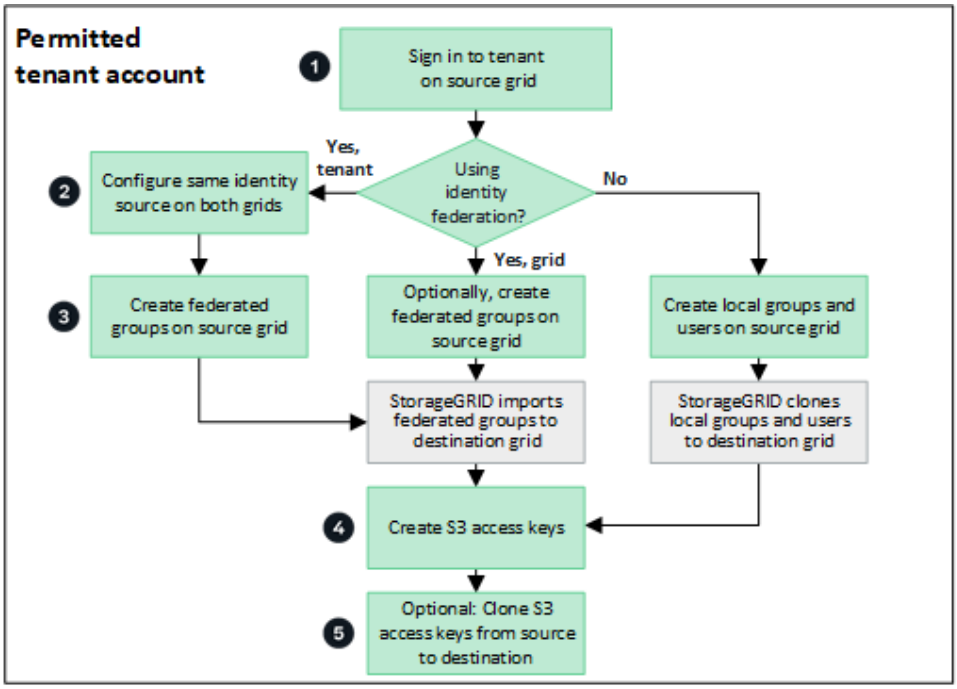
Si se creó o editó un inquilino para utilizar una conexión de federación de grid, ese inquilino se replica desde un sistema StorageGRID (el inquilino de origen) a otro sistema StorageGRID (el inquilino de réplica). Una vez que el inquilino se ha replicado, todos los grupos y usuarios agregados al inquilino de origen se clonan en el inquilino de réplica.

El sistema StorageGRID donde se crea originalmente el inquilino es *source grid* del inquilino. El sistema StorageGRID donde se replica el inquilino es el *grid de destino* del inquilino. Ambas cuentas de inquilino tienen el mismo ID de cuenta, nombre, descripción, cuota de almacenamiento y permisos asignados. pero el inquilino de destino no tiene inicialmente una contraseña de usuario raíz. Para obtener más información, consulte "Qué es el clon de cuenta" y.. "Gestionar inquilinos permitidos".

Se requiere la clonado de la información de la cuenta de inquilino para "replicación entre grid" de objetos de cubo. Tener los mismos grupos de arrendatarios y usuarios en ambas cuadrículas garantiza que pueda acceder a los bloques y objetos correspondientes en cualquiera de las cuadrículas.

Flujo de trabajo de inquilino para el clon de cuenta

Si su cuenta de inquilino tiene el permiso **Use grid federation connection**, revise el diagrama de flujo de trabajo para ver los pasos que realizará para clonar grupos, usuarios y claves de acceso S3.



Estos son los pasos principales del flujo de trabajo:

1 Inicie sesión en el inquilino

Inicie sesión en la cuenta de inquilino en la cuadrícula de origen (la cuadrícula donde se creó inicialmente el inquilino).

2 Opcionalmente, configure la federación de identidades

Si su cuenta de inquilino tiene el permiso **Usar origen de identidad propio** para usar grupos y usuarios federados, configure el mismo origen de identidad (con la misma configuración) tanto para las cuentas de inquilino de origen como de destino. Los grupos y usuarios federados no se pueden clonar a menos que ambas cuadrículas utilicen el mismo origen de identidad. Para ver instrucciones, consulte "Usar la federación de identidades".

3 Crear grupos y usuarios

Al crear grupos y usuarios, comience siempre desde la cuadrícula de origen del inquilino. Cuando se agrega un grupo nuevo, StorageGRID lo clona automáticamente en la cuadrícula de destino.

- Si la federación de identidades está configurada para todo el sistema de StorageGRID o para su cuenta de inquilino, "crear nuevos grupos de arrendatarios" importando grupos federados desde el origen de identidad.
- Si no está utilizando la federación de identidades, "crear nuevos grupos locales" y después "crear usuarios locales".

4 Crear claves de acceso S3

Puede hacerlo "cree sus propias claves de acceso" o hasta "crear claves de acceso de otro usuario" en la

cuadrícula de origen o en la de destino para acceder a los depósitos de dicha cuadrícula.

5 **Opcionalmente, clone las claves de acceso S3**

Si necesita acceder a los depósitos con las mismas claves de acceso en ambas cuadrículas, cree las claves de acceso en la cuadrícula de origen y, a continuación, utilice la API del administrador de inquilinos para clonarlas manualmente en la cuadrícula de destino. Para ver instrucciones, consulte "Clone las claves de acceso S3 mediante la API".

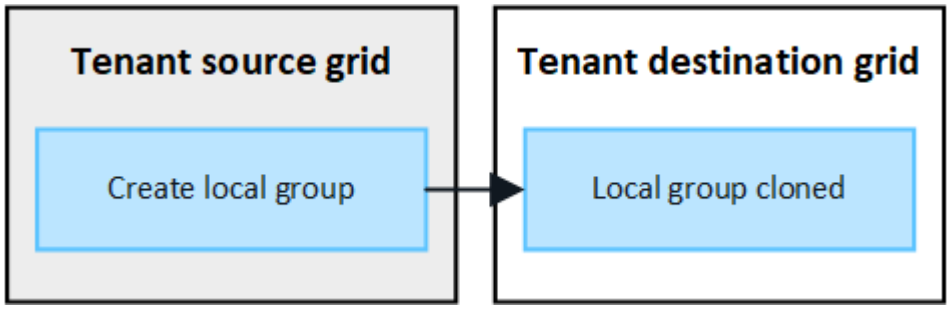
¿Cómo se clonan los grupos, los usuarios y las claves de acceso de S3?

Revise esta sección para entender cómo se clonan los grupos, los usuarios y las claves de acceso S3 entre la cuadrícula de origen de inquilino y el grid de destino de inquilino.

Los grupos locales creados en la cuadrícula de origen se clonan

Después de crear una cuenta de inquilino y replicarla en el grid de destino, StorageGRID clona automáticamente los grupos locales que se agregan a la cuadrícula de origen del inquilino en el grid de destino del inquilino.

Tanto el grupo original como su clon tienen el mismo modo de acceso, permisos de grupo y política de grupos S3. Para ver instrucciones, consulte "Cree grupos para el inquilino de S3".

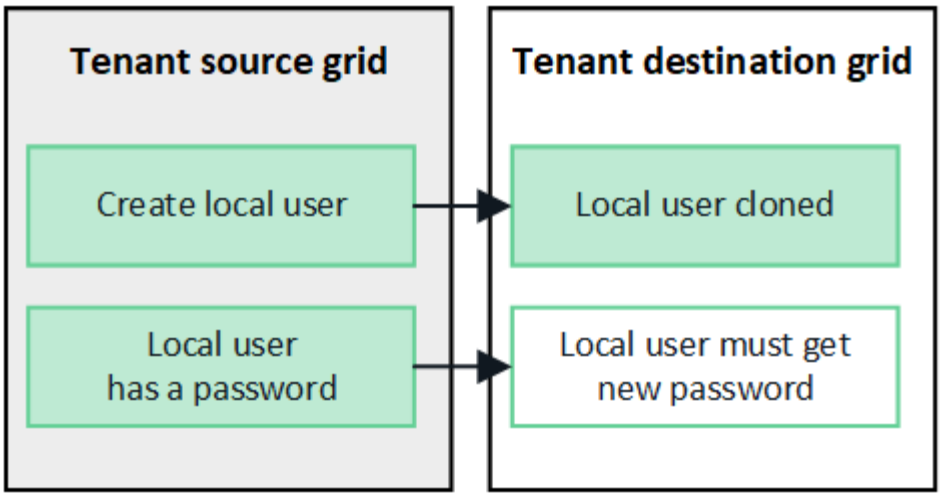


Los usuarios que seleccione al crear un grupo local en la cuadrícula de origen no se incluyen cuando el grupo se clona en la cuadrícula de destino. Por este motivo, no seleccione usuarios al crear el grupo. En su lugar, seleccione el grupo cuando cree los usuarios.

Los usuarios locales creados en la cuadrícula de origen se clonan

Cuando se crea un usuario local nuevo en el grid de origen, StorageGRID clona automáticamente ese usuario en el grid de destino. Tanto el usuario original como su clon tienen la misma configuración de nombre completo, nombre de usuario y **Denegar acceso**. Ambos usuarios también pertenecen a los mismos grupos. Para ver instrucciones, consulte "Gestionar usuarios locales".

Por motivos de seguridad, las contraseñas de usuario local no se clonan en el grid de destino. Si un usuario local necesita acceder a Tenant Manager en la cuadrícula de destino, el usuario raíz de la cuenta de inquilino debe agregar una contraseña para ese usuario en la cuadrícula de destino. Para ver instrucciones, consulte "Gestionar usuarios locales".

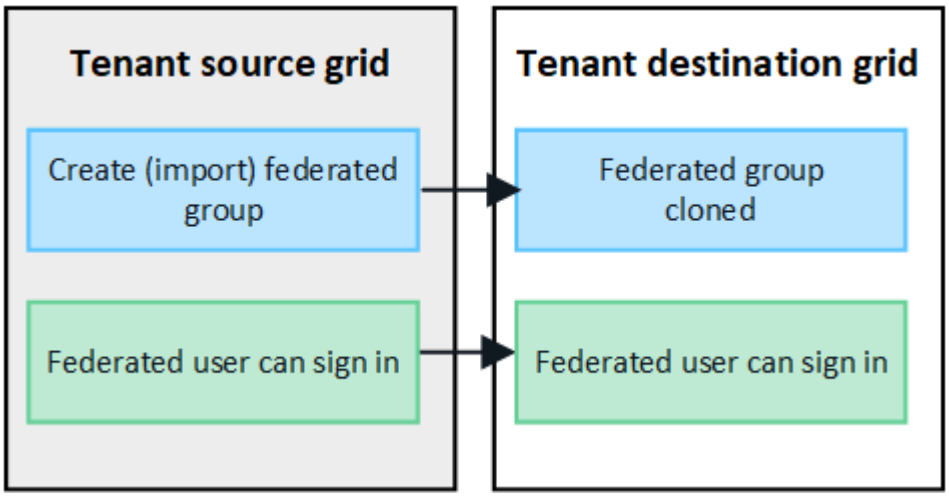


Los grupos federados creados en la cuadrícula de origen se clonan

Suponiendo los requisitos para utilizar el clon de cuenta con "inicio de sesión único" y.. "federación de identidades" se han cumplido, los grupos federados que se crean (se importan) para el inquilino en la cuadrícula de origen se clonan automáticamente en el inquilino en la cuadrícula de destino.

Ambos grupos tienen el mismo modo de acceso, permisos de grupo y política de grupos S3.

Una vez que se crean grupos federados para el inquilino de origen y se clonan en el inquilino de destino, los usuarios federados pueden iniciar sesión en el inquilino en cualquier grid.

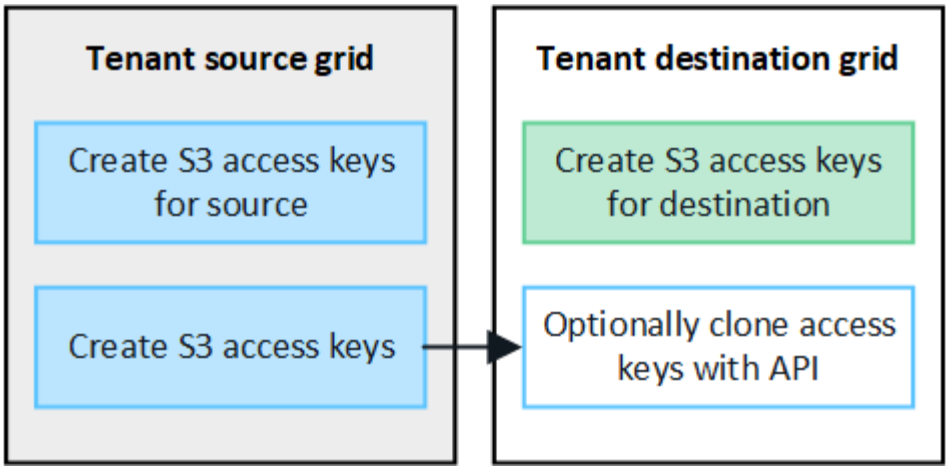


Las claves de acceso S3 se pueden clonar manualmente

StorageGRID no clona automáticamente claves de acceso S3, ya que la seguridad mejora al disponer de diferentes claves en cada grid.

Para gestionar las claves de acceso en las dos cuadrículas, puede realizar una de las siguientes acciones:

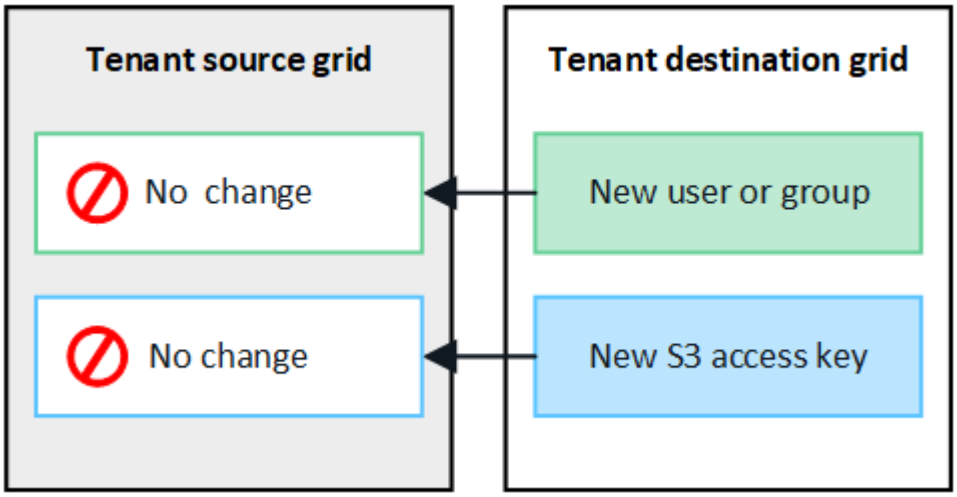
- Si no necesita utilizar las mismas claves para cada cuadrícula, puede hacerlo "cree sus propias claves de acceso" o. "crear claves de acceso de otro usuario" en cada cuadrícula.
- Si necesita utilizar las mismas claves en ambas cuadrículas, puede crear claves en la cuadrícula de origen y, a continuación, utilizar la API del gestor de inquilinos para manualmente "clonar las claves" a la cuadrícula de destino.



Cuando se clonan las claves de acceso S3 para un usuario federado, tanto el usuario como las claves de acceso S3 se clonan en el inquilino de destino.

Los grupos y usuarios que se agregan al grid de destino no se clonan

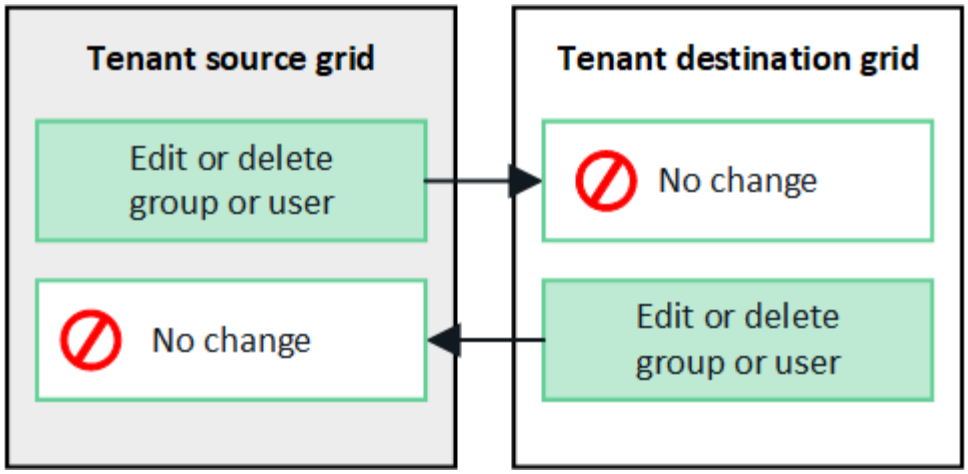
La clonación solo se produce desde la cuadrícula de origen del inquilino al grid de destino del inquilino. Si crea o importa grupos y usuarios en la cuadrícula de destino del inquilino, StorageGRID no clonará estos elementos de vuelta a la cuadrícula de origen del inquilino.



Los grupos, usuarios y claves de acceso editados o eliminados no se clonan

La clonación solo se produce cuando se crean nuevos grupos y usuarios.

Si edita o elimina grupos, usuarios o claves de acceso en cualquiera de las cuadrículas, los cambios no se clonarán en la otra cuadrícula.



Clone las claves de acceso S3 mediante la API

Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, puede usar la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la cuadrícula de origen al inquilino en la cuadrícula de destino.

Antes de empezar

- La cuenta de inquilino tiene el permiso **Use grid federation connection**.
- La conexión de federación de red tiene un **estado de conexión** de **Conectado**.
- Ha iniciado sesión en el gestor de inquilinos en la cuadrícula de origen del inquilino mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Administre sus propias credenciales de S3 o permiso de acceso raíz".
- Si clona claves de acceso para un usuario local, el usuario ya existe en ambas cuadrículas.

> Cuando se clonan las claves de acceso S3 para un usuario federado, se agregan al inquilino de destino las claves de acceso S3 y el usuario.

Clone sus propias claves de acceso

Puede clonar sus propias claves de acceso si necesita acceder a los mismos depósitos en ambas cuadrículas.

Pasos

1. Mediante el administrador de inquilinos en la cuadrícula de origen, "cree sus propias claves de acceso" y descargue el `.csv` archivo.
2. En la parte superior del Administrador de inquilinos, selecciona el icono de ayuda y selecciona **Documentación de API**.
3. En la sección **S3**, seleccione el siguiente punto final:

   `POST /org/users/current-user/replicate-s3-access-key`

4. Seleccione **probar**.

5. En el cuadro de texto **body**, reemplace las entradas de ejemplo de **accessKey** y **secretAccessKey** con los valores del archivo **.csv** que descargó.

   Asegúrese de conservar las comillas dobles alrededor de cada cadena.

6. Si la clave caduca, reemplace la entrada de ejemplo para **Expires** con la fecha y hora de vencimiento como una cadena en formato de datos-tiempo ISO 8601 (por ejemplo, `2024-02-28T22:46:33-08:00`). Si la clave no caduca, introduzca **null** como valor para la entrada **Expires** (o elimine la línea **Expires** y la coma anterior).
7. Seleccione **Ejecutar**.
8. Confirme que el código de respuesta del servidor es **204**, lo que indica que la clave se clonó correctamente en la cuadrícula de destino.

Clonar las claves de acceso de otro usuario

Puede clonar las claves de acceso de otro usuario si necesita acceder a los mismos depósitos en ambas cuadrículas.

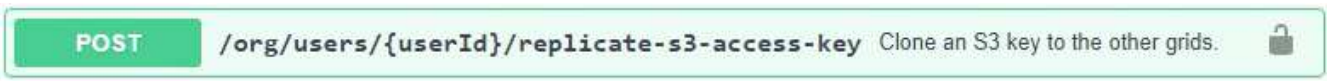
Pasos

1. Mediante el administrador de inquilinos en la cuadrícula de origen, "Cree las claves de acceso S3 del otro usuario" y descargue el `.csv` archivo.
2. En la parte superior del Administrador de inquilinos, selecciona el icono de ayuda y selecciona **Documentación de API**.
3. Obtenga el ID de usuario. Necesitará este valor para clonar las claves de acceso del otro usuario.
   a. En la sección **users**, selecciona el siguiente punto final:

      `GET /org/users`

   b. Seleccione **probar**.
   c. Especifique los parámetros que desee utilizar al buscar usuarios.
   d. Seleccione **Ejecutar**.
   e. Busque el usuario cuyas claves desea clonar y copie el número en el campo **id**.
4. En la sección **S3**, seleccione el siguiente punto final:

   `POST /org/users/{userId}/replicate-s3-access-key`



5. Seleccione **probar**.

6. En el cuadro de texto **UserId**, pega el ID de usuario que copiaste.
7. En el cuadro de texto **body**, reemplace las entradas de ejemplo de **example access key** y **secret access key** con los valores del archivo **.csv** para ese usuario.

   Asegúrese de conservar las comillas dobles alrededor de la cadena.

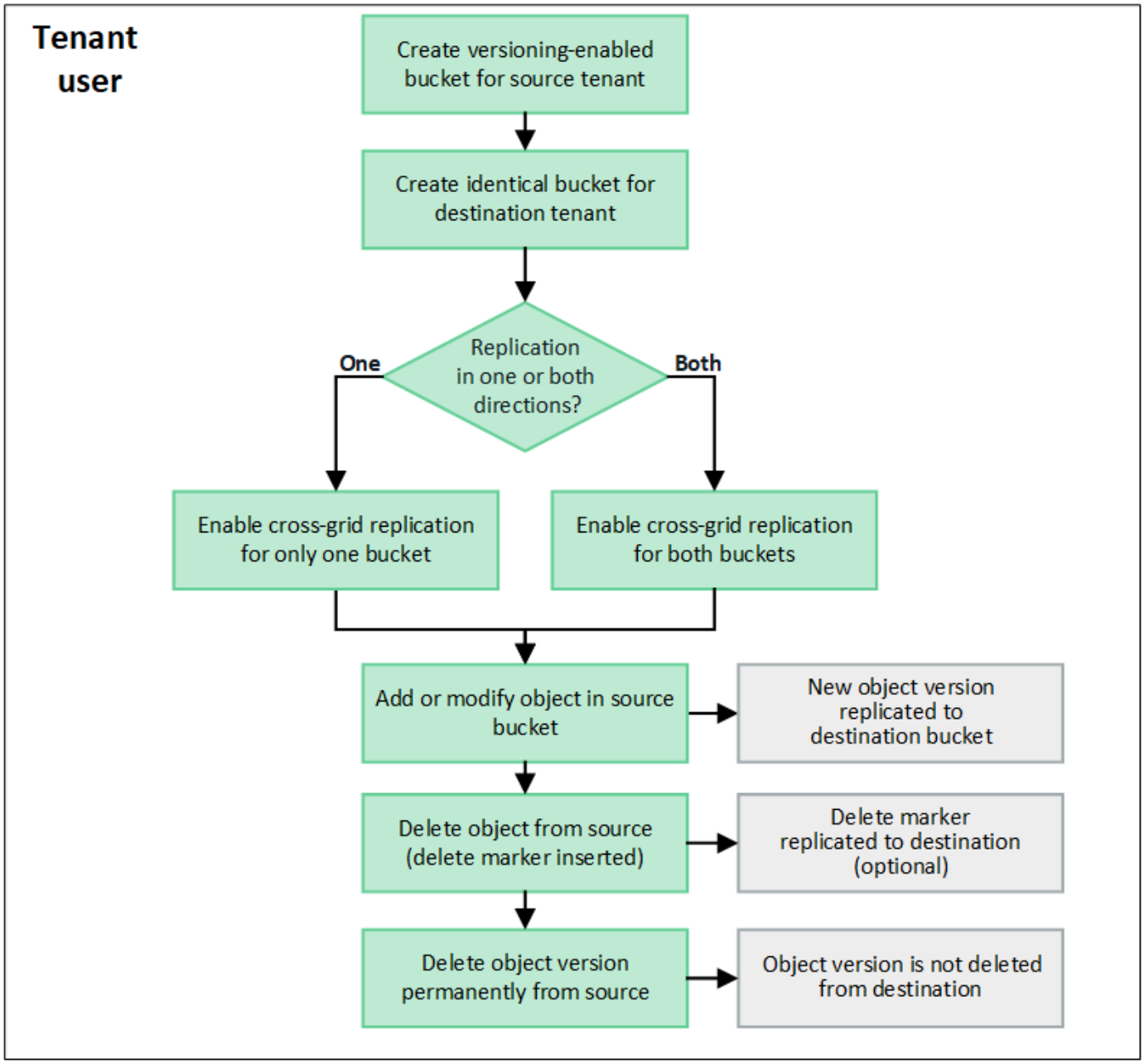
8. Si la clave caduca, reemplace la entrada de ejemplo para **Expires** con la fecha y hora de vencimiento como una cadena en formato de datos-tiempo ISO 8601 (por ejemplo, `2023-02-28T22:46:33-08:00`). Si la clave no caduca, introduzca **null** como valor para la entrada **Expires** (o elimine la línea **Expires** y la coma anterior).
9. Seleccione **Ejecutar**.
10. Confirme que el código de respuesta del servidor es **204**, lo que indica que la clave se clonó correctamente en la cuadrícula de destino.

Gestionar la replicación entre grid

Si a su cuenta de inquilino se le asignó el permiso **Usar conexión de federación de grid** cuando se creó, puede utilizar la replicación entre grid para replicar automáticamente objetos entre buckets en la cuadrícula de origen del inquilino y depósitos en la cuadrícula de destino del inquilino. La replicación entre grid puede producirse en una o en ambas direcciones.

Flujo de trabajo de replicación entre grid

El diagrama de flujo de trabajo resume los pasos que realizará para configurar la replicación entre bloques en dos cuadrículas. Estos pasos se describen con más detalle a continuación.



Configurar la replicación entre grid

Para poder utilizar la replicación entre grid, debe iniciar sesión en las cuentas de tenant correspondientes en cada grid y crear buckets idénticos. A continuación, puede activar la replicación entre grid en cualquiera de los dos bloques o en ambos.

Antes de empezar

- Ha revisado los requisitos para la replicación entre grid. Consulte "Qué es la replicación entre grid".
- Está utilizando un "navegador web compatible".
- La cuenta de inquilino tiene el permiso **Use grid federation connection** y existen cuentas de inquilino idénticas en ambas cuadrículas. Consulte "Gestione los inquilinos permitidos para la conexión de federación de grid".
- El usuario de inquilino al que se conectará como ya existe en ambas cuadrículas y pertenece a un grupo de usuarios que tiene "Permiso de acceso raíz".

- Si va a iniciar sesión en la cuadrícula de destino del inquilino como un usuario local, el usuario raíz de la cuenta de inquilino ha establecido una contraseña para su cuenta de usuario en ese grid.

Cree dos cubos idénticos

Como primer paso, inicie sesión en las cuentas de arrendatario correspondientes en cada cuadrícula y cree cubos idénticos.

Pasos

1. A partir de cualquier cuadrícula de la conexión de federación de grid, cree un nuevo bucket:
   a. Inicie sesión en la cuenta de inquilino con las credenciales de un usuario de inquilino que existe en ambas cuadrículas.

      Si no puede iniciar sesión en la cuadrícula de destino del inquilino como usuario local, confirme que el usuario raíz de la cuenta de inquilino ha establecido una contraseña para su cuenta de usuario.

   b. Siga las instrucciones a. "Cree un bucket de S3".
   c. En la pestaña **Administrar configuración de objetos**, selecciona **Activar control de versiones de objetos**.
   d. Si el bloqueo de objetos S3 está activado para el sistema StorageGRID, no habilite el bloqueo de objetos S3 para el depósito.
   e. Seleccione **Crear cucharón**.
   f. Seleccione **Finalizar**.
2. Repita estos pasos para crear un depósito idéntico para la misma cuenta de inquilino en el otro grid de la conexión de federación de grid.

   Según sea necesario, cada cubo puede utilizar una región diferente.

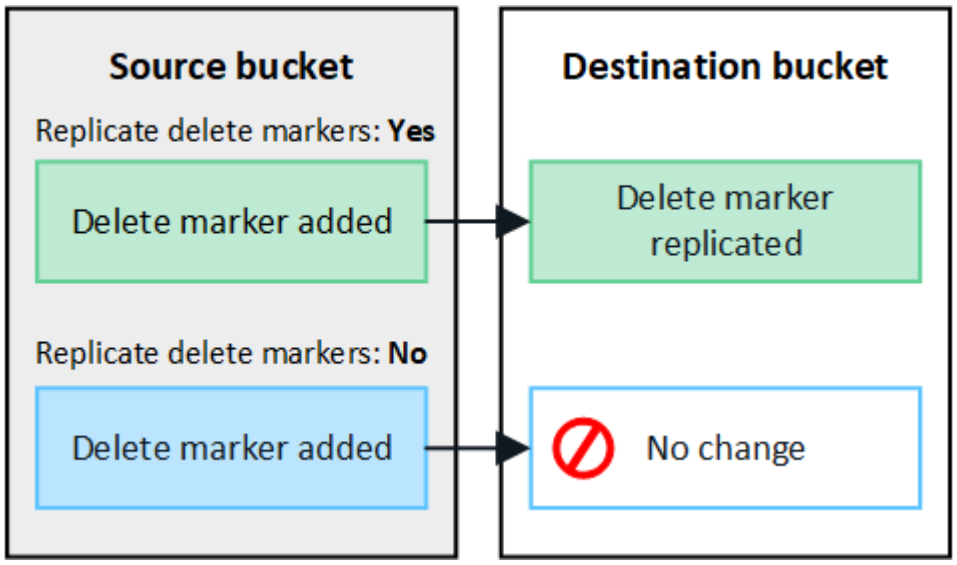
Habilite la replicación entre grid

Debe realizar estos pasos antes de agregar cualquier objeto a cada bloque.

Pasos

1. A partir de una cuadrícula cuyos objetos desea replicar, active "replicación entre grid en una dirección":
   a. Inicie sesión en la cuenta de inquilino del bloque.
   b. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
   c. Seleccione el nombre del cubo de la tabla para acceder a la página de detalles del cubo.
   d. Seleccione la pestaña **Replicación de cuadrícula**.
   e. Seleccione **Activar** y revise la lista de requisitos.
   f. Si se han cumplido todos los requisitos, seleccione la conexión de federación de grid que desea utilizar.
   g. Opcionalmente, cambie la configuración de **replicar marcadores de eliminación** para determinar qué sucede en la cuadrícula de destino si un cliente S3 emite una solicitud de eliminación a la cuadrícula de origen que no incluye un ID de versión:

- **Sí** (por defecto): Se agrega un marcador de borrado al depósito de origen y se replica en el cubo de destino.
- **No**: Se agrega un marcador de borrado al cubo de origen pero no se replica en el cubo de destino.



> Si la solicitud de eliminación incluye un ID de versión, esa versión de objeto se elimina permanentemente del depósito de origen. StorageGRID no replica las solicitudes de eliminación que incluyen un identificador de versión, por lo que la misma versión de objeto no se elimina del destino.

Consulte "Qué es la replicación entre grid" para obtener más detalles.

a. Opcionalmente, cambie la configuración de la categoría de auditoría **Replicación de cuadrícula** para administrar el volumen de los mensajes de auditoría:
   - **Error** (por defecto): Solo se incluyen solicitudes fallidas de replicación entre redes en la salida de la auditoría.
   - **Normal**: Se incluyen todas las solicitudes de replicación entre redes, lo que aumenta significativamente el volumen de la salida de auditoría.
b. Revise las selecciones. No puede cambiar esta configuración a menos que ambos cubos estén vacíos.
c. Seleccione **Habilitar y probar**.

   Después de unos momentos, aparece un mensaje de éxito. Los objetos agregados a este depósito ahora se replicarán automáticamente en la otra cuadrícula. **La replicación de cuadrícula cruzada** se muestra como una característica habilitada en la página de detalles del cubo.

2. Opcionalmente, vaya al cucharón correspondiente en la otra cuadrícula y. "permita la replicación entre grid en ambas direcciones".

Probar la replicación entre grids

Si se habilita la replicación entre grid para un bloque, es posible que deba comprobar que la conexión y la replicación entre grid funcionan correctamente y que los buckets de origen y de destino siguen cumpliendo todos los requisitos (por ejemplo, las versiones siguen activadas).

Antes de empezar

- Está utilizando un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".

Pasos

1. Inicie sesión en la cuenta de inquilino del bloque.
2. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
3. Seleccione el nombre del cubo de la tabla para acceder a la página de detalles del cubo.
4. Seleccione la pestaña **Replicación de cuadrícula**.
5. Seleccione **probar conexión**.

   Si la conexión es correcta, aparece el banner Correcta. De lo contrario, se muestra un mensaje de error que usted y el administrador de grid pueden utilizar para resolver el problema. Para obtener más información, consulte "Solucionar errores de federación de grid".

6. Si la replicación entre redes está configurada para que ocurra en ambas direcciones, vaya al depósito correspondiente en la otra cuadrícula y seleccione **Probar conexión** para verificar que la replicación entre redes funcione en la otra dirección.

Desactive la replicación entre grid

Puede detener de forma permanente la replicación entre grid si ya no desea copiar objetos en la otra grid.

Antes de deshabilitar la replicación entre grid, tenga en cuenta lo siguiente:

- Al desactivar la replicación entre grid no se elimina ningún objeto que ya se haya copiado entre grid. Por ejemplo, los objetos de `my-bucket` En la cuadrícula 1 en la que se ha copiado `my-bucket` En Grid 2 no se eliminan si deshabilita la replicación entre grid para ese bloque. Si desea eliminar estos objetos, debe eliminarlos manualmente.
- Si se activó la replicación entre grid para cada uno de los buckets (es decir, si la replicación se produce en ambas direcciones), puede deshabilitar la replicación entre grid para uno o ambos buckets. Por ejemplo, puede que desee desactivar la replicación de objetos de `my-bucket` En la cuadrícula 1 a. `my-bucket` En Grid 2, mientras continúa replicando objetos desde `my-bucket` En la cuadrícula 2 a. `my-bucket` En la cuadrícula 1.
- Debe deshabilitar la replicación entre grid para poder quitar el permiso de un inquilino para utilizar la conexión de federación de grid. Consulte "Gestionar inquilinos permitidos".
- Si deshabilita la replicación entre grid para un bucket que contiene objetos, no podrá volver a habilitar la replicación entre grid a menos que elimine todos los objetos de los buckets de origen y de destino.

> ⚠ No puede volver a activar la replicación a menos que ambos buckets estén vacíos.

Antes de empezar

- Está utilizando un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".

Pasos

1. A partir de la cuadrícula cuyos objetos ya no desea replicar, detenga la replicación entre grid del bloque:
   a. Inicie sesión en la cuenta de inquilino del bloque.
   b. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.

c. Seleccione el nombre del cubo de la tabla para acceder a la página de detalles del cubo.

d. Seleccione la pestaña **Replicación de cuadrícula**.

e. Seleccione **Desactivar replicación**.

f. Si está seguro de que desea deshabilitar la replicación entre redes para este depósito, escriba **Sí** en el cuadro de texto y seleccione **Desactivar**.

   Después de unos momentos, aparece un mensaje de éxito. Los nuevos objetos agregados a este depósito ya no se pueden replicar automáticamente en el otro grid. **La replicación entre redes** ya no se muestra como una característica habilitada en la página Buckets.

2. Si la replicación entre grid se configuró para que se produzca en ambas direcciones, vaya al bucket correspondiente en la otra grid y detenga la replicación entre grid en la otra dirección.

Ver conexiones de federación de grid

Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, puede ver las conexiones permitidas.

Antes de empezar

- La cuenta de inquilino tiene el permiso **Use grid federation connection**.
- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".

Pasos

1. Selecciona **STORAGE (S3)** > **Grid federation connections**.

   Aparece la página de conexión de Grid federation e incluye una tabla que resume la siguiente información:

Columna	Descripción
Nombre de conexión	Las conexiones de federación de grid que este inquilino tiene permiso para utilizar.
Buckets con replicación entre grid	Para cada conexión de federación de grid, los buckets de inquilinos que tienen habilitada la replicación entre grid. Los objetos agregados a estos cubos se replicarán en la otra cuadrícula de la conexión.
Último error	Para cada conexión de federación de grid, se produce el error más reciente, si lo hay, cuando los datos se están replicando en la otra cuadrícula. Consulte Borre el último error.

2. Si lo desea, seleccione un nombre de cubo a. "ver detalles del período".

Borrar el último error

Un error puede aparecer en la columna **last error** por uno de estos motivos:

- No se ha encontrado la versión del objeto de origen.
- No se ha encontrado el depósito de origen.

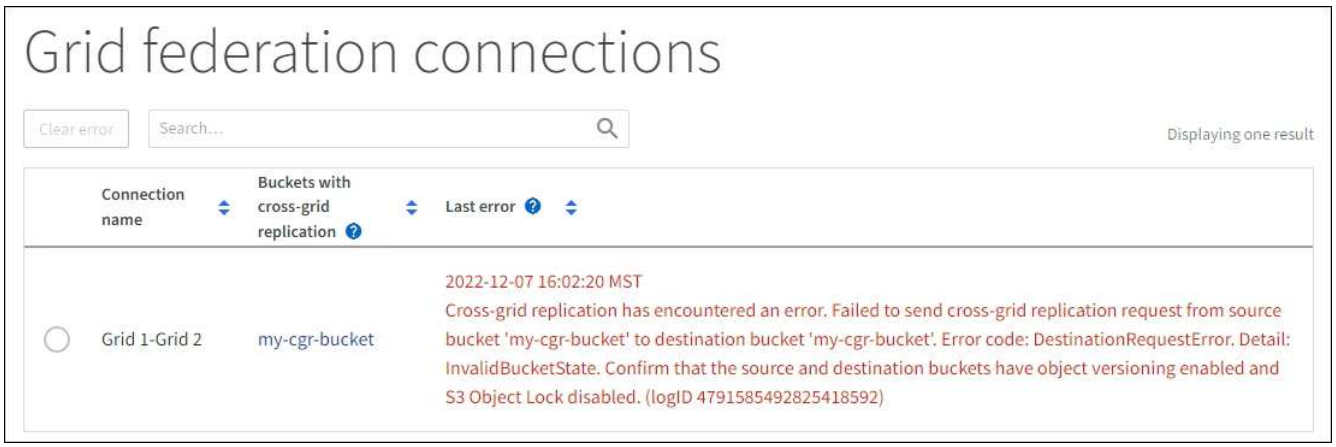
- Se ha suprimido el depósito de destino.
- Una cuenta diferente ha vuelto a crear el bloque de destino.
- Se ha suspendido el control de versiones del bloque de destino.
- La misma cuenta ha vuelto a crear el depósito de destino, pero ahora no tiene versiones.

> Esta columna solo muestra el último error de replicación entre cuadrículas que se produce; no se mostrarán los errores anteriores que podrían haberse producido.

Pasos

1. Si aparece un mensaje en la columna **Último error**, vea el texto del mensaje.

   Por ejemplo, este error indica que el depósito de destino para la replicación entre grid estaba en un estado no válido, posiblemente porque el control de versiones estaba suspendido o porque se activó el bloqueo de objetos S3.



2. Realice las acciones recomendadas. Por ejemplo, si se suspendió el control de versiones en el bloque de destino para la replicación entre grid, vuelva a habilitar el control de versiones para ese bloque.
3. Seleccione la conexión de la tabla.
4. Seleccione **Borrar error**.
5. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
6. Espere 5-6 minutos e incorpore un objeto nuevo en el bloque. Confirme que el mensaje de error no vuelve a aparecer.

   > Para asegurarse de que el mensaje de error se borra, espere al menos 5 minutos después de la marca de tiempo del mensaje antes de introducir un nuevo objeto.

7. Para determinar si se ha producido un error en la replicación de algún objeto debido al error de depósito, consulte "Identifique y vuelva a intentar operaciones de replicación fallidas".

Gestionar grupos y usuarios

Usar la federación de identidades

El uso de la federación de identidades agiliza la configuración de usuarios y grupos de inquilinos, y permite a los usuarios de inquilinos iniciar sesión en la cuenta de inquilinos

utilizando credenciales conocidas.

Configurar la federación de identidades para el Administrador de inquilinos

Puede configurar la federación de identidades para el administrador de inquilinos si desea que los grupos de inquilinos y los usuarios se gestionen en otro sistema como Active Directory, Azure Active Directory (Azure AD), OpenLDAP u Oracle Directory Server.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Se utiliza Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidades.

> Si desea utilizar un servicio LDAP v3 que no esté en la lista, póngase en contacto con el soporte técnico.

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Consulte Instrucciones para configurar el servidor OpenLDAP.
- Si planea utilizar la seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidades debe usar TLS 1.2 o 1.3. Consulte "Cifrados compatibles para conexiones TLS salientes".

Acerca de esta tarea

Si puede configurar un servicio de federación de identidades para su inquilino depende de cómo se haya configurado su cuenta de inquilino. Es posible que el inquilino comparta el servicio de federación de identidades configurado para Grid Manager. Si ve este mensaje cuando accede a la página Identity Federation, no puede configurar un origen de identidad federado independiente para este arrendatario.

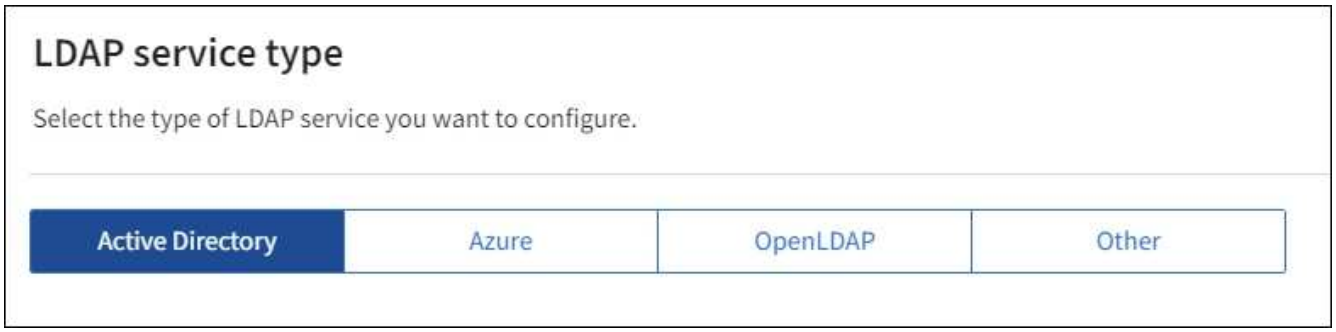
> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

Introducir configuración

Al configurar Identify federation, proporciona los valores que StorageGRID necesita para conectarse a un servicio LDAP.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **federación de identidades**.
2. Seleccione **Activar federación de identidades**.
3. En la sección Tipo de servicio LDAP, seleccione el tipo de servicio LDAP que desea configurar.



Seleccione **otros** para configurar valores para un servidor LDAP que utilice Oracle Directory Server.

4. Si ha seleccionado **otros**, complete los campos de la sección atributos LDAP . De lo contrario, vaya al paso siguiente.
   - **Nombre único de usuario**: Nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo es equivalente a. `sAMAccountName` Para Active Directory y. `uid` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `uid`.
   - **UUID de usuario**: Nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a. `objectGUID` Para Active Directory y. `entryUUID` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `nsuniqueid`. El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
   - **Nombre único del grupo**: Nombre del atributo que contiene el identificador único de un grupo LDAP. Este atributo es equivalente a. `sAMAccountName` Para Active Directory y. `cn` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `cn`.
   - **UUID de grupo**: Nombre del atributo que contiene el identificador único permanente de un grupo LDAP. Este atributo es equivalente a. `objectGUID` Para Active Directory y. `entryUUID` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `nsuniqueid`. El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
5. Para todos los tipos de servicio LDAP, introduzca la información de servidor LDAP y conexión de red necesaria en la sección Configure LDAP Server.
   - **Hostname**: El nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP.
   - **Puerto**: El puerto utilizado para conectarse al servidor LDAP.

     El puerto predeterminado para STARTTLS es 389 y el puerto predeterminado para LDAPS es 636. Sin embargo, puede utilizar cualquier puerto siempre que su firewall esté configurado correctamente.

   - **Nombre de usuario**: La ruta completa del nombre completo (DN) para el usuario que se conectará al servidor LDAP.

     Para Active Directory, también puede especificar el nombre de inicio de sesión de nivel inferior o el nombre principal del usuario.

     El usuario especificado debe tener permiso para enumerar grupos y usuarios y para tener acceso a los siguientes atributos:

     - `sAMAccountName` o. `uid`

- `objectGUID`, `entryUUID`, o. `nsuniqueid`
- `cn`
- `memberOf` o. `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, y. `userPrincipalName`
- **Azure**: `accountEnabled` y.. `userPrincipalName`

◦ **Contraseña**: La contraseña asociada al nombre de usuario.

> Si cambia la contraseña en el futuro, debe actualizarla en esta página.

◦ **DN base de grupo**: La ruta completa del nombre distinguido (DN) para un subárbol LDAP que desea buscar grupos. En el ejemplo de Active Directory (a continuación), se pueden usar como grupos federados todos los grupos cuyo nombre distintivo sea relativo al DN base (DC=storagegrid,DC=example,DC=com).

> Los valores de **Nombre único de grupo** deben ser únicos dentro del **DN base de grupo** al que pertenecen.

◦ **DN base de usuario**: La ruta completa del nombre completo (DN) de un subárbol LDAP que desea buscar usuarios.

> Los valores de **Nombre único de usuario** deben ser únicos dentro del **DN base de usuario** al que pertenecen.

◦ **Formato de nombre de usuario de enlace** (opcional): El patrón de nombre de usuario predeterminado StorageGRID debe usarse si el patrón no se puede determinar automáticamente.

Se recomienda proporcionar **Formato de nombre de usuario Bind** porque puede permitir que los usuarios inicien sesión si StorageGRID no puede enlazar con la cuenta de servicio.

Introduzca uno de estos patrones:

- **Patrón UserPrincipalName (Active Directory y Azure)**: `[USERNAME]@*example*.com`
- **Patrón de nombre de inicio de sesión de nivel inferior (Active Directory y Azure)**: `*example*\[USERNAME]`
- **Patrón de nombre completo**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Incluya **[USERNAME]** exactamente como está escrito.

6. En la sección Seguridad de la capa de transporte (TLS), seleccione una configuración de seguridad.
   ◦ **Use STARTTLS**: Utilice STARTTLS para asegurar las comunicaciones con el servidor LDAP. Esta es la opción recomendada para Active Directory, OpenLDAP u otros, pero esta opción no es compatible con Azure.
   ◦ **Use LDAPS**: La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debe seleccionar esta opción para Azure.
   ◦ **No utilice TLS**: El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Azure.

El uso de la opción **no usar TLS** no es compatible si el servidor de Active Directory aplica la firma LDAP. Debe usar STARTTLS o LDAPS.

7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.
   - **Utilizar certificado CA del sistema operativo**: Utilice el certificado predeterminado de CA de red instalado en el sistema operativo para asegurar las conexiones.
   - **Utilizar certificado de CA personalizado**: Utilice un certificado de seguridad personalizado.

     Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto del certificado de CA.

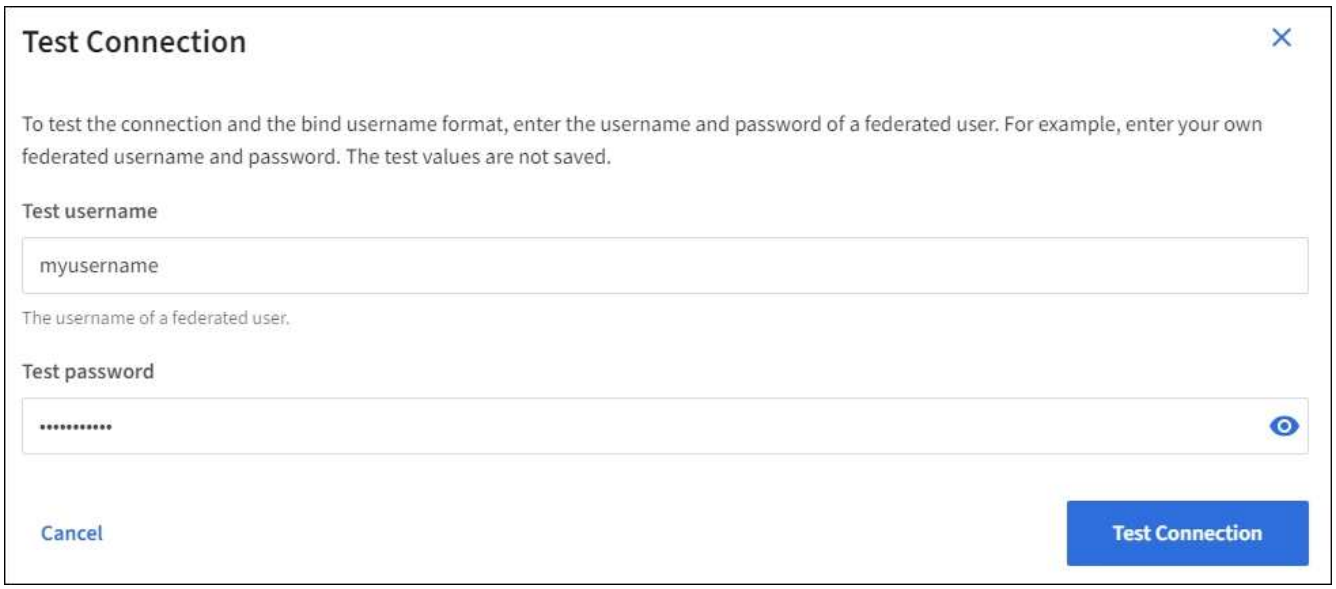
Pruebe la conexión y guarde la configuración

Después de introducir todos los valores, es necesario probar la conexión para poder guardar la configuración. StorageGRID verifica la configuración de conexión del servidor LDAP y el formato de nombre de usuario de enlace, si proporcionó uno.

Pasos

1. Seleccione **probar conexión**.
2. Si no se proporciona un formato de nombre de usuario de enlace:
   - Si la configuración de conexión es válida, aparecerá un mensaje que indica que la conexión se ha realizado correctamente. Seleccione **Guardar** para guardar la configuración.
   - Si la configuración de conexión no es válida, aparecerá un mensaje que indica que no se ha podido establecer la conexión de prueba. Seleccione **Cerrar**. Luego, resuelva cualquier problema y vuelva a probar la conexión.
3. Si proporcionó un formato de nombre de usuario de enlace, introduzca el nombre de usuario y la contraseña de un usuario federado válido.

   Por ejemplo, introduzca su propio nombre de usuario y contraseña. No incluya ningún carácter especial en el nombre de usuario, como @ o /.



   - Si la configuración de conexión es válida, aparecerá un mensaje que indica que la conexión se ha realizado correctamente. Seleccione **Guardar** para guardar la configuración.

- Aparecerá un mensaje de error si las opciones de conexión, el formato de nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva los problemas y vuelva a probar la conexión.

Forzar la sincronización con el origen de identidades

El sistema StorageGRID sincroniza periódicamente grupos federados y usuarios del origen de identidades. Puede forzar el inicio de la sincronización si desea habilitar o restringir los permisos de usuario lo antes posible.

Pasos

1. Vaya a la página federación de identidades.
2. Seleccione **servidor de sincronización** en la parte superior de la página.

   El proceso de sincronización puede tardar bastante tiempo en función del entorno.

   > La alerta **fallo de sincronización de la federación de identidades** se activa si hay un problema al sincronizar grupos federados y usuarios del origen de identidades.

Deshabilitar la federación de identidades

Puede deshabilitar temporalmente o de forma permanente la federación de identidades para grupos y usuarios. Cuando la federación de identidades está deshabilitada, no existe comunicación entre StorageGRID y el origen de identidades. Sin embargo, cualquier configuración que haya configurado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidades en el futuro.

Acerca de esta tarea

Antes de deshabilitar la federación de identidades, debe tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que hayan iniciado sesión en ese momento, retendrán el acceso al sistema StorageGRID hasta que caduque la sesión, pero no podrán iniciar sesión después de que caduque la sesión.
- No se realizará la sincronización entre el sistema StorageGRID y el origen de identidad, y no se realizarán alertas ni alarmas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Habilitar federación de identidad** está desactivada si el inicio de sesión único (SSO) está configurado en **enabled** o **Sandbox Mode**. El estado de SSO de la página Single Sign-On debe ser **Desactivado** antes de poder deshabilitar la federación de identidades. Consulte "Desactive el inicio de sesión único".

Pasos

1. Vaya a la página federación de identidades.
2. Desmarque la casilla de verificación **Habilitar federación de identidad**.

Instrucciones para configurar el servidor OpenLDAP

Si desea utilizar un servidor OpenLDAP para la federación de identidades, debe configurar ajustes específicos en el servidor OpenLDAP.

En el caso de fuentes de identidad que no sean ActiveDirectory ni Azure, StorageGRID no bloqueará automáticamente el acceso S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine cualquier clave S3 para el usuario o elimine al usuario de todos los grupos.

Revestimientos memberOf y reft

Se deben habilitar las superposiciones memberof y reft. Para obtener más información, consulte las instrucciones para el mantenimiento de miembros del grupo inverso en "Documentación de OpenLDAP: Guía del administrador de la versión 2.4".

Indización

Debe configurar los siguientes atributos OpenLDAP con las palabras clave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Además, asegúrese de que los campos mencionados en la ayuda para Nombre de usuario estén indexados para un rendimiento óptimo.

Consulte la información sobre el mantenimiento de pertenencia a grupos inversa en la "Documentación de OpenLDAP: Guía del administrador de la versión 2.4".

Gestionar grupos de inquilinos

Cree grupos para un inquilino de S3

Es posible gestionar permisos para grupos de usuarios S3 importando grupos federados o creando grupos locales.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Si planea importar un grupo federado, tiene "federación de identidades configurada", y el grupo federado ya existe en el origen de identidad configurado.
- Si su cuenta de inquilino tiene el permiso **Use grid federation connection**, ha revisado el flujo de trabajo y las consideraciones para "clonación de usuarios y grupos de inquilinos", y ha iniciado sesión en la cuadrícula de origen del inquilino.

Acceda al asistente Crear grupo

Como primer paso, acceda al asistente de creación de grupos.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, confirme que aparece un

banner azul, indicando que los nuevos grupos creados en esta cuadrícula se clonarán en el mismo inquilino en la otra cuadrícula de la conexión. Si este banner no aparece, puede que haya iniciado sesión en la cuadrícula de destino del inquilino.

3. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

Pasos

1. Seleccione la ficha **Grupo local** para crear un grupo local o seleccione la ficha **Grupo federado** para importar un grupo desde el origen de identidad configurado previamente.

   Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan utilizar las aplicaciones cliente para gestionar los recursos del inquilino, en función de los permisos de grupo.

2. Introduzca el nombre del grupo.
   - **Grupo local**: Introduzca tanto un nombre para mostrar como un nombre exclusivo. Puede editar el nombre para mostrar más adelante.

     Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, se producirá un error de clonación si el mismo **nombre único** ya existe para el inquilino en la cuadrícula de destino.

   - **Grupo federado**: Introduzca el nombre único. Para Active Directory, el nombre único es el nombre asociado con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `uid` atributo.
3. Seleccione **continuar**.

Administrar permisos de grupo

Los permisos de grupo controlan las tareas que los usuarios pueden realizar en el gestor de inquilinos y en la API de gestión de inquilinos.

Pasos

1. Para **Modo de acceso**, seleccione una de las siguientes opciones:
   - **Read-write** (por defecto): Los usuarios pueden iniciar sesión en Tenant Manager y administrar la configuración del inquilino.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden hacer ningún cambio ni realizar ninguna operación en el administrador de inquilinos o la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

   > Si un usuario pertenece a varios grupos y cualquier grupo está establecido en sólo lectura, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

2. Seleccione uno o más permisos para este grupo.

   Consulte "Permisos de gestión de inquilinos".

3. Seleccione **continuar**.

Establezca la política de grupo S3

La política de grupo determina qué permisos de acceso S3 tendrán los usuarios.

Pasos

1. Seleccione la política que desea usar para este grupo.

Política de grupo	Descripción
Sin acceso S3	Predeterminado. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que el acceso se conceda con una política de bloque. Si selecciona esta opción, de forma predeterminada, solo el usuario raíz tendrá acceso a recursos de S3.
Acceso de sólo lectura	Los usuarios de este grupo tienen acceso de solo lectura a los recursos de S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puede editar esta cadena.
Acceso total	Los usuarios de este grupo tienen acceso completo a recursos de S3, incluidos los bloques. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puede editar esta cadena.

Política de grupo	Descripción
Mitigación del ransomware	Esta política de ejemplo se aplica a todos los depósitos de este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden suprimir de forma permanente objetos de los bloques que tienen activado el control de versiones de objetos. Los usuarios del administrador de inquilinos que tienen el permiso **Administrar todos los cubos** pueden anular esta política de grupo. Limite el permiso Gestionar todos los buckets a usuarios de confianza y use la autenticación multifactor (MFA) cuando esté disponible.
Personalizado	A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto.

2. Si ha seleccionado **personalizado**, introduzca la directiva de grupo. Cada política de grupo tiene un límite de tamaño de 5,120 bytes. Debe introducir una cadena con formato JSON válida.

   Para obtener información detallada sobre las políticas de grupo, incluida la sintaxis del idioma y los ejemplos, consulte "Ejemplo de políticas de grupo".

3. Si está creando un grupo local, seleccione **continuar**. Si está creando un grupo federado, seleccione **Crear grupo** y **Finalizar**.

Añadir usuarios (sólo grupos locales)

Puede guardar el grupo sin agregar usuarios o, opcionalmente, puede agregar cualquier usuario local que ya exista.

> Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, los usuarios que seleccione al crear un grupo local en la cuadrícula de origen no se incluyen cuando el grupo se clona en la cuadrícula de destino. Por este motivo, no seleccione usuarios al crear el grupo. En su lugar, seleccione el grupo cuando cree los usuarios.

Pasos

1. Opcionalmente, seleccione uno o varios usuarios locales para este grupo.
2. Seleccione **Crear grupo** y **Finalizar**.

   El grupo creado aparece en la lista de grupos.

   Si su cuenta de inquilino tiene el permiso **Use grid federation connection** y usted está en la cuadrícula de origen del inquilino, el nuevo grupo se clona en la cuadrícula de destino del inquilino. **Success** aparece como **Cloning status** en la sección Overview de la página de detalles del grupo.

Cree grupos para un inquilino de Swift

Es posible gestionar los permisos de acceso para una cuenta de inquilino de Swift mediante la importación de grupos federados o la creación de grupos locales. Al menos un grupo debe tener el permiso de administrador de Swift, que se requiere para gestionar los contenedores y los objetos de una cuenta de inquilino de Swift.

Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Si planea importar un grupo federado, tiene "federación de identidades configurada", y el grupo federado ya existe en el origen de identidad configurado.

Acceda al asistente Crear grupo

Pasos

Como primer paso, acceda al asistente de creación de grupos.

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

Pasos

1. Seleccione la ficha **Grupo local** para crear un grupo local o seleccione la ficha **Grupo federado** para importar un grupo desde el origen de identidad configurado previamente.

   Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan utilizar las aplicaciones cliente para gestionar los recursos del inquilino, en función de los permisos de grupo.

2. Introduzca el nombre del grupo.
   - **Grupo local**: Introduzca tanto un nombre para mostrar como un nombre exclusivo. Puede editar el nombre para mostrar más adelante.
   - **Grupo federado**: Introduzca el nombre único. Para Active Directory, el nombre único es el nombre asociado con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `uid` atributo.
3. Seleccione **continuar**.

Administrar permisos de grupo

Los permisos de grupo controlan las tareas que los usuarios pueden realizar en el gestor de inquilinos y en la API de gestión de inquilinos.

Pasos

1. Para **Modo de acceso**, seleccione una de las siguientes opciones:
   - **Read-write** (por defecto): Los usuarios pueden iniciar sesión en Tenant Manager y administrar la configuración del inquilino.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden hacer ningún cambio ni realizar ninguna operación en el administrador de inquilinos o la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

Si un usuario pertenece a varios grupos y cualquier grupo está establecido en sólo lectura, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

2. Seleccione la casilla de verificación **acceso raíz** si los usuarios del grupo necesitan iniciar sesión en el Administrador de inquilinos o en la API de administración de inquilinos.
3. Seleccione **continuar**.

Configure la política de grupo de Swift

Los usuarios de Swift necesitan permiso de administrador para autenticarse en la API REST DE Swift para crear contenedores e ingerir objetos.

1. Seleccione la casilla de verificación **Swift administrator** si los usuarios del grupo necesitan usar la API REST DE Swift para administrar contenedores y objetos.
2. Si está creando un grupo local, seleccione **continuar**. Si está creando un grupo federado, seleccione **Crear grupo** y **Finalizar**.

Añadir usuarios (sólo grupos locales)

Puede guardar el grupo sin agregar usuarios o, opcionalmente, puede agregar cualquier usuario local que ya exista.

Pasos

1. Opcionalmente, seleccione uno o varios usuarios locales para este grupo.

   Si aún no ha creado usuarios locales, puede agregar este grupo al usuario en la página Usuarios. Consulte "Gestionar usuarios locales".

2. Seleccione **Crear grupo** y **Finalizar**.

   El grupo creado aparece en la lista de grupos.

Permisos de gestión de inquilinos

Antes de crear un grupo de arrendatarios, tenga en cuenta qué permisos desea asignar a ese grupo. Los permisos de administración de inquilinos determinan qué tareas pueden realizar los usuarios con el Administrador de inquilinos o la API de gestión de inquilinos. Un usuario puede pertenecer a uno o más grupos. Los permisos son acumulativos si un usuario pertenece a varios grupos.

Para iniciar sesión en el Administrador de arrendatarios o utilizar la API de administración de arrendatarios, los usuarios deben pertenecer a un grupo que tenga al menos un permiso. Todos los usuarios que puedan iniciar sesión pueden realizar las siguientes tareas:

- Vea la consola
- Cambiar su propia contraseña (para usuarios locales)

Para todos los permisos, la configuración del modo de acceso del grupo determina si los usuarios pueden cambiar la configuración y realizar operaciones o si sólo pueden ver la configuración y las características relacionadas.

Si un usuario pertenece a varios grupos y cualquier grupo está establecido en sólo lectura, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

Puede asignar los siguientes permisos a un grupo. Tenga en cuenta que los inquilinos de S3 y los inquilinos de Swift tienen diferentes permisos de grupo.

Permiso	Descripción	Detalles
Acceso raíz	Proporciona acceso completo al administrador de inquilinos y a la API de gestión de inquilinos.	Los usuarios de Swift deben tener permiso de acceso raíz para iniciar sesión en la cuenta de inquilino.
Administrador	Solo para inquilinos Swift. Proporciona acceso completo a los contenedores y objetos de Swift para esta cuenta de inquilino	Los usuarios de Swift deben contar con el permiso de administrador de Swift para realizar cualquier operación con la API REST DE Swift.
Gestione sus propias credenciales de S3	Permite a los usuarios crear y eliminar sus propias claves de acceso S3.	Los usuarios que no tienen este permiso no ven la opción de menú **STORAGE (S3)** > **My S3 access keys**.
Ver todos los cubos	**S3 inquilinos**: Permite a los usuarios ver todas las configuraciones de cubos y cubos. • Inquilinos Swift*: Permite a los usuarios de Swift ver todos los contenedores y configuraciones de contenedores utilizando la API de administración de inquilinos.	Los usuarios que no tienen el permiso Ver todos los cubos o Gestionar todos los cubos no ven la opción de menú **Buckets**. Este permiso se sustituye por el permiso Gestionar todos los cubos. No afecta a las políticas de grupo o bloque S3 utilizadas por los clientes S3 o la consola S3. Solo puede asignar este permiso a grupos de Swift desde la API de gestión de inquilinos. No puede asignar este permiso a grupos Swift mediante el administrador de inquilinos.
Gestionar todos los cucharones	**S3 inquilinos**: Permite a los usuarios utilizar el Administrador de inquilinos y la API de administración de inquilinos para crear y eliminar buckets S3 y para administrar la configuración de todos los S3 buckets en la cuenta de inquilino, independientemente de las políticas de buckets o grupos S3. • Inquilinos Swift*: Permite a los usuarios Swift controlar la consistencia de los contenedores Swift mediante la API de administración de inquilinos.	Los usuarios que no tienen el permiso Ver todos los cubos o Gestionar todos los cubos no ven la opción de menú **Buckets**. Este permiso sustituye al permiso Ver todos los cubos. No afecta a las políticas de grupo o bloque S3 utilizadas por los clientes S3 o la consola S3. Solo puede asignar este permiso a grupos de Swift desde la API de gestión de inquilinos. No puede asignar este permiso a grupos Swift mediante el administrador de inquilinos.

Permiso	Descripción	Detalles
Gestionar puntos finales	Permite a los usuarios utilizar el Gestor de inquilinos o la API de gestión de inquilinos para crear o editar puntos finales de servicio de plataforma, que se utilizan como destino para los servicios de plataforma de StorageGRID.	Los usuarios que no tienen este permiso no ven la opción de menú **Platform services endpoints**.
Utilice la pestaña Consola de S3	Cuando se combina con el permiso Ver todos los cubos o Gestionar todos los cubos, permite a los usuarios ver y gestionar objetos desde la pestaña Consola de S3 en la página de detalles de un bloque.	

Gestionar grupos

Gestione los grupos de arrendatarios según sea necesario para ver, editar o duplicar un grupo y mucho más.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".

Ver o editar grupo

Puede ver y editar la información básica y los detalles de cada grupo.

Pasos

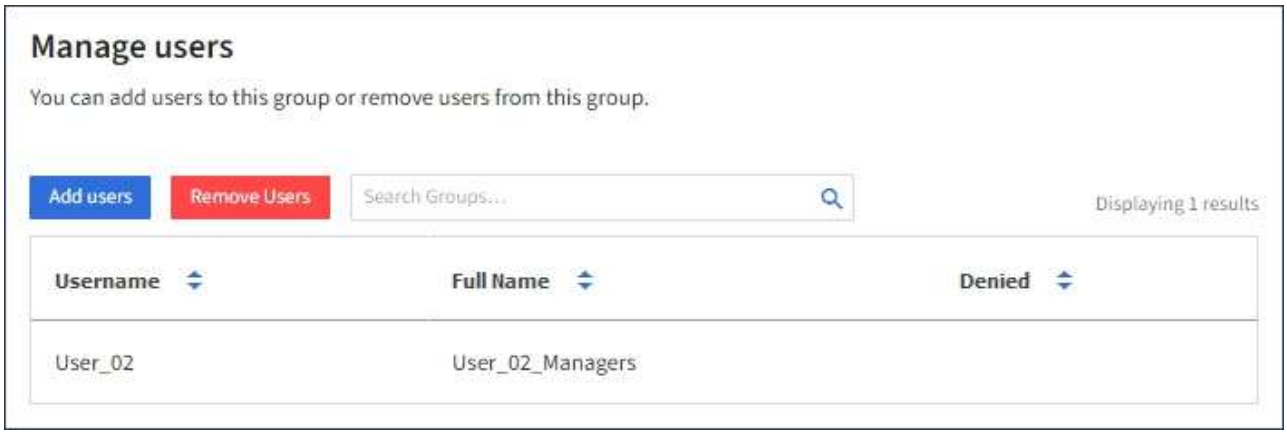
1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Revise la información proporcionada en la página Grupos, que muestra información básica de todos los grupos locales y federados de esta cuenta de arrendatario.

   Si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo grupos en la cuadrícula de origen del inquilino:

   - Un mensaje de banner indica que si edita o elimina un grupo, los cambios no se sincronizarán con la otra cuadrícula.
   - Según sea necesario, un mensaje de banner indica si los grupos no se clonaron en el inquilino en la cuadrícula de destino. Puede hacerlo volver a intentar un clon de grupo eso falló.
3. Si desea cambiar el nombre del grupo:
   a. Seleccione la casilla de verificación para el grupo.
   b. Selecciona **Acciones** > **Editar nombre de grupo**.
   c. Introduzca el nuevo nombre.
   d. Selecciona **Guardar cambios.**
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
   - Seleccione el nombre del grupo.

- Selecciona la casilla de verificación del grupo y selecciona **Acciones** > **Ver detalles del grupo**.

5. Revise la sección Visión General, que muestra la siguiente información para cada grupo:
   - Nombre para mostrar
   - Nombre exclusivo
   - Tipo
   - Modo de acceso
   - Permisos
   - S3 Política
   - Número de usuarios en este grupo
   - Campos adicionales si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo el grupo en la cuadrícula de origen del inquilino:
     - Estado de clonación, ya sea **Success** o **Failure**
     - Un banner azul que indica que si edita o elimina este grupo, los cambios no se sincronizarán con la otra cuadrícula.
6. Edite la configuración del grupo según sea necesario. Consulte "Cree grupos para un inquilino de S3" y.. "Cree grupos para un inquilino de Swift" para obtener más información acerca de lo que se debe introducir.
   a. En la sección Descripción general, cambie el nombre mostrado seleccionando el nombre o el icono de edición .
   b. En la pestaña **Permisos de grupo**, actualice los permisos y seleccione **Guardar cambios**.
   c. En la pestaña **Política de grupo**, realice los cambios y seleccione **Guardar cambios**.
      - Si está editando un grupo S3, seleccione opcionalmente una política de grupo S3 diferente o introduzca la cadena JSON de una política personalizada, según corresponda.
      - Si está editando un grupo Swift, opcionalmente seleccione o desactive la casilla de verificación **Swift Administrator**.
7. Para añadir uno o varios usuarios locales existentes al grupo:
   a. Seleccione la ficha Usuarios.



   b. Selecciona **Añadir usuarios**.
   c. Seleccione los usuarios existentes que desea agregar y seleccione **Agregar usuarios**.

      Aparece un mensaje de éxito en la parte superior derecha.

8. Para eliminar usuarios locales del grupo:
   a. Seleccione la ficha Usuarios.
   b. Selecciona **Eliminar usuarios**.
   c. Seleccione los usuarios que desea eliminar y seleccione **Eliminar usuarios**.

      Aparece un mensaje de éxito en la parte superior derecha.

9. Confirma que has seleccionado **Guardar cambios** para cada sección que cambiaste.

Grupo duplicado

Puede duplicar un grupo existente para crear nuevos grupos más rápidamente.

> Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y duplica un grupo de la cuadrícula de origen del inquilino, el grupo duplicado se clonará en la cuadrícula de destino del inquilino.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de control del grupo que desea duplicar.
3. Seleccione **acciones** > **Duplicar grupo**.
4. Consulte "Cree grupos para un inquilino de S3" o. "Cree grupos para un inquilino de Swift" para obtener más información acerca de lo que se debe introducir.
5. Seleccione **Crear grupo**.

Vuelva a intentar clonar el grupo

Para volver a intentar un clon que generó errores:

1. Seleccione cada grupo que indique *(Error de clonación)* debajo del nombre del grupo.
2. Selecciona **Acciones** > **Clonar grupos**.
3. Vea el estado de la operación de clonación desde la página de detalles de cada grupo que está clonando.

Para obtener más información, consulte "Clone los usuarios y los grupos de inquilinos".

Elimine uno o más grupos

Puede eliminar uno o varios grupos. Cualquier usuario que pertenezca únicamente a un grupo que se haya eliminado ya no podrá iniciar sesión en el gestor de inquilinos ni utilizar la cuenta de inquilino.

> Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y eliminas un grupo, StorageGRID no eliminará el grupo correspondiente en la otra cuadrícula. Si necesita mantener esta información sincronizada, debe eliminar el mismo grupo de ambas cuadrículas.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de verificación para cada grupo que desee eliminar.
3. Selecciona **Acciones** > **Eliminar grupo** o **Acciones** > **Eliminar grupos**.

Se muestra un cuadro de diálogo de confirmación.

4. Selecciona **Borrar grupo** o **Eliminar grupos**.

Gestionar usuarios locales

Puede crear usuarios locales y asignarles grupos locales para determinar las funciones a las que pueden acceder estos usuarios. El gestor de inquilinos incluye un usuario local predefinido, denominado «root». Aunque puede agregar y eliminar usuarios locales, no puede eliminar el usuario root.

> Si el inicio de sesión único (SSO) está habilitado para el sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el gestor de inquilinos o en la API de gestión de inquilinos, aunque pueden utilizar aplicaciones cliente para acceder a los recursos del inquilino, según los permisos del grupo.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Si su cuenta de inquilino tiene el permiso **Use grid federation connection**, ha revisado el flujo de trabajo y las consideraciones para "clonación de usuarios y grupos de inquilinos", y ha iniciado sesión en la cuadrícula de origen del inquilino.

Cree un usuario local

Puede crear un usuario local y asignarlos a uno o varios grupos locales para controlar sus permisos de acceso.

Los usuarios de S3 que no pertenecen a ningún grupo no tienen permisos de administración ni se les aplican S3 políticas de grupo. Es posible que estos usuarios tengan acceso a bloques de S3 otorgado a través de una política de bloques.

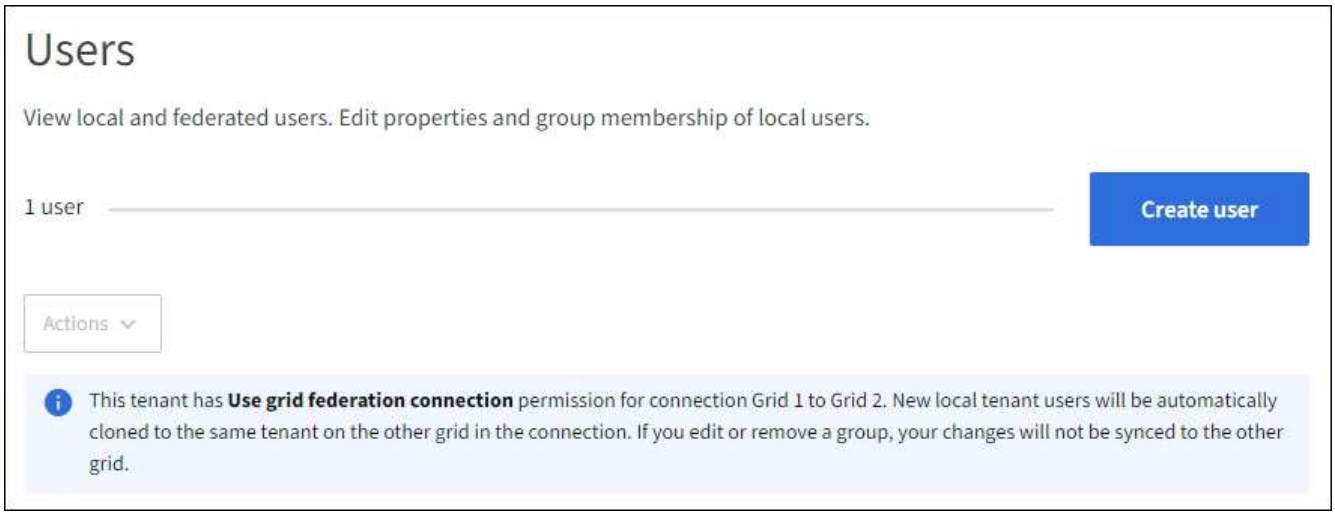
Los usuarios de Swift que no pertenezcan a ningún grupo no tienen permisos de administración ni acceso a contenedor Swift.

Acceda al asistente Crear usuario

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.

   Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, un banner azul indica que esta es la cuadrícula de origen del inquilino. Todos los usuarios locales que cree en esta cuadrícula se clonarán en la otra cuadrícula de la conexión.



2. Seleccione **Crear usuario**.

Introduzca las credenciales

Pasos

1. Para el paso **Introducir credenciales de usuario**, complete los siguientes campos.

Campo	Descripción
Nombre completo	El nombre completo de este usuario, por ejemplo, el nombre y apellidos de una persona o el nombre de una aplicación.
Nombre de usuario	Nombre que utilizará este usuario para iniciar sesión. Los nombres de usuario deben ser únicos y no se pueden cambiar. **Nota**: Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, se producirá un error de clonación si el mismo **Nombre de usuario** ya existe para el inquilino en la cuadrícula de destino.
Contraseña y confirme la contraseña	La contraseña que el usuario utilizará inicialmente al iniciar sesión.
Denegar el acceso	Seleccione **Sí** para evitar que este usuario inicie sesión en la cuenta de inquilino, aunque todavía pertenezca a uno o más grupos. Por ejemplo, selecciona **Sí** para suspender temporalmente la capacidad de un usuario para iniciar sesión.

2. Seleccione **continuar**.

Asignar a grupos

Pasos

1. Asigne el usuario a uno o más grupos locales para determinar qué tareas se pueden realizar.

   La asignación de un usuario a grupos es opcional. Si lo prefiere, puede seleccionar usuarios al crear o

editar grupos.

Los usuarios que no pertenezcan a ningún grupo no tendrán permisos de administración. Los permisos son acumulativos. Los usuarios tendrán todos los permisos para todos los grupos a los que pertenezcan. Consulte "Permisos de gestión de inquilinos".

2. Seleccione **Crear usuario**.

   Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y usted está en la cuadrícula de origen del inquilino, el nuevo usuario local se clona en la cuadrícula de destino del inquilino. **Success** aparece como **Cloning status** en la sección Overview de la página de detalles del usuario.

3. Seleccione **Finalizar** para volver a la página Usuarios.

Ver o editar usuario local

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. Revise la información proporcionada en la página Usuarios, que muestra información básica para todos los usuarios locales y federados de esta cuenta de arrendatario.

   Si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo al usuario en la cuadrícula de origen del inquilino:

   - Un mensaje de banner indica que si edita o elimina un usuario, los cambios no se sincronizarán con la otra cuadrícula.
   - Según sea necesario, un mensaje de banner indica si los usuarios no se clonaron en el inquilino en la cuadrícula de destino. Puede hacerlo vuelva a intentar un clon de usuario que haya fallado.
3. Si desea cambiar el nombre completo del usuario:
   a. Seleccione la casilla de control para el usuario.
   b. Selecciona **Acciones** > **Editar nombre completo**.
   c. Introduzca el nuevo nombre.
   d. Selecciona **Guardar cambios.**
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
   - Seleccione el nombre de usuario.
   - Selecciona la casilla de verificación para el usuario y selecciona **Acciones** > **Ver detalles de usuario**.
5. Revise la sección Visión General, que muestra la siguiente información para cada usuario:
   - Nombre completo
   - Nombre de usuario
   - Tipo de usuario
   - Acceso denegado
   - Modo de acceso
   - Pertenencia a grupos
   - Campos adicionales si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo al usuario en la cuadrícula de origen del inquilino:
     - Estado de clonación, ya sea **Success** o **Failure**

- Un banner azul que indica que si edita este usuario, los cambios no se sincronizarán con la otra cuadrícula.

6. Edite la configuración del usuario según sea necesario. Consulte Crear usuario local para obtener más información acerca de lo que se debe introducir.
   a. En la sección Descripción general, cambie el nombre completo seleccionando el nombre o el icono de edición .

      No puede cambiar el nombre de usuario.

   b. En la pestaña **Contraseña**, cambie la contraseña del usuario y seleccione **Guardar cambios**.
   c. En la pestaña **Acceso**, selecciona **No** para permitir que el usuario inicie sesión o selecciona **Sí** para evitar que el usuario inicie sesión. Luego, selecciona **Guardar cambios**.
   d. En la pestaña **Teclas de acceso**, selecciona **Crear clave** y sigue las instrucciones para "Creando las claves de acceso S3 de otro usuario".
   e. En la pestaña **Grupos**, selecciona **Editar grupos** para agregar el usuario a los grupos o eliminar al usuario de los grupos. Luego, selecciona **Guardar cambios**.
7. Confirma que has seleccionado **Guardar cambios** para cada sección que cambiaste.

Usuario local duplicado

Puede duplicar un usuario local para crear un usuario nuevo más rápidamente.

> Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y duplica un usuario de la cuadrícula de origen del inquilino, el usuario duplicado se clonará en la cuadrícula de destino del inquilino.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. Seleccione la casilla de control para el usuario que desea duplicar.
3. Selecciona **Acciones** > **Usuario duplicado**.
4. Consulte Crear usuario local para obtener más información acerca de lo que se debe introducir.
5. Seleccione **Crear usuario**.

Reintente clonar el usuario

Para volver a intentar un clon que generó errores:

1. Seleccione cada usuario que indique *(Error de clonación)* debajo del nombre de usuario.
2. Selecciona **Acciones** > **Clonar usuarios**.
3. Vea el estado de la operación de clonación desde la página de detalles de cada usuario que está clonando.

Para obtener más información, consulte "Clone los usuarios y los grupos de inquilinos".

Elimine uno o varios usuarios locales

Puede eliminar de forma permanente uno o varios usuarios locales que ya no necesiten acceder a la cuenta de inquilino de StorageGRID.

Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y eliminas a un usuario local, StorageGRID no eliminará al usuario correspondiente en la otra cuadrícula. Si necesita mantener esta información sincronizada, debe eliminar el mismo usuario de ambas cuadrículas.

Debe utilizar el origen de identidad federado para eliminar usuarios federados.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. Seleccione la casilla de verificación para cada usuario que desee eliminar.
3. Selecciona **Acciones** > **Eliminar usuario** o **Acciones** > **Eliminar usuarios**.

   Se muestra un cuadro de diálogo de confirmación.

4. Seleccione **Eliminar usuario** o **Eliminar usuarios**.

Gestión de claves de acceso de S3

Gestionar claves de acceso S3: Descripción general

Cada usuario de una cuenta de inquilino de S3 debe tener una clave de acceso para almacenar y recuperar objetos en el sistema StorageGRID. Una clave de acceso consta de un ID de clave de acceso y una clave de acceso secreta.

Las claves de acceso S3 se pueden gestionar de la siguiente manera:

- Los usuarios que tienen el permiso **Administrar sus propias credenciales de S3** pueden crear o eliminar sus propias claves de acceso de S3.
- Los usuarios que tienen el permiso **root access** pueden administrar las claves de acceso para la cuenta root de S3 y todos los demás usuarios. Las claves de acceso raíz proporcionan acceso completo a todos los bloques y objetos para el inquilino, a menos que se deshabilite explícitamente mediante una política de bloque.

StorageGRID admite la autenticación Signature versión 2 y Signature versión 4. No se permite el acceso de cuenta cruzada a menos que una política de bloque lo habilite explícitamente.

Cree sus propias claves de acceso S3

Si usa un inquilino de S3 y tiene el permiso correspondiente, puede crear sus propias claves de acceso S3. Debe tener una clave de acceso para acceder a los cubos y objetos.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Administre sus propias credenciales de S3 o permiso de acceso raíz".

Acerca de esta tarea

Puede crear una o varias claves de acceso S3 que le permiten crear y gestionar bloques para su cuenta de

inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con su nuevo ID de clave de acceso y clave de acceso secreta. Por seguridad, no cree más claves de las que necesita, y elimine las claves que no está utilizando. Si sólo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la antigua y, a continuación, elimine la anterior.

Cada clave puede tener un tiempo de caducidad específico o no puede caducar. Siga estas directrices para el tiempo de caducidad:

- Establezca un tiempo de caducidad para sus llaves para limitar su acceso a un período de tiempo determinado. Establecer un tiempo de caducidad corto puede ayudar a reducir el riesgo si el ID de clave de acceso y la clave de acceso secreta están expuestos accidentalmente. Las claves caducadas se eliminan automáticamente.
- Si el riesgo de seguridad en su entorno es bajo y no necesita crear periódicamente claves nuevas, no tiene que establecer un tiempo de caducidad para las claves. Si decide más tarde crear claves nuevas, elimine manualmente las claves antiguas.

> Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de su cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Mis claves de acceso**.

   Aparecerá la página Mis claves de acceso y mostrará una lista de las claves de acceso existentes.

2. Seleccione **Crear clave**.
3. Debe realizar una de las siguientes acciones:
   - Seleccione **no establezca un tiempo de caducidad** para crear una clave que no caducará. (Predeterminado)
   - Seleccione **establecer un tiempo de caducidad** y establezca la fecha y la hora de caducidad.

     > La fecha de caducidad puede ser un máximo de cinco años a partir de la fecha actual. El tiempo de caducidad puede ser un mínimo de un minuto desde la hora actual.

4. Seleccione **Crear clave de acceso**.

   Aparece el cuadro de diálogo Descargar clave de acceso, en el que se enumeran el ID de clave de acceso y la clave de acceso secreta.

5. Copie el ID de la clave de acceso y la clave de acceso secreta a una ubicación segura, o seleccione **Descargar .csv** para guardar un archivo de hoja de cálculo que contenga el ID de clave de acceso y la clave de acceso secreta.

   > No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información. No puede copiar ni descargar claves después de cerrar el cuadro de diálogo.

6. Seleccione **Finalizar**.

   La nueva clave aparece en la página Mis claves de acceso.

7. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, utilice opcionalmente la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la cuadrícula de origen al inquilino en la cuadrícula de destino. Consulte "Clone las claves de acceso S3 mediante la API".

Consulte las claves de acceso de S3

Si está utilizando un inquilino de S3 y tiene el "permiso apropiado", Puede ver una lista de sus S3 teclas de acceso. Puede ordenar la lista por tiempo de caducidad, de modo que puede determinar qué claves caducarán pronto. Según sea necesario, puedes "crear nuevas claves" o. "teclas de eliminación" que ya no utiliza.

> Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de su cuenta y nunca las comparta con otros usuarios.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene las credenciales Administrar sus propias credenciales S3 "permiso".

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Mis claves de acceso**.
2. Desde la página Mis claves de acceso, ordene las claves de acceso existentes por **Tiempo de caducidad** o **ID de clave de acceso**.
3. Según sea necesario, cree nuevas claves o elimine las claves que ya no esté utilizando.

   Si crea claves nuevas antes de que caduquen las claves existentes, puede empezar a utilizar las nuevas claves sin perder temporalmente el acceso a los objetos de la cuenta.

   Las claves caducadas se eliminan automáticamente.

Elimine sus propias claves de acceso de S3

Si usa un inquilino de S3 y tiene el permiso correspondiente, puede eliminar sus propias claves de acceso S3. Cuando se elimina una clave de acceso, ya no se puede utilizar para acceder a los objetos y los bloques de la cuenta de inquilino.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Usted tiene la "Administre sus propios permisos de credenciales de S3".

> Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de su cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Mis claves de acceso**.
2. En la página Mis claves de acceso, seleccione la casilla de verificación de cada clave de acceso que desee eliminar.
3. Seleccione **tecla Eliminar**.
4. En el cuadro de diálogo de confirmación, seleccione **Tecla Eliminar**.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página.

Cree las claves de acceso S3 de otro usuario

Si usa un inquilino de S3 y tiene el permiso apropiado, puede crear claves de acceso S3 para otros usuarios, como las aplicaciones que necesitan acceso a bloques y objetos.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".

Acerca de esta tarea

Puede crear una o varias claves de acceso de S3 para otros usuarios, de modo que puedan crear y gestionar bloques para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con el nuevo ID de clave de acceso y la clave de acceso secreta. Por seguridad, no cree más claves de las que necesita el usuario y elimine las claves que no se están utilizando. Si sólo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la antigua y, a continuación, elimine la anterior.

Cada clave puede tener un tiempo de caducidad específico o no puede caducar. Siga estas directrices para el tiempo de caducidad:

- Establezca un tiempo de caducidad para que las claves limiten el acceso del usuario a un determinado período de tiempo. Establecer un tiempo de caducidad corto puede ayudar a reducir el riesgo si el ID de clave de acceso y la clave de acceso secreta se exponen accidentalmente. Las claves caducadas se eliminan automáticamente.
- Si el riesgo de seguridad de su entorno es bajo y no es necesario crear periódicamente claves nuevas, no es necesario establecer un tiempo de caducidad de las claves. Si decide más tarde crear claves nuevas, elimine manualmente las claves antiguas.

> Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. Seleccione el usuario cuyas claves de acceso de S3 desee gestionar.

   Aparece la página de detalles del usuario.

3. Seleccione **teclas de acceso** y, a continuación, seleccione **tecla de creación**.

4. Debe realizar una de las siguientes acciones:
   - Selecciona **No establecer un tiempo de caducidad** para crear una clave que no caduque. (Predeterminado)
   - Seleccione **establecer un tiempo de caducidad** y establezca la fecha y la hora de caducidad.

   > La fecha de caducidad puede ser un máximo de cinco años a partir de la fecha actual. El tiempo de caducidad puede ser un mínimo de un minuto desde la hora actual.

5. Seleccione **Crear clave de acceso**.

   Se muestra el cuadro de diálogo Descargar clave de acceso, en el que se enumeran el ID de clave de acceso y la clave de acceso secreta.

6. Copie el ID de la clave de acceso y la clave de acceso secreta a una ubicación segura, o seleccione **Descargar .csv** para guardar un archivo de hoja de cálculo que contenga el ID de clave de acceso y la clave de acceso secreta.

   > No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información. No puede copiar ni descargar claves después de cerrar el cuadro de diálogo.

7. Seleccione **Finalizar**.

   La nueva clave aparece en la ficha teclas de acceso de la página de detalles del usuario.

8. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, utilice opcionalmente la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la cuadrícula de origen al inquilino en la cuadrícula de destino. Consulte "Clone las claves de acceso S3 mediante la API".

Ver las claves de acceso S3 de otro usuario

Si usa un inquilino de S3 y tiene los permisos adecuados, puede ver las claves de acceso S3 de otro usuario. Puede ordenar la lista por tiempo de caducidad para que pueda determinar qué claves caducarán pronto. Según sea necesario, puede crear nuevas claves y eliminar claves que ya no estén en uso.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

> Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. En la página Usuarios, seleccione el usuario cuyas S3 claves de acceso desea ver.

3. En la página Detalles del usuario, selecciona **Teclas de acceso**.
4. Ordene las teclas por **tiempo de caducidad** o **ID de clave de acceso**.
5. Según sea necesario, cree nuevas claves y elimine manualmente las que ya no estén en uso.

   Si crea claves nuevas antes de que caduquen las claves existentes, el usuario podrá empezar a utilizar las nuevas claves sin perder temporalmente el acceso a los objetos de la cuenta.

   Las claves caducadas se eliminan automáticamente.

Información relacionada

"Cree las claves de acceso S3 de otro usuario"

"Elimine las claves de acceso S3 de otro usuario"

Elimine las claves de acceso S3 de otro usuario

Si usa un inquilino de S3 y tiene los permisos adecuados, puede eliminar las claves de acceso S3 de otro usuario. Cuando se elimina una clave de acceso, ya no se puede utilizar para acceder a los objetos y los bloques de la cuenta de inquilino.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

> Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves de acceso de forma regular, elimine las claves que no utilice de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. En la página Usuarios, seleccione el usuario cuyas S3 claves de acceso desea administrar.
3. En la página Detalles del usuario, selecciona **Teclas de acceso** y, a continuación, selecciona la casilla de verificación para cada clave de acceso
   desea eliminar.
4. Seleccione **acciones** > **Borrar clave seleccionada**.
5. En el cuadro de diálogo de confirmación, seleccione **Tecla Eliminar**.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página.

Gestión de bloques S3

Cree un bloque de S3

Puede usar el administrador de inquilinos para crear bloques S3 para los datos de objetos.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene acceso raíz o Gestionar todos los bloques "permiso". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

> Los permisos para establecer o modificar las propiedades de Object Lock de grupos o objetos de S3 pueden ser concedidos por "política de bloques o política de grupo".

- Si tiene previsto habilitar el bloqueo de objetos de S3 para un depósito, un administrador de grid ha habilitado la configuración global de bloqueo de objetos de S3 para el sistema StorageGRID y ha revisado los requisitos para los bloques y objetos de bloqueo de objetos de S3. Consulte "Utilice Bloqueo de objetos S3 para retener objetos".

Acceda al asistente

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
2. Seleccione **Crear cucharón**.

Introduzca los detalles

Pasos

1. Introduzca los detalles del cucharón.

Campo	Descripción
Nombre del bloque	Un nombre para el depósito que cumple con estas reglas: • Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino). • Debe ser compatible con DNS. • Debe incluir al menos 3 y no más de 63 caracteres. • Cada etiqueta debe comenzar y terminar con una letra minúscula o un número y solo puede utilizar letras minúsculas, números y guiones. • No debe utilizar periodos en solicitudes de estilo alojadas virtuales. Los períodos provocarán problemas en la verificación del certificado comodín del servidor. Para obtener más información, consulte "Documentación de Amazon Web Services (AWS) sobre reglas de nomenclatura de bloques". **Nota**: No puedes cambiar el nombre del cubo después de crear el cubo.

Campo	Descripción
Región	La región del cubo. El administrador de StorageGRID gestiona las regiones disponibles. La región de un bloque puede afectar la política de protección de datos aplicada a los objetos. De forma predeterminada, todos los bloques se crean en la `us-east-1` región. **Nota**: No puedes cambiar la región después de crear el cubo.

2. Seleccione **continuar**.

Gestionar la configuración del objeto

Pasos

1. Opcionalmente, habilite el control de versiones del objeto para el bloque.

   Habilite el control de versiones de objetos si desea almacenar cada versión de cada objeto en este bloque. A continuación, puede recuperar versiones anteriores de un objeto según sea necesario. Debe habilitar el control de versiones de objetos si el bloque se va a utilizar para la replicación entre grid.

2. Si la opción Bloqueo de objetos S3 global está habilitada, habilite opcionalmente Bloqueo de objetos S3 para que el depósito almacene objetos utilizando un modelo WORM.

   Habilite el bloqueo de objetos S3 para un depósito solo si necesita mantener objetos durante un tiempo fijo, por ejemplo, para cumplir con ciertos requisitos normativos. S3 Object Lock es una configuración permanente que le ayuda a evitar que los objetos se eliminen o sobrescriban durante un período de tiempo fijo o indefinidamente.

   > Una vez que se habilita la configuración Bloqueo de objetos S3 para un depósito, no se puede desactivar. Cualquier persona con los permisos correctos puede agregar objetos a este depósito que no se pueden cambiar. Es posible que no pueda eliminar estos objetos o el cubo en sí.

   Si habilita S3 Object Lock para un bloque, el control de versiones de bloques se habilita automáticamente.

3. Si seleccionó **Habilitar bloqueo de objetos S3**, opcionalmente habilite **Retención predeterminada** para este depósito.

   Cuando se habilita **Retención predeterminada**, los nuevos objetos agregados al depósito se protegerán automáticamente de ser eliminados o sobrescritos. La configuración **default retention** no se aplica a los objetos que tienen sus propios periodos de retención.

   a. Si **Retención predeterminada** está habilitada, especifique un **Modo de retención predeterminado** para el depósito.

Modo de retención predeterminado	Descripción
Cumplimiento de normativas	• El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta. • La fecha de retención del objeto se puede aumentar, pero no se puede reducir. • No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha.
Gobernanza	• Usuarios con `s3:BypassGovernanceRetention` el permiso puede utilizar el `x-amz-bypass-governance-retention: true` solicitar cabecera para omitir la configuración de retención. • Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha. • Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

b. Si **Retención predeterminada** está habilitada, especifique el **Período de retención predeterminado** para el depósito.

   El **período de retención predeterminado** indica cuánto tiempo deben conservarse los nuevos objetos agregados a este depósito, a partir del momento en que se ingieren. Especifique un valor entre 1 y 36.500 días o entre 1 y 100 años, ambos incluidos.

4. Seleccione **Crear cucharón**.

   El cucharón se crea y se agrega a la tabla de la página Cuches.

5. Opcionalmente, selecciona **Ir a la página de detalles del cubo** a. "ver detalles del período" y realizar la configuración adicional.

Ver detalles del período

Puede ver los depósitos en su cuenta de inquilino.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Acceso raíz, Gestionar todos los bloques o Ver todos los bloques". Estos permisos anulan la configuración de permisos en las políticas de grupo o bloque.

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.

   Aparecerá la página Buckets.

2. Revise la información de resumen de cada bloque.

   Según sea necesario, puede ordenar la información por cualquier columna o puede avanzar y retroceder

por la lista.

> Los valores de recuento de objetos y espacio utilizado que se muestran son estimaciones. Estas estimaciones se ven afectadas por el tiempo de los ingests, la conectividad de red y el estado del nodo. Si los bloques tienen habilitado el control de versiones, las versiones de objetos eliminados se incluyen en el recuento de objetos.

Columna	Descripción
Nombre	El nombre único del depósito, que no se puede cambiar.
Funciones activadas	Lista de funciones activadas para el depósito.
Bloqueo de objetos de S3	Si el bloqueo de objetos S3 está activado para el depósito. Esta columna sólo aparece si Bloqueo de objetos S3 está activado para la cuadrícula. Esta columna también muestra información para todos los segmentos compatibles anteriores.
Región	La región del cubo, que no se puede cambiar.
Recuento de objetos	Núm. De objetos en este depósito. Cuando se agregan o se eliminan objetos, es posible que este valor no se actualice de inmediato. Si los cubos tienen el control de versiones activado, se incluyen versiones de objetos no actuales en este valor.
Espacio utilizado	El tamaño lógico de todos los objetos del bloque. El tamaño lógico no incluye el espacio real necesario para las copias replicadas o con código de borrado o para los metadatos de objetos.
Fecha de creación	La fecha y la hora en la que se creó el bloque.

3. Para ver los detalles de un cubo específico, seleccione el nombre del cubo en la tabla.

   Aparece la página de detalles bucket. En esta página, puede realizar las siguientes tareas si tiene los permisos necesarios:

   - Configure y gestione las opciones de bloque:
     - "Etiquetas de políticas de ILM"
     - "Gestione la coherencia de los bloques"
     - "Últimas actualizaciones de hora de acceso"
     - "Control de versiones de objetos"
     - "Bloqueo de objetos de S3"
     - "Retención de cucharón por defecto"
   - Configurar el acceso al bloque, por ejemplo "Uso compartido de recursos de origen cruzado (CORS)"
   - "Gestione los servicios de la plataforma" (Si se permite para el inquilino), incluida la replicación de CloudMirror, las notificaciones de eventos y la integración de búsqueda

- Habilite y. "gestionar la replicación entre grid" (Si se permite para el inquilino) replicar los objetos ingeridos en este bucket en otro sistema StorageGRID
- Acceda a "S3 Consola" para gestionar los objetos del depósito
- "Eliminar todos los objetos de un depósito"
- "Eliminar un cubo" eso ya está vacío

Aplique una etiqueta de política de ILM a un bloque

Elija una etiqueta de política de ILM para aplicarla a un bloque en función de sus requisitos de almacenamiento de objetos.

La política de ILM controla dónde se almacenan los datos de objetos y si se eliminan después de un cierto período de tiempo. Su administrador de grid crea políticas de ILM y las asigna a las etiquetas de políticas de ILM cuando usa varias políticas activas.

Evite reasignar con frecuencia la etiqueta de política de un bucket. De lo contrario, pueden producirse problemas de rendimiento.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Acceso raíz, Gestionar todos los bloques o Ver todos los bloques". Estos permisos anulan la configuración de permisos en las políticas de grupo o bloque.

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.

   Aparecerá la página Buckets. Según sea necesario, puede ordenar la información por cualquier columna o puede avanzar y retroceder por la lista.

2. Seleccione el nombre del bloque al que desea asignar una etiqueta de política de ILM.

   También puede cambiar la asignación de etiquetas de política de ILM de un bloque que ya tenga una etiqueta asignada.

   Los valores de recuento de objetos y espacio utilizado que se muestran son estimaciones. Estas estimaciones se ven afectadas por el tiempo de los ingests, la conectividad de red y el estado del nodo. Si los bloques tienen habilitado el control de versiones, las versiones de objetos eliminados se incluyen en el recuento de objetos.

3. En la pestaña Bucket options, expanda el acordeón de etiqueta de política de ILM. Este acordeón solo aparece si el administrador de grid ha habilitado el uso de etiquetas de política personalizadas.
4. Lea la descripción de cada etiqueta de política para determinar qué etiqueta se debe aplicar al depósito.

   Si se cambia la etiqueta de política de ILM de un bloque, se activará la reevaluación de ILM de todos los objetos del bloque. Si la nueva política conserva los objetos durante un tiempo limitado, los objetos más antiguos se eliminarán.

5. Seleccione el botón de radio de la etiqueta que desea asignar al depósito.
6. Seleccione **Guardar cambios**. Se establecerá una nueva etiqueta de cubo S3 en el cucharón con la llave

`NTAP-SG-ILM-BUCKET-TAG` Y el valor del nombre de etiqueta de la política de ILM.

Asegúrese de que las aplicaciones S3 no anulen ni eliminen accidentalmente la nueva etiqueta de depósito. Si se omite esta etiqueta al aplicar un TagSet nuevo al bloque, los objetos del bloque se volverán a evaluar según la política de ILM predeterminada.

Establezca y modifique las etiquetas de políticas de ILM mediante solo la API del administrador de inquilinos o del administrador de inquilinos donde se valida la etiqueta de política de ILM. No modifique el `NTAP-SG-ILM-BUCKET-TAG` Etiqueta de política de gestión de la vida útil de la información mediante la API de PutBucketTagging de S3 o la API de DeleteBucketTagging de S3.

El cambio de la etiqueta de política asignada a un bloque tiene un impacto temporal en el rendimiento mientras los objetos se reevalúan con la nueva política de ILM.

Gestione la coherencia de los bloques

Los valores de coherencia se pueden utilizar para especificar la disponibilidad de cambios de configuración de bloques, así como para proporcionar un equilibrio entre la disponibilidad de los objetos dentro de un bloque y la coherencia de dichos objetos en distintos nodos de almacenamiento y sitios. Puede cambiar los valores de coherencia para que sean diferentes de los valores predeterminados para que las aplicaciones cliente puedan satisfacer sus necesidades operativas.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Directrices de coherencia de bloques

La coherencia de bloques se utiliza para determinar la coherencia de las aplicaciones cliente que afectan a los objetos dentro de ese bloque S3. En general, debe utilizar la consistencia **Read-after-new-write** para sus cubos.

Cambie la consistencia del bloque

Si la consistencia de **Read-after-new-write** no cumple con los requisitos de la aplicación cliente, puede cambiar la consistencia configurando la consistencia del depósito o utilizando el `Consistency-Control` encabezado. La `Consistency-Control` el cabezal anula la consistencia del cucharón.

Cuando se cambia la consistencia de un depósito, sólo se garantiza que los objetos que se ingieren después del cambio cumplan con la configuración revisada.

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
2. Seleccione el nombre del cubo de la tabla.

   Aparece la página de detalles bucket.

3. En la pestaña **Opciones de cucharón**, selecciona el acordeón **.
4. Seleccione una coherencia para las operaciones realizadas en los objetos de este bloque.
   - **Todo**: Proporciona el más alto nivel de consistencia. Todos los nodos reciben los datos inmediatamente o se produce un error en la solicitud.
   - **Strong-global**: Garantiza la consistencia de lectura tras escritura para todas las solicitudes de los clientes en todos los sitios.
   - **Strong-site**: Garantiza la consistencia de lectura después de escritura para todas las solicitudes de los clientes dentro de un sitio.
   - **Read-after-new-write** (por defecto): Proporciona consistencia de lectura después de escritura para nuevos objetos y consistencia eventual para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
   - **Disponible**: Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.
5. Seleccione **Guardar cambios**.

Qué sucede cuando se cambia la configuración del bloque

Los cubos tienen varios ajustes que afectan al comportamiento de los cubos y los objetos dentro de esos cubos.

Los siguientes ajustes de cucharón utilizan la consistencia **strong** de forma predeterminada. Si no hay dos o más nodos de almacenamiento disponibles en ningún sitio, o si no hay un sitio disponible, es posible que no esté disponible ningún cambio en estos ajustes.

- "Eliminación de bloque vacío en segundo plano"
- "Hora del último acceso"
- "Ciclo de vida del cucharón"
- "Política de bloques"
- "Etiquetado de cucharones"
- "Control de versiones del cucharón"
- "Bloqueo de objetos de S3"
- "Cifrado de bloques"

> El valor de coherencia para el control de versiones de bloque, el bloqueo de objetos de S3 y el cifrado de bloque no se puede establecer en un valor que no es muy consistente.

Los siguientes ajustes de cucharón no utilizan una gran consistencia y tienen una mayor disponibilidad para los cambios. Los cambios en estos ajustes pueden tardar algún tiempo antes de tener un efecto.

- "Configuración de servicios de plataforma: Notificación, replicación o integración de búsqueda"
- "Configuración de CORS"
- Cambie la consistencia del cucharón

Si la coherencia predeterminada que se utiliza al cambiar la configuración del bloque no cumple con los requisitos de la aplicación cliente, puede cambiar la coherencia mediante el `Consistency-Control` encabezado del "API REST DE S3" o mediante el `reducedConsistency` o. `force` de la "API de gestión de inquilinos".

Activar o desactivar las actualizaciones de la hora del último acceso

Cuando los administradores de grid crean las reglas de gestión del ciclo de vida de la información (ILM) para un sistema StorageGRID, puede especificar si desea mover ese objeto a una ubicación de almacenamiento diferente. Si usa un inquilino de S3, puede aprovechar esas reglas al habilitar actualizaciones en la última hora de acceso para los objetos de un bloque de S3.

Estas instrucciones solo se aplican a los sistemas StorageGRID que incluyen al menos una regla de ILM que utiliza la opción **last access time** como filtro avanzado o como tiempo de referencia. Puede ignorar estas instrucciones si el sistema StorageGRID no incluye dicha regla. Consulte "Utilice la última hora de acceso en las reglas de ILM" para obtener más detalles.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Acerca de esta tarea

El tiempo de último acceso es una de las opciones disponibles para la instrucción de colocación de **Tiempo de referencia** para una regla de ILM. Establecer el tiempo de referencia para una regla como el tiempo de último acceso permite a los administradores de grid especificar que los objetos se coloquen en determinadas ubicaciones de almacenamiento según la fecha en que se recuperaron por última vez esos objetos (se leyeron o vieron).

Por ejemplo, para asegurarse de que los objetos que se ven recientemente permanecen en un almacenamiento más rápido, el administrador de grid puede crear una regla de ILM que especifique lo siguiente:

- Los objetos que se han recuperado durante el último mes deben permanecer en los nodos de almacenamiento local.
- Los objetos que no se han recuperado en el último mes deben moverse a una ubicación externa.

De forma predeterminada, las actualizaciones de la hora del último acceso están desactivadas. Si su sistema StorageGRID incluye una regla de ILM que utiliza la opción **last access time** y desea que esta opción se aplique a los objetos de este depósito, debe habilitar las actualizaciones a la última hora de acceso para los S3 buckets especificados en esa regla.

La actualización del último tiempo de acceso cuando se recupera un objeto puede reducir el rendimiento de la StorageGRID, especialmente en objetos pequeños.

El impacto en el rendimiento se produce con las actualizaciones del último tiempo de acceso porque StorageGRID debe realizar estos pasos adicionales cada vez que se recuperan los objetos:

- Actualice los objetos con nuevas marcas de tiempo

- Añada los objetos a la cola de ILM para poder reevaluarlos según las reglas y políticas actuales de ILM

La tabla resume el comportamiento aplicado a todos los objetos del bloque cuando la hora de último acceso está desactivada o habilitada.

Tipo de solicitud	Comportamiento si la hora del último acceso está desactivada (valor predeterminado)		Comportamiento si la hora del último acceso está activada	
	¿Hora de último acceso actualizada?	¿Objeto añadido a la cola de evaluación de ILM?	¿Hora de último acceso actualizada?	¿Objeto añadido a la cola de evaluación de ILM?
Solicitud para recuperar un objeto, su lista de control de acceso o sus metadatos	No	No	Sí	Sí
Solicitud para actualizar los metadatos de un objeto	Sí	Sí	Sí	Sí
Solicite copiar un objeto de un bloque a otro	• No, para la copia de origen • Sí, para la copia de destino	• No, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino	• Sí, para la copia de origen • Sí, para la copia de destino
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
2. Seleccione el nombre del cubo de la tabla.

   Aparece la página de detalles bucket.

3. En la pestaña **Opciones de cubo**, selecciona el acordeón **Últimas actualizaciones de hora de acceso**.
4. Activar o desactivar las actualizaciones de hora del último acceso.
5. Seleccione **Guardar cambios**.

Cambiar el control de versiones del objeto para un bloque

Si utiliza un inquilino S3, puede cambiar el estado de control de versiones de los bloques S3.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.
- Todos los nodos de almacenamiento están disponibles.

Acerca de esta tarea

Puede habilitar o suspender el control de versiones de objetos de un bloque. Después de activar el control de versiones para un depósito, no puede volver a un estado sin versiones. Sin embargo, puede suspender el control de versiones del bloque.

- Desactivado: El control de versiones no se ha activado nunca
- Activado: El control de versiones está activado
- Suspendido: El control de versiones se ha habilitado anteriormente y se ha suspendido

Para obtener más información, consulte lo siguiente:

- "Control de versiones de objetos"
- "Reglas de ILM y políticas para objetos con versiones de S3 (ejemplo 4)"
- "Cómo se eliminan los objetos"

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
2. Seleccione el nombre del cubo de la tabla.

   Aparece la página de detalles bucket.

3. Desde la pestaña **Opciones de cubo**, selecciona el acordeón **Control de versiones de objeto**.
4. Seleccione un estado de control de versiones para los objetos de este bloque.

   El control de versiones de objetos debe permanecer habilitado para un bucket que se utiliza para la replicación entre grid. Si se habilita el bloqueo de objetos S3 o la compatibilidad con versiones heredadas, se desactivarán las opciones **versiones de objetos**.

Opción	Descripción
Habilite el control de versiones	Habilite el control de versiones de objetos si desea almacenar cada versión de cada objeto en este bloque. A continuación, puede recuperar versiones anteriores de un objeto según sea necesario. Los objetos que ya estaban en el bloque se versionarán cuando los modifique un usuario.
Suspender las versiones	Suspenda el control de versiones de objetos si ya no desea crear nuevas versiones de objetos. Aún puede recuperar cualquier versión de objeto existente.

5. Seleccione **Guardar cambios**.

Utilice Bloqueo de objetos S3 para retener objetos

Puede utilizar S3 Object Lock si los cubos y los objetos deben cumplir con los requisitos normativos de retención.

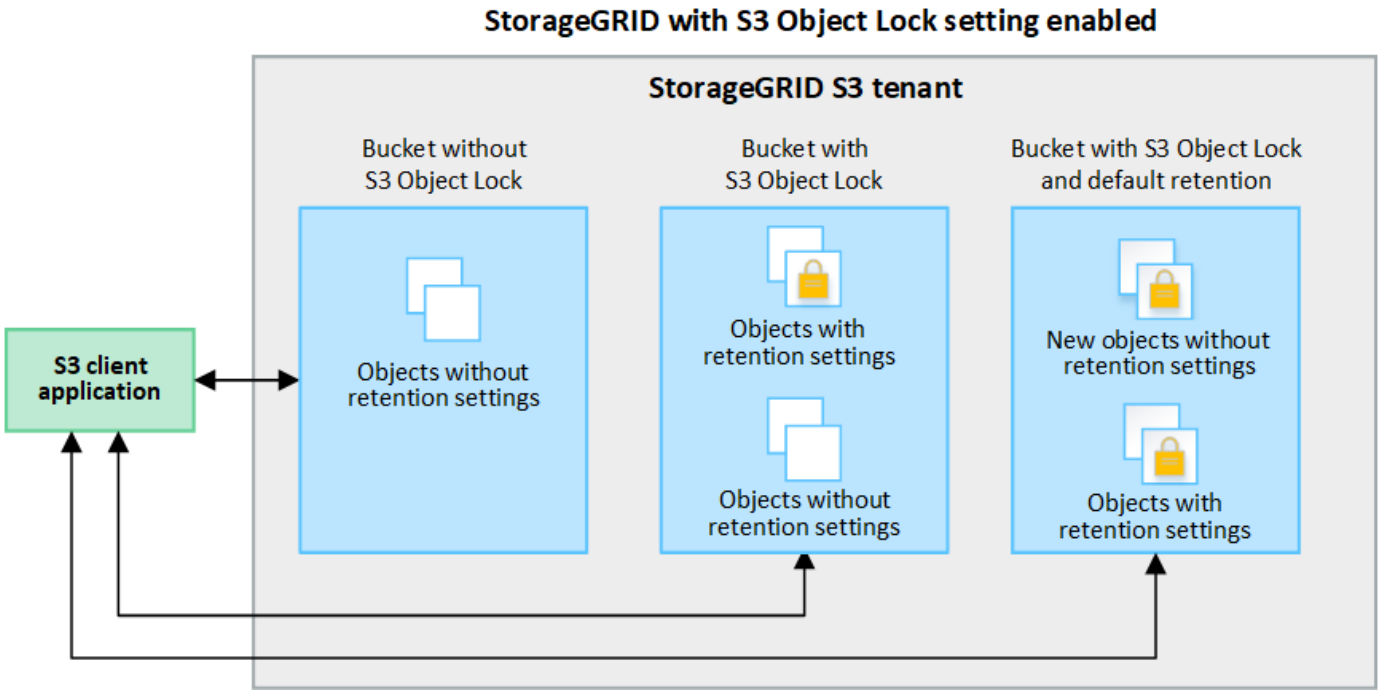
¿Qué es el bloqueo de objetos de S3?

La función StorageGRID S3 Object Lock es una solución de protección de objetos equivalente a S3 Object Lock en Amazon simple Storage Service (Amazon S3).

Tal y como se muestra en la figura, cuando se habilita la opción global de bloqueo de objetos de S3 para un sistema StorageGRID, una cuenta de inquilino de S3 puede crear bloques con o sin la función de bloqueo de objetos de S3 habilitada. Si un bucket tiene S3 Object Lock habilitado, se requiere el control de versiones de bucket y se habilita automáticamente.

Si un bucket tiene S3 Object Lock habilitado, las aplicaciones cliente S3 pueden especificar, de manera opcional, la configuración de retención para cualquier versión de objeto guardada en ese bucket.

Además, un bloque que tiene S3 Object Lock habilitado puede tener opcionalmente un modo de retención y un período de retención predeterminados. La configuración predeterminada se aplica solo a los objetos que se agregan al depósito sin su propia configuración de retención.



Modos de retención

La función de bloqueo de objetos StorageGRID S3 admite dos modos de retención para aplicar diferentes niveles de protección a los objetos. Estos modos son equivalentes a los modos de retención de Amazon S3.

- En modo de cumplimiento:
  - El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta.
  - La fecha de retención del objeto se puede aumentar, pero no se puede reducir.
  - No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha.

- En modo de gobierno:
  - Los usuarios con permiso especial pueden utilizar un encabezado de omisión en las solicitudes para modificar ciertos valores de retención.
  - Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha.
  - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

Configuración de retención para versiones de objetos

Si se crea un depósito con S3 Object Lock habilitado, los usuarios pueden utilizar la aplicación cliente S3 para especificar opcionalmente los siguientes valores de retención para cada objeto que se agregue al depósito:

- **Modo de retención**: Ya sea cumplimiento o gobierno.
- **Retain-until-date**: Si la fecha de retención de una versión de objeto está en el futuro, el objeto se puede recuperar, pero no se puede eliminar.
- **Retención legal**: La aplicación de una retención legal a una versión de objeto bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesite poner una retención legal en un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, pero permanece en su lugar hasta que se elimina explícitamente. La retención legal es independiente de la retención hasta la fecha.

  > Si un objeto se encuentra bajo una conservación legal, nadie puede eliminarlo, independientemente de su modo de retención.

  Para obtener más información sobre la configuración del objeto, consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3".

Valor de retención predeterminado para los depósitos

Si se crea un depósito con S3 Object Lock habilitado, los usuarios pueden especificar opcionalmente los siguientes ajustes predeterminados para el bloque:

- **Modo de retención predeterminado**: Ya sea cumplimiento o gobierno.
- **Período de retención predeterminado**: Cuánto tiempo deben conservarse las nuevas versiones de objetos añadidas a este depósito, a partir del día en que se agregan.

La configuración de bloque predeterminada se aplica solo a objetos nuevos que no tienen su propia configuración de retención. Los objetos de cubo existentes no se ven afectados al agregar o cambiar estos valores predeterminados.

Consulte "Cree un bloque de S3" y.. "Actualizar S3 Retención predeterminada de bloqueo de objetos".

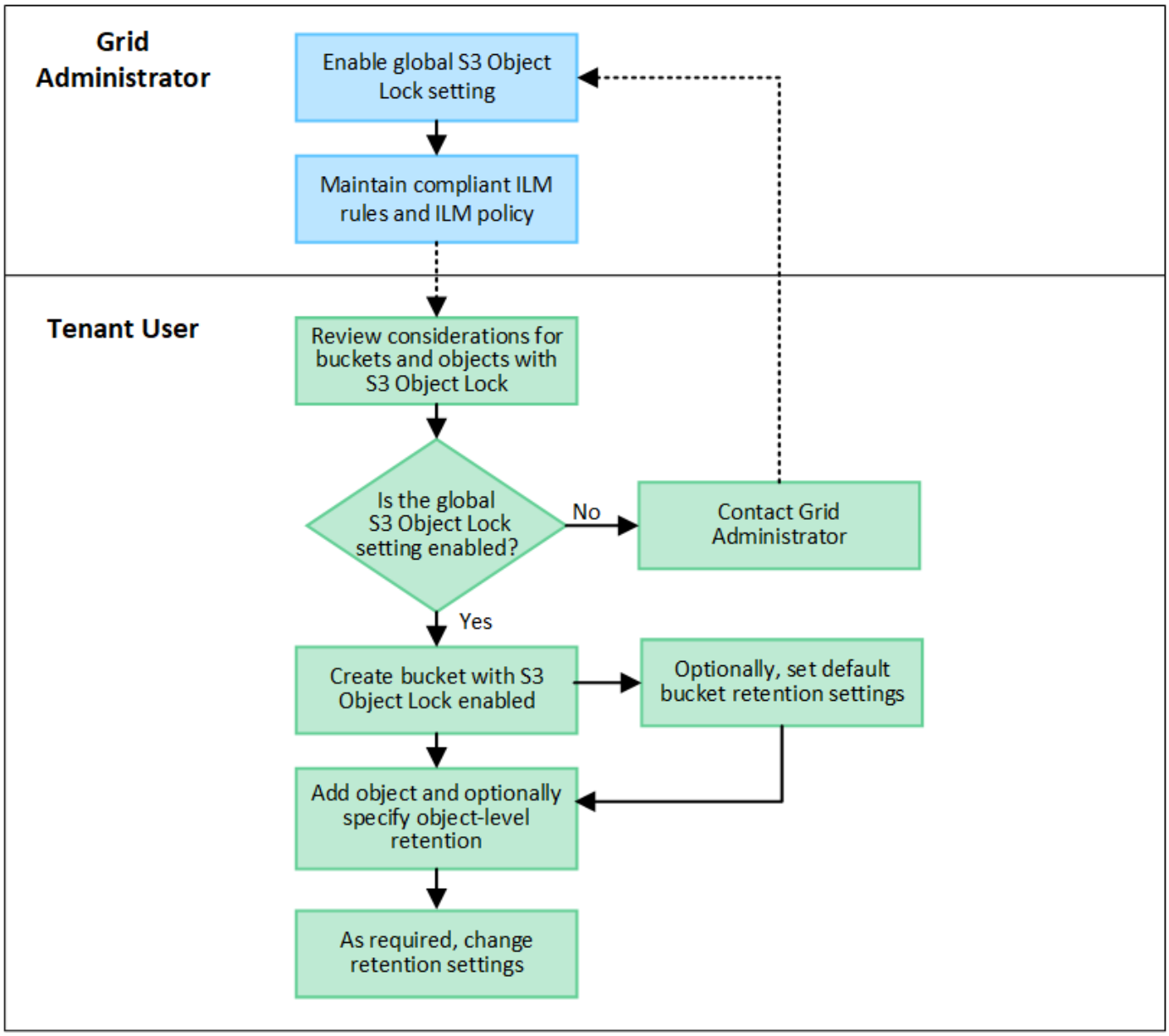
Flujo de trabajo de bloqueo de objetos de S3

En el diagrama de flujo de trabajo, se muestran los pasos de alto nivel para usar la función de bloqueo de objetos de S3 en StorageGRID.

Para poder crear bloques con el bloqueo de objetos S3 habilitado, el administrador de grid debe habilitar el valor global de bloqueo de objetos S3 para todo el sistema StorageGRID. El administrador de grid también debe asegurarse de que la política de gestión del ciclo de vida de la información (ILM) sea conforme; debe cumplir los requisitos de los buckets con bloqueo de objetos S3 habilitado. Para obtener más información,

póngase en contacto con el administrador de grid o consulte las instrucciones para "Gestionar objetos con S3 Object Lock".

Después de habilitar la configuración global S3 Object Lock, puede crear buckets con S3 Object Lock habilitado y, opcionalmente, especificar la configuración de retención predeterminada para cada bucket. Además, puede utilizar la aplicación cliente S3 para especificar opcionalmente la configuración de retención para cada versión de objeto.



Requisitos para bloques con bloqueo de objetos de S3 habilitado

- Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, puede usar el administrador de inquilinos, la API de gestión de inquilinos o la API REST de S3 para crear bloques con el bloqueo de objetos S3 habilitado.
- Si planea utilizar el bloqueo de objetos S3, debe habilitar el bloqueo de objetos S3 al crear el bloque. No puede activar el bloqueo de objetos S3 para un depósito existente.
- Cuando se habilita el bloqueo de objetos S3 para un bloque, StorageGRID habilita automáticamente el control de versiones para ese bloque. No puede desactivar el bloqueo de objetos de S3 ni suspender el control de versiones del depósito.

- De manera opcional, puede especificar un modo de retención y un período de retención predeterminados para cada bloque mediante el administrador de inquilinos, la API de gestión de inquilinos o la API DE REST S3. La configuración de retención predeterminada del depósito se aplica solo a los nuevos objetos agregados al depósito que no tienen su propia configuración de retención. Puede anular esta configuración predeterminada especificando un modo de retención y Retain-until-date para cada versión del objeto cuando se cargue.
- Se admite la configuración de ciclo de vida de bloques para los bloques con S3 Object Lock habilitado.
- La replicación de CloudMirror no es compatible para bloques con el bloqueo de objetos S3 habilitado.

Requisitos para objetos en bloques con S3 Object Lock habilitado

- Para proteger una versión de objeto, puede especificar la configuración de retención predeterminada para el bloque, o bien puede especificar la configuración de retención para cada versión de objeto. La configuración de retención a nivel de objeto se puede especificar mediante la aplicación cliente S3 o la API DE REST S3.
- La configuración de retención se aplica a versiones individuales de objetos. Una versión de objeto puede tener una configuración de retención hasta fecha y una retención legal, una pero no la otra, o ninguna. Al especificar una configuración de retención hasta fecha o de retención legal para un objeto, sólo se protege la versión especificada en la solicitud. Puede crear nuevas versiones del objeto, mientras que la versión anterior del objeto permanece bloqueada.

Ciclo de vida de los objetos en bloques con S3 Object Lock habilitado

Cada objeto que se guarda en un depósito con S3 Object Lock habilitado pasa por las siguientes etapas:

1. **Procesamiento de objetos**

   Cuando se agrega una versión de objeto al depósito que tiene S3 Object Lock habilitado, la configuración de retención se aplica de la siguiente manera:

   - Si se especifica la configuración de retención para el objeto, se aplica la configuración de nivel de objeto. Se ignoran todos los valores predeterminados de los depósitos.
   - Si no se especifica ninguna configuración de retención para el objeto, se aplica la configuración de bloque predeterminada, si existe.
   - Si no se especifica ninguna configuración de retención para el objeto o el depósito, el objeto no está protegido por S3 Object Lock.

   Si se aplica una configuración de retención, tanto el objeto como cualquier metadatos definidos por el usuario S3 se protegen.

2. **Retención y eliminación de objetos**

   StorageGRID almacena varias copias de cada objeto protegido durante el período de retención especificado. El número y el tipo exactos de copias de objetos y las ubicaciones de almacenamiento están determinados por las reglas conformes a la normativa de las políticas de ILM activas. Si se puede eliminar un objeto protegido antes de alcanzar su fecha de retención hasta la fecha, depende de su modo de retención.

   - Si un objeto se encuentra bajo una conservación legal, nadie puede eliminarlo, independientemente de su modo de retención.

¿Puedo seguir gestionando los depósitos compatibles heredados?

La función de bloqueo de objetos S3 sustituye la función Compliance disponible en versiones anteriores de StorageGRID. Si ha creado cubos compatibles con una versión anterior de StorageGRID, puede seguir gestionando la configuración de estos bloques; sin embargo, ya no puede crear nuevos bloques compatibles. Para ver instrucciones, consulte "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5".

Actualizar S3 Retención predeterminada de bloqueo de objetos

Si habilitó S3 Object Lock al crear el bucket, puede editar el bucket para cambiar la configuración de retención predeterminada. Puede habilitar (o deshabilitar) la retención predeterminada y establecer un modo de retención y un período de retención predeterminados.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.
- S3 Bloqueo de objetos está habilitado globalmente para su sistema StorageGRID, y usted habilitó S3 Bloqueo de objetos al crear el bucket. Consulte "Utilice Bloqueo de objetos S3 para retener objetos".

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
2. Seleccione el nombre del cubo de la tabla.

   Aparece la página de detalles bucket.

3. En la pestaña **Opciones de cubo**, selecciona el acordeón **S3 Object Lock**.
4. Opcionalmente, habilita o deshabilita **Retención predeterminada** para este depósito.

   Los cambios realizados en esta configuración no se aplican a objetos que ya estén en el depósito ni a objetos que puedan tener sus propios períodos de retención.

5. Si **Retención predeterminada** está habilitada, especifique un **Modo de retención predeterminado** para el depósito.

Modo de retención predeterminado	Descripción
Cumplimiento de normativas	• El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta. • La fecha de retención del objeto se puede aumentar, pero no se puede reducir. • No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha.

Modo de retención predeterminado	Descripción
Gobernanza	• Usuarios con `s3:BypassGovernanceRetention` el permiso puede utilizar el `x-amz-bypass-governance-retention: true` solicitar cabecera para omitir la configuración de retención. • Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha. • Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

6. Si **Retención predeterminada** está habilitada, especifique el **Período de retención predeterminado** para el depósito.

   El **período de retención predeterminado** indica cuánto tiempo deben conservarse los nuevos objetos agregados a este depósito, a partir del momento en que se ingieren. Especifique un valor entre 1 y 36.500 días o entre 1 y 100 años, ambos incluidos.

7. Seleccione **Guardar cambios**.

Configurar el uso compartido de recursos de origen cruzado (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un depósito de S3 si desea que las aplicaciones web de otros dominios puedan acceder a ese depósito y a los objetos de ese depósito.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

Acerca de esta tarea

El uso compartido de recursos de origen cruzado (CORS) es un mecanismo de seguridad que permite a las aplicaciones web de cliente de un dominio acceder a los recursos de un dominio diferente. Por ejemplo, supongamos que se utiliza un bloque de S3 llamado `Images` para almacenar gráficos. Configurando CORS para `Images` bloque, puede permitir que las imágenes de ese bloque se muestren en el sitio web `http://www.example.com`.

Activar CORS para un cucharón

Pasos

1. Utilice un editor de texto para crear el XML necesario.

   Este ejemplo muestra el XML utilizado para habilitar CORS para un bloque de S3. Este XML permite a cualquier dominio enviar solicitudes GET al bloque, pero sólo permite el `http://www.example.com` Dominio para enviar solicitudes DE PUBLICACIÓN Y ELIMINACIÓN. Se permiten todos los encabezados de las solicitudes.

```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

Para obtener más información acerca del XML de configuración de CORS, consulte "Documentación de Amazon Web Services (AWS): Guía para desarrolladores de Amazon simple Storage Service".

2. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
3. Seleccione el nombre del cubo de la tabla.

   Aparece la página de detalles bucket.

4. En la pestaña **Acceso a cubos**, selecciona el acordeón **Uso compartido de recursos de origen cruzado (CORS)**.
5. Seleccione la casilla de verificación **Activar CORS**.
6. Pegue el XML de configuración de CORS en el cuadro de texto.
7. Seleccione **Guardar cambios**.

Modificar el ajuste de CORS

Pasos

1. Actualice el XML de configuración de CORS en el cuadro de texto, o seleccione **Borrar** para empezar de nuevo.
2. Seleccione **Guardar cambios**.

Desactive el ajuste CORS

Pasos

1. Desactive la casilla de verificación **Activar CORS**.
2. Seleccione **Guardar cambios**.

Suprimir objetos del depósito

Puede utilizar el gestor de inquilinos para suprimir los objetos de uno o más depósitos.

Consideraciones y requisitos

Antes de realizar estos pasos, tenga en cuenta lo siguiente:

- Cuando elimina los objetos de un depósito, StorageGRID elimina de forma permanente todos los objetos y todas las versiones de objetos de cada bloque seleccionado de todos los nodos y sitios del sistema StorageGRID. StorageGRID también quita todos los metadatos de objetos relacionados. No podrá recuperar esta información.
- La eliminación de todos los objetos de un bloque puede demorar minutos, días o incluso semanas, según el número de objetos, copias de objetos y operaciones simultáneas.
- Si un cucharón tiene "S3 Bloqueo de objetos activado", Puede permanecer en el estado **Deleting objects: Read-only** para *Years*.

> Un depósito que utiliza S3 Object Lock permanecerá en el estado **Deleting objects: Read-only** hasta que se alcance la fecha de retención para todos los objetos y se eliminen las retenciones legales.

- Mientras los objetos se eliminan, el estado del depósito es **Eliminando objetos: Solo lectura**. En este estado, no puede agregar nuevos objetos al depósito.
- Cuando todos los objetos se han eliminado, el bloque permanece en su estado de solo lectura. Puede realizar una de las siguientes acciones:
  - Vuelva a colocar el depósito en modo de escritura y reutilícelo para objetos nuevos
  - Elimine el cucharón
  - Mantenga el bucket en modo de solo lectura para reservar su nombre para uso futuro
- Si un bloque tiene el control de versiones de objetos activado, los marcadores de eliminación que se crearon en StorageGRID 11,8 o posterior se pueden eliminar mediante la eliminación de objetos en las operaciones de bloque.
- Si un bloque tiene el control de versiones de objetos activado, la operación de supresión de objetos no eliminará los marcadores de supresión creados en StorageGRID 11,7 o anteriores. Consulte la información sobre la eliminación de objetos en un depósito en "Cómo se eliminan los objetos con versiones de S3".
- Si utiliza "replicación entre grid", tenga en cuenta lo siguiente:
  - El uso de esta opción no elimina ningún objeto del depósito en la otra cuadrícula.
  - Si selecciona esta opción para el depósito de origen, se activará la alerta **Fallo de replicación entre redes** si agrega objetos al depósito de destino en la otra cuadrícula. Si no puede garantizar que nadie agregará objetos al depósito de la otra cuadrícula, "desactive la replicación entre grid" para ese depósito antes de eliminar todos los objetos de cubo.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz". Este permiso anula la configuración de permisos en las políticas de grupo o bloque.

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.

   Aparece la página Buckets y muestra todos los bloques S3 existentes.

2. Utilice el menú **Acciones** o la página de detalles de un cubo específico.

Menú Actions

a. Seleccione la casilla de comprobación de cada bloque desde el que desea eliminar objetos.

b. Selecciona **Acciones** > **Eliminar objetos en el cubo**.

Detalles

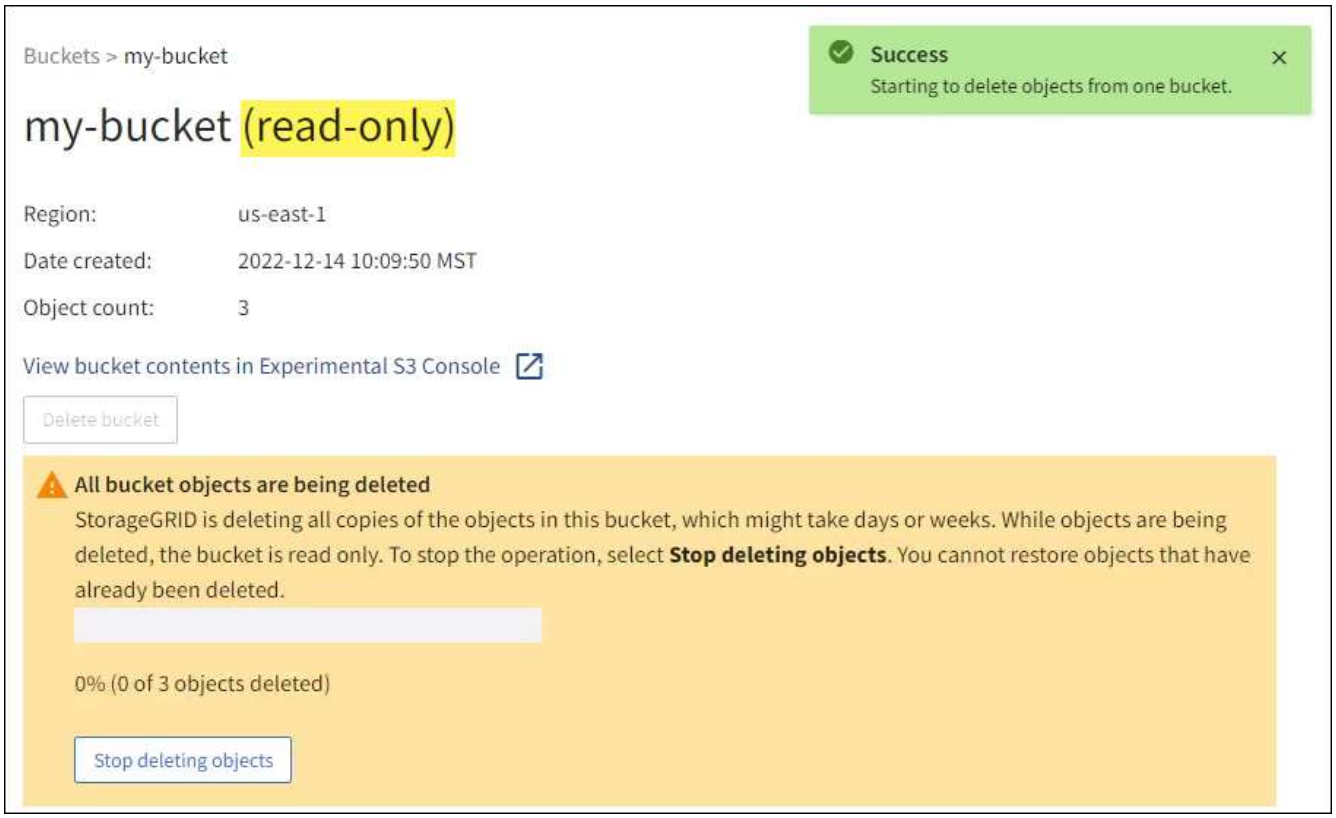
a. Seleccione un nombre de cubo para mostrar sus detalles.

b. Seleccione **Eliminar objetos en el cubo**.

3. Cuando aparezca el cuadro de diálogo de confirmación, revise los detalles, introduzca **Sí** y seleccione **Aceptar**.
4. Espere a que comience la operación de eliminación.

   Después de unos minutos:

   - Aparece un banner de estado amarillo en la página de detalles del depósito. La barra de progreso representa el porcentaje de objetos que se han suprimido.
   - **(solo lectura)** aparece después del nombre del cubo en la página de detalles del cubo.
   - **(Eliminación de objetos: Solo lectura)** aparece junto al nombre del cubo en la página Buckets.

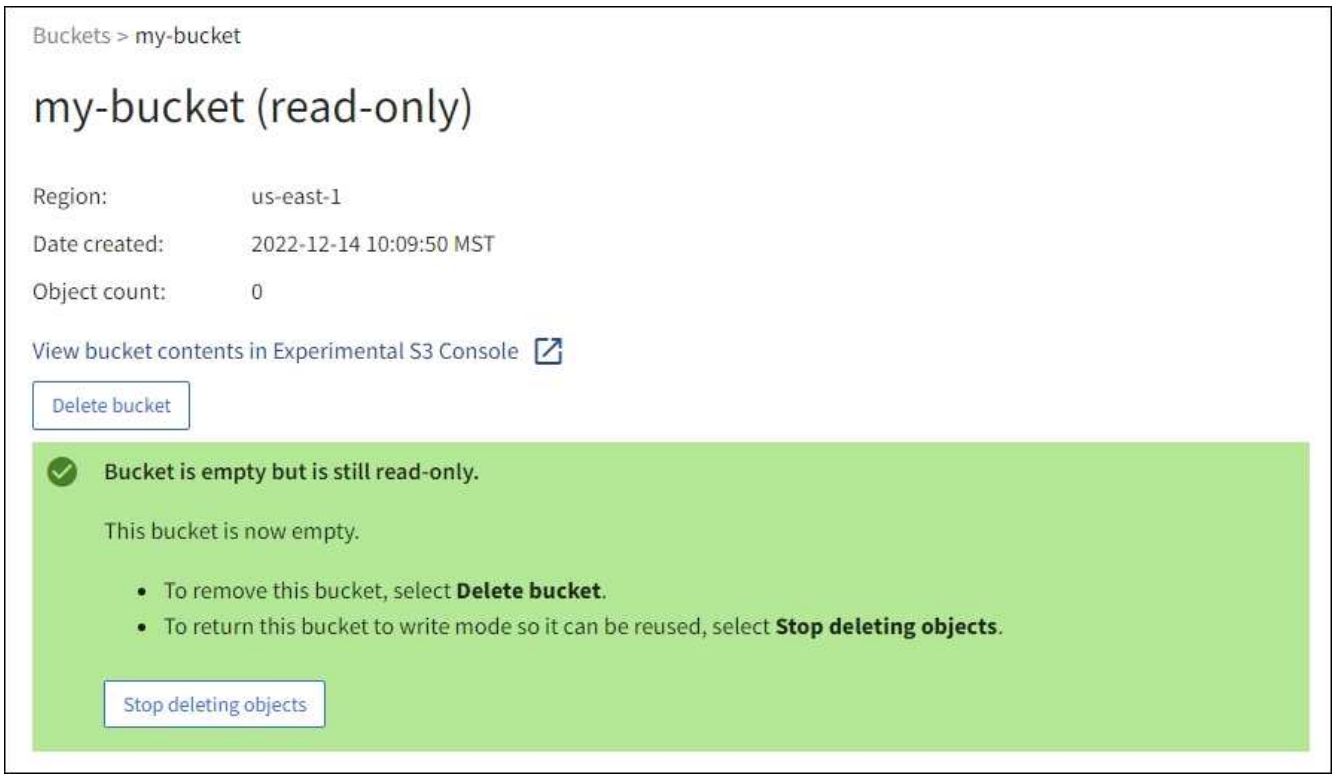


5. Según sea necesario mientras se ejecuta la operación, seleccione **Detener eliminación de objetos** para detener el proceso. Luego, opcionalmente, seleccione **Eliminar objetos en el cubo** para reanudar el proceso.

   Cuando selecciona **Dejar de eliminar objetos**, el depósito vuelve al modo de escritura; sin embargo, no puede acceder ni restaurar ningún objeto que se haya eliminado.

6. Espere a que se complete la operación.

   Cuando el depósito está vacío, se actualiza el banner de estado, pero el depósito permanece como de sólo lectura.



7. Debe realizar una de las siguientes acciones:
   - Salga de la página para mantener el depósito en modo de sólo lectura. Por ejemplo, puede mantener un depósito vacío en modo de solo lectura para reservar el nombre del depósito para uso futuro.
   - Eliminar el bloque. Puede seleccionar **Eliminar cubo** para eliminar un solo cubo o devolver la página Buckets y seleccionar **Acciones** > **Eliminar** cubos para eliminar más de un cubo.

     Si no puede suprimir un depósito con versiones después de eliminar todos los objetos, puede que permanezcan los marcadores de supresión. Para eliminar el cucharón, debe eliminar todos los marcadores de borrado restantes.

   - Vuelva a colocar el depósito en modo de escritura y, opcionalmente, reutilícelo para objetos nuevos. Puede seleccionar **Dejar de eliminar objetos** para un solo depósito o volver a la página Buckets y seleccionar **Acción** > **Dejar de eliminar objetos** para más de un depósito.

Eliminar bloque de S3

Puede usar el administrador de inquilinos para eliminar uno o varios bloques de S3 vacíos.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

- Los cucharones que desea eliminar están vacíos. Si los depósitos que desea suprimir están *NOT* vacíos, "suprimir objetos del depósito".

Acerca de esta tarea

Estas instrucciones describen cómo eliminar un bloque de S3 mediante el administrador de inquilinos. También se pueden eliminar bloques de S3 con el "API de gestión de inquilinos" o la "API REST DE S3".

No se puede eliminar un bucket de S3 si contiene objetos, versiones de objetos no actuales o marcadores de eliminación. Para obtener más información sobre cómo se eliminan los objetos con versiones S3, consulte "Cómo se eliminan los objetos".

Pasos

1. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.

   Aparece la página Buckets y muestra todos los bloques S3 existentes.

2. Utilice el menú **Acciones** o la página de detalles de un cubo específico.

   Menú Actions

   a. Seleccione la casilla de verificación de cada bloque que desee eliminar.

   b. Selecciona **Acciones** > **Eliminar cubos**.

   Detalles

   a. Seleccione un nombre de cubo para mostrar sus detalles.

   b. Seleccione **Eliminar cubo**.

3. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí**.

   StorageGRID confirma que cada cucharón está vacío y, a continuación, elimina cada cucharón. Esta operación puede llevar algunos minutos.

   Si un segmento no está vacío, aparece un mensaje de error. Debe "elimine todos los objetos y cualquier marcador de borrado del depósito" antes de poder eliminar el depósito.

Utilice la consola S3

Puede utilizar S3 Console para ver y gestionar los objetos de un bucket de S3.

La consola S3 le permite:

- Cargar, descargar, renombrar, copiar, mover, y eliminar objetos
- Vea, revierta, descargue y elimine versiones de objetos
- Buscar objetos por prefijo
- Administrar etiquetas de objetos
- Ver los metadatos de objetos
- Ver, crear, cambiar nombre, copiar, mover, y elimine carpetas

S3 Console proporciona una experiencia de usuario mejorada para los casos más comunes. No está diseñado para sustituir las operaciones de la CLI o la API en todas las situaciones.

Si el uso de S3 Console provoca operaciones que tardan demasiado (por ejemplo, minutos u horas), considere:

- Reducción del número de objetos seleccionados
- Uso de métodos no gráficos (API o CLI) para acceder a los datos

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Si desea gestionar objetos, pertenece a un grupo de usuarios que tiene el permiso de acceso root. Como alternativa, pertenece a un grupo de usuarios que tiene el permiso Usar la pestaña Consola de S3 y el permiso Ver todos los cubos o Gestionar todos los cubos. Consulte "Permisos de gestión de inquilinos".
- Se ha configurado una política de grupo o bloque S3 para el usuario. Consulte "Utilice las políticas de acceso de bloques y grupos".
- Conoce el ID de clave de acceso del usuario y la clave de acceso secreta. Opcionalmente, usted tiene un `.csv` archivo que contiene esta información. Consulte "instrucciones para crear claves de acceso".

Pasos

1. Seleccione **STORAGE** > **Buckets** > ***bucket name***.
2. Seleccione la ficha Consola de S3.
3. Pegue el ID de clave de acceso y la clave de acceso secreta en los campos. De lo contrario, seleccione **cargar teclas de acceso** y seleccione el `.csv` archivo.
4. Seleccione **Iniciar sesión**.
5. Aparece la tabla de objetos de cubo. Puede gestionar objetos según sea necesario.

Información adicional

- **Buscar por prefijo**: La función de búsqueda de prefijo solo busca objetos que comiencen con una palabra específica relativa a la carpeta actual. La búsqueda no incluye objetos que contengan la palabra en otro lugar. Esta regla también se aplica a los objetos dentro de las carpetas. Por ejemplo, una búsqueda de `folder1/folder2/somefile-` devolvería objetos que se encuentran dentro de `folder1/folder2/` y empezar con la palabra `somefile-`.
- * Arrastre y suelte *: Puede arrastrar y soltar archivos desde el administrador de archivos de su computadora a S3 Console. Sin embargo, no puede cargar carpetas.
- **Operaciones en carpetas**: Cuando se mueve, copia o cambia el nombre de una carpeta, todos los objetos de la carpeta se actualizan de uno en uno, lo que puede llevar tiempo.
- **Eliminación permanente cuando el control de versiones del bucket está desactivado**: Cuando sobrescribe o elimina un objeto en un bucket con el control de versiones desactivado, la operación es permanente. Consulte "Cambiar el control de versiones del objeto para un bloque".

Gestione servicios de plataformas S3

Administrar servicios de plataforma: Descripción general

Los servicios de plataforma de StorageGRID pueden ayudarte a implementar una estrategia de cloud híbrido permitiéndote enviar notificaciones de eventos y copias de

objetos S3 y metadatos de objetos a destinos externos.

Si se permite el uso de servicios de plataforma para su cuenta de inquilino, puede configurar los siguientes servicios para cualquier bloque de S3:

Replicación de CloudMirror

Uso "Servicio de replicación CloudMirror de StorageGRID" Para reflejar objetos específicos de un bloque de StorageGRID en un destino externo especificado.

Por ejemplo, podría usar la replicación de CloudMirror para reflejar registros de clientes específicos en Amazon S3 y, a continuación, aprovechar los servicios de AWS para realizar análisis de los datos.

> La replicación de CloudMirror no es compatible si el bloque de origen tiene la función S3 Object Lock habilitada.

Notificaciones

Uso "notificaciones de eventos por bloque" Para enviar notificaciones sobre acciones específicas realizadas en objetos a un Amazon Simple Notification Service (Amazon SNS) externo especificado.

Por ejemplo, podría configurar que se envíen alertas a administradores acerca de cada objeto agregado a un bloque, donde los objetos representan los archivos de registro asociados a un evento crítico del sistema.

> Aunque la notificación de eventos se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos S3 (incluido el estado retener hasta fecha y retención legal) de los objetos no se incluirán en los mensajes de notificación.

Servicio de integración de búsqueda

Utilice la "servicio de integración de búsqueda" Para enviar metadatos de objetos S3 a un índice de Elasticsearch especificado donde se pueden buscar o analizar los metadatos mediante un servicio externo.

Por ejemplo, podría configurar sus bloques para que envíen metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, podría usar Elasticsearch para realizar búsquedas en los bloques y ejecutar análisis sofisticados de los patrones presentes en los metadatos de objetos.

> Aunque la integración de Elasticsearch se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos de S3 (incluidos los Estados Retain Until Date and Legal Hold) de los objetos no se incluirán en los mensajes de notificación.

Puesto que la ubicación objetivo de los servicios de la plataforma suele ser externa a la puesta en marcha de StorageGRID, los servicios de plataforma le proporcionan la potencia y la flexibilidad que se obtiene al utilizar recursos de almacenamiento externo, servicios de notificación y servicios de búsqueda o análisis para sus datos.

Se puede configurar cualquier combinación de servicios de plataforma para un único bloque de S3. Por ejemplo, podría configurar el servicio CloudMirror y las notificaciones en un bloque de StorageGRID S3 de manera que pueda reflejar objetos específicos en Amazon simple Storage Service, al tiempo que envía una notificación sobre cada objeto de ese tipo a una aplicación de supervisión de terceros para ayudarle a realizar un seguimiento de los gastos de AWS.

Un administrador de StorageGRID debe habilitar el uso de servicios de plataforma para cada cuenta de inquilino mediante el Administrador de grid o la API de gestión de grid.

Cómo se configuran los servicios de plataforma

Los servicios de plataforma se comunican con los puntos finales externos que configure mediante "Administrador de inquilinos" o la "API de gestión de inquilinos". Cada extremo representa un destino externo, como un bloque de S3 de StorageGRID, un bloque de Amazon Web Services, un tema de Amazon SNS o un clúster de Elasticsearch alojado localmente, en AWS o en otro lugar.

Después de crear un punto final externo, puede activar un servicio de plataforma para un bloque agregando configuración XML al bloque. La configuración XML identifica los objetos en los que debe actuar el bloque, la acción que debe tomar el bloque y el extremo que el bloque debe utilizar para el servicio.

Debe agregar configuraciones XML independientes para cada servicio de plataforma que desee configurar. Por ejemplo:

- Si desea que todos los objetos con las claves comiencen `/images` Para replicarse en un bloque de Amazon S3, debe añadir una configuración de replicación al bloque de origen.
- Si también desea enviar notificaciones cuando estos objetos están almacenados en el bloque, debe añadir una configuración de notificaciones.
- Por último, si desea indexar los metadatos de estos objetos, debe agregar la configuración de notificación de metadatos que se utiliza para implementar la integración de búsquedas.

El formato de la configuración XML está regido por las API DE REST de S3 que se usan para implementar los servicios de plataforma StorageGRID:

Servicio de plataforma	API REST DE S3	Consulte
Replicación de CloudMirror	• GetBucketReplication • PutBucketReplication	• "Replicación de CloudMirror" • "Operaciones en bloques"
Notificaciones	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "Notificaciones" • "Operaciones en bloques"
Integración de búsqueda	• OBTENGA la configuración de notificación de metadatos del bloque de datos • Configuración de notificaciones de metadatos de PUT Bucket	• "Integración de búsqueda" • "Operaciones personalizadas de StorageGRID"

Información relacionada

"Consideraciones sobre los servicios de plataforma"

Puede habilitar la replicación de CloudMirror para un bloque de S3 si desea que StorageGRID replique los objetos especificados que se añadan al bloque en uno o más bloques de destino.

La replicación de CloudMirror funciona independientemente de las políticas de gestión de la vida útil de la información activas del grid. El servicio CloudMirror replica los objetos cuando se almacenan en el bloque de origen y los envía al Lo antes posible. de bloque de destino. La entrega de objetos replicados se activa cuando la ingesta de objetos se realiza correctamente.

> La replicación de CloudMirror tiene similitudes y diferencias importantes con la función de replicación entre grid. Para obtener más información, consulte "Compare la replicación entre grid y la replicación de CloudMirror".

Si habilita la replicación de CloudMirror para un bloque existente, solo se replican los nuevos objetos agregados a ese bloque. Todos los objetos existentes del bloque no se replican. Para forzar la replicación de objetos existentes, puede actualizar los metadatos del objeto existente ejecutando una copia de objeto.

> Si utiliza la replicación de CloudMirror para copiar objetos a un destino de Amazon S3, tenga en cuenta que Amazon S3 limita el tamaño de los metadatos definidos por el usuario dentro de cada encabezado de solicitud PUT a 2 KB. Si un objeto tiene metadatos definidos por el usuario mayores de 2 KB, ese objeto no se replicará.

En StorageGRID, puede replicar los objetos de un solo bloque en varios bloques de destino. Para ello, especifique el destino de cada regla en el XML de configuración de replicación. No puede replicar un objeto en más de un bloque a la vez.

Además, puede configurar la replicación de CloudMirror en bloques con versiones o sin versiones, y puede especificar un bloque con versiones o sin versiones como destino. Puede utilizar cualquier combinación de cubos con versiones y sin versiones. Por ejemplo, puede especificar un bloque con versiones como destino para un bloque de origen sin versiones o viceversa. También puede replicar entre cubos sin versiones.

El comportamiento de eliminación del servicio de replicación CloudMirror es el mismo que el comportamiento de eliminación del servicio de replicación entre regiones (CRR) proporcionado por Amazon S3 — al eliminar un objeto de un bloque de origen nunca se elimina un objeto replicado en el destino. Si se van a crear versiones de los cubos de origen y de destino, se replica el marcador de borrado. Si el bloque de destino no tiene versiones, al eliminar un objeto del bloque de origen no se replicará el marcador DELETE en el bloque de destino ni se eliminará el objeto de destino.

A medida que los objetos se replican en el bloque de destino, StorageGRID los marca como «réplicas». Un bucket de StorageGRID de destino no replicará objetos marcados como réplicas de nuevo, lo que le protegerá de bucles de replicación accidentales. Este marcado de réplica es interno en StorageGRID y no le impide utilizar AWS CRR cuando se utiliza un bloque de Amazon S3 como destino.

> El encabezado personalizado utilizado para marcar una réplica es `x-ntap-sg-replica`. Esta Marca evita una duplicación en cascada. StorageGRID sí admite un CloudMirror bidireccional entre dos grids.

La singularidad y el orden de los eventos en el cubo de destino no están garantizados. Puede que más de una copia idéntica de un objeto de origen se proporcione en el destino como resultado de las operaciones realizadas para garantizar un éxito en la entrega. En raras ocasiones, cuando se actualiza el mismo objeto de forma simultánea desde dos o más sitios StorageGRID distintos, es posible que la ordenación de las

operaciones en el bloque de destino no coincida con la ordenación de eventos en el bloque de origen.

La replicación de CloudMirror suele configurarse para utilizar un bloque de S3 externo como destino. Sin embargo, también puede configurar la replicación para que utilice otra implementación de StorageGRID o cualquier servicio compatible con S3.

Comprender las notificaciones para bloques

Puede habilitar la notificación de eventos para un bucket de S3 si desea que StorageGRID envíe notificaciones sobre eventos especificados a un clúster Kafka de destino o a Amazon Simple Notification Service.

Puede hacerlo "configure las notificaciones de eventos" Asociando XML de configuración de notificación a un bloque de origen. El XML de configuración de notificaciones sigue las convenciones de S3 para configurar notificaciones de buckets, con el tema Kafka o Amazon SNS de destino especificado como URN de un punto final.

Las notificaciones de eventos se crean en el bloque de origen tal y como se especifica en la configuración de notificación y se envían al destino. Si un evento asociado con un objeto se realiza correctamente, se crea una notificación sobre ese evento y se pone en cola para su entrega.

La singularidad y el orden de las notificaciones no están garantizados. Como resultado de las operaciones realizadas para garantizar el éxito en la entrega, se podría enviar más de una notificación de un evento al destino. Además, como la entrega es asíncrona, no se garantiza que la ordenación del tiempo de las notificaciones en el destino coincida con la ordenación de eventos del bloque de origen, especialmente en las operaciones que se originan en diferentes sitios de StorageGRID. Puede utilizar el `sequencer` Introduzca el mensaje de evento para determinar el orden de los eventos de un objeto determinado, como se describe en la documentación de Amazon S3.

Notificaciones y mensajes compatibles

Las notificaciones de eventos de StorageGRID siguen la API de Amazon S3 con algunas limitaciones:

- Se admiten los siguientes tipos de evento:
  - S3:ObjetoCreado:*
  - S3:ObjectCreated:Put
  - S3:ObjectCreated:Post
  - S3:ObjectCreated:Copiar
  - S3:ObjectCreated:CompleteMultipartUpload
  - S3:ObjectRemoved:*
  - S3:ObjectRemoved:Eliminar
  - S3:ObjectRemoved:DeleteMarkerCreated
  - S3:ObjectRestore:Post
- Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar, pero no incluyen algunas claves ni utilizan valores específicos para otros, como se muestra en la tabla:

Nombre de clave	Valor de StorageGRID
EventSource	`sgws:s3`
AwsRegion	no incluido
x-amz-id-2	no incluido
arn	`urn:sgws:s3:::bucket_name`

Comprender el servicio de integración de búsquedas

Puede habilitar la integración de búsqueda para un bloque de S3 si desea usar un servicio de búsqueda y análisis de datos externo para sus metadatos de objetos.

El servicio de integración de búsqueda es un servicio StorageGRID personalizado que envía de forma automática y asíncrona los metadatos de objetos de S3 a un extremo de destino cada vez que se actualiza un objeto o sus metadatos. A continuación, puede usar herramientas sofisticadas de búsqueda, análisis de datos, visualización o aprendizaje automático que proporciona el servicio de destino para buscar, analizar y obtener información de sus datos de objetos.

Puede activar el servicio de integración de búsqueda para cualquier bloque con versiones o sin versiones. La integración de búsqueda se configura asociando el XML de configuración de notificación de metadatos al bloque que especifica los objetos en los que actuar y el destino de los metadatos del objeto.

Las notificaciones se generan en forma de un documento JSON denominado con el nombre del bloque, el nombre del objeto y el ID de versión, si los hubiera. Cada notificación de metadatos contiene un conjunto estándar de metadatos del sistema para el objeto, además de todas las etiquetas del objeto y los metadatos del usuario.

> Para las etiquetas y los metadatos de usuario, StorageGRID pasa las fechas y los números a Elasticsearch como cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para interpretar estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para la asignación dinámica de campos y para asignar formatos de fecha. Debe habilitar las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Después de indexar un documento, no puede editar los tipos de campo del documento en el índice.

Las notificaciones se generan y se ponen en cola para su entrega siempre que:

- Se crea un objeto.
- Se elimina un objeto, incluso cuando se eliminan objetos como resultado del funcionamiento de la política de ILM de la cuadrícula.
- Los metadatos o las etiquetas de los objetos son añadidos, actualizados o eliminados. El conjunto completo de metadatos y etiquetas se envía siempre al momento de la actualización, no sólo los valores modificados.

Después de agregar XML de configuración de notificación de metadatos a un bloque, se envían notificaciones para los objetos nuevos que cree y para los objetos que modifique mediante la actualización de sus datos, metadatos de usuario o etiquetas. Sin embargo, no se envían notificaciones de ningún objeto que ya estuviera

en el bloque. Para garantizar que los metadatos de objeto de todos los objetos del bloque se envíen al destino, debe realizar una de las siguientes acciones:

- Configure el servicio de integración de búsqueda inmediatamente después de crear el bloque y antes de agregar ningún objeto.
- Realice una acción en todos los objetos que ya están en el bloque que activará un mensaje de notificación de metadatos que se enviará al destino.

El servicio de integración de búsqueda StorageGRID admite un clúster de Elasticsearch como destino. Al igual que con los demás servicios de plataforma, el destino se especifica en el extremo cuyo URN se utiliza en el XML de configuración del servicio. Utilice la "Herramienta de matriz de interoperabilidad de NetApp" Para determinar las versiones compatibles de Elasticsearch.

Información relacionada

"XML de configuración para la integración de búsqueda"

"Metadatos de objetos incluidos en las notificaciones de metadatos"

"JSON generado por el servicio de integración de búsqueda"

"Configure el servicio de integración de búsqueda"

Consideraciones sobre los servicios de plataforma

Antes de implementar los servicios de la plataforma, revise las recomendaciones y consideraciones sobre el uso de estos servicios.

Para obtener más información sobre S3, consulte "USE LA API DE REST DE S3".

Consideraciones sobre el uso de servicios de plataforma

Consideración	Detalles
Supervisión del extremo de destino	Debe supervisar la disponibilidad de cada extremo de destino. Si se pierde la conectividad con el extremo de destino durante un periodo de tiempo prolongado y existe una gran acumulación de solicitudes, se producirá un error en las solicitudes de cliente adicionales (como solicitudes PUT) a StorageGRID. Debe volver a intentar estas solicitudes con errores cuando se pueda acceder al extremo.

Consideración	Detalles
Limitación de punto final de destino	El software StorageGRID puede reducir las solicitudes entrantes de S3 para un bloque si la velocidad a la que se envían las solicitudes supera la velocidad a la que el extremo de destino puede recibir las solicitudes. La limitación sólo se produce cuando hay una acumulación de solicitudes que están a la espera de ser enviadas al extremo de destino. El único efecto visible es que las solicitudes entrantes de S3 tardarán más en ejecutarse. Si empieza a detectar un rendimiento significativamente más lento, debe reducir la tasa de procesamiento o utilizar un extremo con mayor capacidad. Si la acumulación de solicitudes sigue creciendo, las operaciones de S3 del cliente (como SOLICITUDES PUT) fallarán en el futuro. Las solicitudes de CloudMirror tienen más probabilidades de que se vean afectadas por el rendimiento del extremo de destino, ya que estas solicitudes suelen requerir más transferencia de datos que las solicitudes de integración de búsqueda o notificación de eventos.
Solicitud de garantías	StorageGRID garantiza la realización de pedidos de operaciones en un objeto dentro de un sitio. Siempre que todas las operaciones contra un objeto se encuentren en el mismo sitio, el estado del objeto final (para replicación) será siempre igual al estado en StorageGRID. StorageGRID hace todo un esfuerzo por intentar solicitar solicitudes cuando se realizan operaciones en todos los sitios de StorageGRID. Por ejemplo, si escribe un objeto inicialmente en el sitio A y después sobrescribe el mismo objeto en el sitio B, no se garantiza que el objeto final replicado por CloudMirror en el bloque de destino sea el más nuevo.
Eliminaciones de objetos condicionados por ILM	Para coincidir con el comportamiento de eliminación de AWS CRR y Amazon Simple Notification Service, CloudMirror y las solicitudes de notificación de eventos no se envían cuando se elimina un objeto del bloque de origen debido a las reglas de gestión de la vida útil de la información de StorageGRID. Por ejemplo, no se envían solicitudes de notificaciones de eventos o CloudMirror si una regla de ILM elimina un objeto después de 14 días. Por el contrario, las solicitudes de integración de búsqueda se envían cuando los objetos se eliminan debido a ILM.

Consideración	Detalles
Utilizando puntos finales Kafka	Para puntos finales Kafka, TLS mutuo no es compatible. Como resultado, si tiene `ssl.client.auth` establezca en `required` En su configuración de Kafka broker, puede causar problemas de configuración de punto final de Kafka. La autenticación de los puntos finales de Kafka utiliza los siguientes tipos de autenticación. Estos tipos son diferentes de los utilizados para la autenticación de otros puntos finales, como Amazon SNS, y requieren credenciales de nombre de usuario y contraseña. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Nota:** Los ajustes de proxy de almacenamiento configurados no se aplican a los endpoints de servicios de la plataforma Kafka.

Consideraciones sobre el uso del servicio de replicación de CloudMirror

Consideración	Detalles
Estado de replicación	StorageGRID no admite el `x-amz-replication-status` encabezado.
Tamaño del objeto	El tamaño máximo de los objetos que se pueden replicar en un bloque de destino mediante el servicio de replicación de CloudMirror es de 5 TIB, que es el mismo que el tamaño máximo de objeto *admitido*. **Nota**: El tamaño máximo *Recommended* para una sola operación PutObject es de 5 GiB (5.368.709.120 bytes). Si tiene objetos que sean mayores de 5 GIB, utilice la carga de varias partes en su lugar.
Versiones de bloques e ID de versión	Si el bloque de S3 de origen de StorageGRID tiene habilitado el control de versiones, también debe habilitar el control de versiones para el bloque de destino. Al usar el control de versiones, tenga en cuenta que el orden de las versiones de objetos en el bloque de destino es el mejor esfuerzo y no está garantizado por el servicio CloudMirror, debido a las limitaciones del protocolo S3. **Nota**: Los ID de versión para el depósito de origen en StorageGRID no están relacionados con los ID de versión para el depósito de destino.

Consideración	Detalles
Etiquetado para versiones de objetos	El servicio CloudMirror no replica ninguna solicitud PutObjectTagging o DeleteObjectTagging que proporcione un ID de versión, debido a las limitaciones del protocolo S3. Debido a que los ID de versión para el origen y el destino no están relacionados, no hay forma de garantizar que se replique una actualización de etiqueta para un ID de versión específico. Por el contrario, el servicio CloudMirror replica las solicitudes PutObjectTagging o las solicitudes DeleteObjectTagging que no especifican un ID de versión. Estas solicitudes actualizan las etiquetas de la clave más reciente (o la versión más reciente si el bloque está versionado). También se replican búsquedas normales con etiquetas (no actualizaciones de etiquetado).
Cargas en varias partes y. `ETag` valores	Cuando se crea un mirroring de objetos cargados con una carga de varias partes, el servicio CloudMirror no conserva las piezas. Como resultado, el `ETag` el valor del objeto reflejado será diferente al `ETag` valor del objeto original.
Objetos cifrados con SSE-C (cifrado en el lado del servidor con claves proporcionadas por el cliente)	El servicio CloudMirror no admite objetos cifrados con SSE-C. Si intenta procesar un objeto en el bloque de origen para la replicación de CloudMirror y la solicitud incluye los encabezados de solicitud de SSE-C, se produce un error en la operación.
Bloque con S3 Object Lock habilitado	Si el bucket S3 de destino para la replicación de CloudMirror tiene S3 Object Lock habilitado, el intento de configurar la replicación de bucket (PutBucketReplication) fallará con un error ACCESSDENIED.

Configure los extremos de servicios de la plataforma

Para poder configurar un servicio de plataforma para un bloque, debe configurar al menos un extremo para que sea el destino del servicio de plataforma.

El acceso a servicios de la plataforma está habilitado por inquilino por un administrador de StorageGRID. Para crear o utilizar un punto final de servicios de plataforma, debe ser un usuario inquilino con permiso de gestión de puntos finales o acceso raíz, en una cuadrícula cuya red se ha configurado para permitir que los nodos de almacenamiento accedan a recursos de punto final externo. Para un solo inquilino, puede configurar un máximo de 500 puntos finales de servicios de plataforma. Si desea obtener más información, póngase en contacto con el administrador de StorageGRID.

¿Qué es un extremo de servicios de plataforma?

Al crear un extremo de servicios de plataforma, se especifica la información que StorageGRID necesita para acceder al destino externo.

Por ejemplo, si desea replicar objetos de un bucket de StorageGRID en un bucket de Amazon S3, cree un punto final de servicios de plataforma que incluya la información y las credenciales que necesita StorageGRID para acceder al bucket de destino en Amazon.

Cada tipo de servicio de plataforma requiere su propio extremo, por lo que debe configurar al menos un extremo para cada servicio de plataforma que tenga previsto utilizar. Después de definir un extremo de servicios de plataforma, se utiliza URN del extremo como destino en el XML de configuración utilizado para

habilitar el servicio.

Puede utilizar el mismo extremo que el destino para más de un bloque de origen. Por ejemplo, se pueden configurar varios bloques de origen para que envíen metadatos de objetos al mismo extremo de integración de búsqueda, de modo que se puedan realizar búsquedas en varios bloques. También puede configurar un depósito de origen para que utilice más de un extremo como destino, lo que permite hacer cosas como enviar notificaciones sobre la creación de objetos a un tema de Amazon Simple Notification Service (Amazon SNS) y notificaciones sobre la eliminación de objetos a un segundo tema de Amazon SNS.

Extremos para la replicación de CloudMirror

StorageGRID admite extremos de replicación que representan bloques de S3. Estos bloques se pueden alojar en Amazon Web Services, la misma puesta en marcha de StorageGRID remota o en otro servicio.

Extremos para notificaciones

StorageGRID es compatible con los extremos Amazon SNS y Kafka. No se admiten el servicio de cola simple (SQS) ni los extremos de AWS Lambda.

Para puntos finales Kafka, TLS mutuo no es compatible. Como resultado, si tiene `ssl.client.auth` establezca en `required` En su configuración de Kafka broker, puede causar problemas de configuración de punto final de Kafka.

Extremos del servicio de integración de búsqueda

StorageGRID admite extremos de integración de búsqueda que representan clústeres de Elasticsearch. Estos clústeres de Elasticsearch pueden estar en un centro de datos local o alojados en un cloud de AWS o en otro lugar.

El extremo de integración de búsqueda hace referencia a un índice y un tipo específicos de Elasticsearch. Debe crear el índice en Elasticsearch antes de crear el extremo en StorageGRID o se producirá un error en la creación del extremo. No es necesario crear el tipo antes de crear el punto final. StorageGRID creará el tipo si es necesario al enviar metadatos de objetos al extremo.

Información relacionada

"Administre StorageGRID"

Especifique URN para el extremo de servicios de la plataforma

Al crear un extremo de servicios de plataforma, debe especificar un nombre de recurso único (URN). Utilizará el URN para hacer referencia al punto final cuando cree un XML de configuración para el servicio de plataforma. El URN de cada extremo debe ser único.

StorageGRID valida los extremos de los servicios de la plataforma a medida que se crean. Antes de crear un extremo de servicios de plataforma, confirme que el recurso especificado en el extremo existe y que se puede alcanzar.

URN elementos

El URN de un extremo de servicios de plataforma debe comenzar con cualquiera de los dos `arn:aws` o. `urn:mysite`, como se indica a continuación:

- Si el servicio está alojado en Amazon Web Services (AWS), utilice `arn:aws`

- Si el servicio está alojado en Google Cloud Platform (GCP), utilice `arn:aws`
- Si el servicio se aloja localmente, utilice `urn:mysite`

Por ejemplo, si especifica el URN para un extremo de CloudMirror alojado en StorageGRID, el URN podría comenzar con `urn:sgws`.

El siguiente elemento de URN especifica el tipo de servicio de plataforma, como se indica a continuación:

Servicio	Tipo
Replicación de CloudMirror	`s3`
Notificaciones	`sns` o. `kafka`
Integración de búsqueda	`es`

Por ejemplo, para seguir especificando URN para un extremo de CloudMirror alojado en StorageGRID, debería añadir `s3` para conseguirlo `urn:sgws:s3`.

El elemento final del URN identifica el recurso de destino específico en el URI de destino.

Servicio	Recurso específico
Replicación de CloudMirror	`bucket-name`
Notificaciones	`sns-topic-name` o. `kafka-topic-name`
Integración de búsqueda	`domain-name/index-name/type-name` **Nota:** Si el clúster Elasticsearch está **no** configurado para crear índices automáticamente, debe crear el índice manualmente antes de crear el punto final.

Urnas para servicios alojados en AWS y GCP

Para las entidades AWS y GCP, el URN completo es un AWS ARN válido. Por ejemplo:

- Replicación de CloudMirror:

```
arn:aws:s3:::bucket-name
```

- Notificaciones:

```
arn:aws:sns:region:account-id:topic-name
```

- Integración de búsqueda:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

Para un extremo de integración de búsqueda de AWS, la `domain-name` debe incluir la cadena literal `domain/`, como se muestra aquí.

Servicios alojados localmente

Al usar servicios alojados localmente en lugar de servicios de cloud, puede especificar el URN de cualquier forma que cree una URN válida y única, siempre y cuando URN incluya los elementos necesarios en la tercera y última posición. Puede dejar los elementos indicados por opcional en blanco o puede especificarlos de cualquier forma que le ayude a identificar el recurso y hacer que el URN sea único. Por ejemplo:

- Replicación de CloudMirror:

  ```
  urn:mysite:s3:optional:optional:bucket-name
  ```

  En el caso de un extremo de CloudMirror alojado en StorageGRID, es posible especificar una URN válida que comience por `urn:sgws`:

  ```
  urn:sgws:s3:optional:optional:bucket-name
  ```

- Notificaciones:

  Especifique un punto final de Amazon Simple Notification Service:

  ```
  urn:mysite:sns:optional:optional:sns-topic-name
  ```

  Especifique un punto final Kafka:

  ```
  urn:mysite:kafka:optional:optional:kafka-topic-name
  ```

- Integración de búsqueda:

  ```
  urn:mysite:es:optional:optional:domain-name/index-name/type-name
  ```

  Para los extremos de integración de búsqueda alojados localmente, el `domain-name` Element puede ser cualquier cadena siempre que el URN del extremo sea único.

Cree un extremo de servicios de plataforma

Debe crear al menos un extremo del tipo correcto para poder habilitar un servicio de

plataforma.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Pertenece a un grupo de usuarios que tiene el "Gestionar puntos finales o permisos de acceso raíz".
- Se ha creado el recurso al que hace referencia el punto final de servicios de plataforma:
  - Replicación de CloudMirror: Bloque de S3
  - Notificación de eventos: Tema de Amazon Simple Notification Service (Amazon SNS) o Kafka
  - Notificación de búsqueda: Índice de Elasticsearch, si el clúster de destino no está configurado para crear índices automáticamente.
- Tiene la información sobre el recurso de destino:
  - Host y puerto para el Identificador uniforme de recursos (URI)

    > Si piensa utilizar un bloque alojado en un sistema StorageGRID como extremo para la replicación de CloudMirror, póngase en contacto con el administrador de grid para determinar los valores que debe introducir.

  - Nombre del recurso único (URN)

    "Especifique URN para el extremo de servicios de la plataforma"

  - Credenciales de autenticación (si es necesario):

Extremos de integración de búsquedas de AWS

Para los extremos de integración de búsqueda de AWS, puede usar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave de acceso secreta
- Basic HTTP: Nombre de usuario y contraseña
- CAP (C2S Access Portal): URL de credenciales temporales, certificados de servidor y de cliente, claves de cliente y una contraseña de clave privada de cliente opcional.

Replicación de CloudMirror y extremos de Amazon SNS

Para la replicación de CloudMirror y los extremos de Amazon SNS, puede usar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave de acceso secreta
- CAP (C2S Access Portal): URL de credenciales temporales, certificados de servidor y de cliente, claves de cliente y una contraseña de clave privada de cliente opcional.

Puntos finales de Kafka

Para los puntos finales de Kafka, puede utilizar las siguientes credenciales:

- SASL/PLAIN: Nombre de usuario y contraseña
- SASL/SCRAM-SHA-256: Nombre de usuario y contraseña
- SASL/SCRAM-SHA-512: Nombre de usuario y contraseña

- Certificado de seguridad (si se utiliza un certificado de CA personalizado)

- Si las funciones de seguridad de Elasticsearch están activadas, tiene el privilegio de clúster de supervisión para las pruebas de conectividad y el privilegio WRITE INDEX o los privilegios INDEX y DELETE INDEX para las actualizaciones de documentos.

Pasos

1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**. Aparece la página de extremos de servicios de plataforma.
2. Seleccione **Crear punto final**.
3. Introduzca un nombre para mostrar para describir brevemente el extremo y su propósito.

   El tipo de servicio de plataforma que soporta el punto final se muestra junto al nombre del punto final cuando se muestra en la página de puntos finales, por lo que no es necesario incluir esa información en el nombre.

4. En el campo **URI**, especifique el Identificador de recursos único (URI) del extremo.

   Utilice uno de los siguientes formatos:

   ```
   https://host:port
   http://host:port
   ```

   Si no especifica un puerto, se utilizan los siguientes puertos predeterminados:

   - Puerto 443 para URI HTTPS y puerto 80 para URI HTTP (mayoría de extremos)
   - Puerto 9092 para URI HTTPS y HTTP (solo puntos finales Kafka)

   Por ejemplo, el URI para un bloque alojado en StorageGRID podría ser:

   ```
   https://s3.example.com:10443
   ```

   En este ejemplo: `s3.example.com` Representa la entrada DNS para la IP virtual (VIP) del grupo de alta disponibilidad (ha) de StorageGRID, y. `10443` representa el puerto definido en el extremo del equilibrador de carga.

   > Siempre que sea posible, debe conectarse a un grupo de alta disponibilidad de nodos de equilibrio de carga para evitar un único punto de error.

   Del mismo modo, el URI para un bloque alojado en AWS podría ser:

   ```
   https://s3-aws-region.amazonaws.com
   ```

   > Si el punto final se utiliza para el servicio de replicación de CloudMirror, no incluya el nombre del bloque en el URI. Incluye el nombre de bloque en el campo **URN**.

5. Introduzca el nombre de recurso único (URN) para el extremo.

No puede cambiar el URN de un punto final después de crear el punto final.

6. Seleccione **continuar**.
7. Seleccione un valor para **Tipo de autenticación**.

Extremos de integración de búsquedas de AWS

Introduzca o cargue las credenciales para un extremo de integración de búsqueda de AWS.

Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
Clave de acceso	Usa credenciales de estilo AWS para autenticar conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta
HTTP básico	Utiliza un nombre de usuario y una contraseña para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña
CAP (Portal de acceso C2S)	Usa certificados y claves para autenticar las conexiones al destino.	• URL de credenciales temporales • Certificado de CA de servidor (carga de archivo PEM) • Certificado de cliente (carga de archivo PEM) • Clave privada de cliente (carga de archivo PEM, formato cifrado OpenSSL o formato de clave privada no cifrado) • Contraseña de clave privada de cliente (opcional)

Replicación de CloudMirror o extremos de Amazon SNS

Introduzca o cargue las credenciales para una replicación de CloudMirror o un extremo de Amazon SNS.

Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
Clave de acceso	Usa credenciales de estilo AWS para autenticar conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta

Tipo de autenticación	Descripción	Credenciales
CAP (Portal de acceso C2S)	Usa certificados y claves para autenticar las conexiones al destino.	• URL de credenciales temporales • Certificado de CA de servidor (carga de archivo PEM) • Certificado de cliente (carga de archivo PEM) • Clave privada de cliente (carga de archivo PEM, formato cifrado OpenSSL o formato de clave privada no cifrado) • Contraseña de clave privada de cliente (opcional)

Puntos finales de Kafka

Introduzca o cargue las credenciales para un punto final de Kafka.

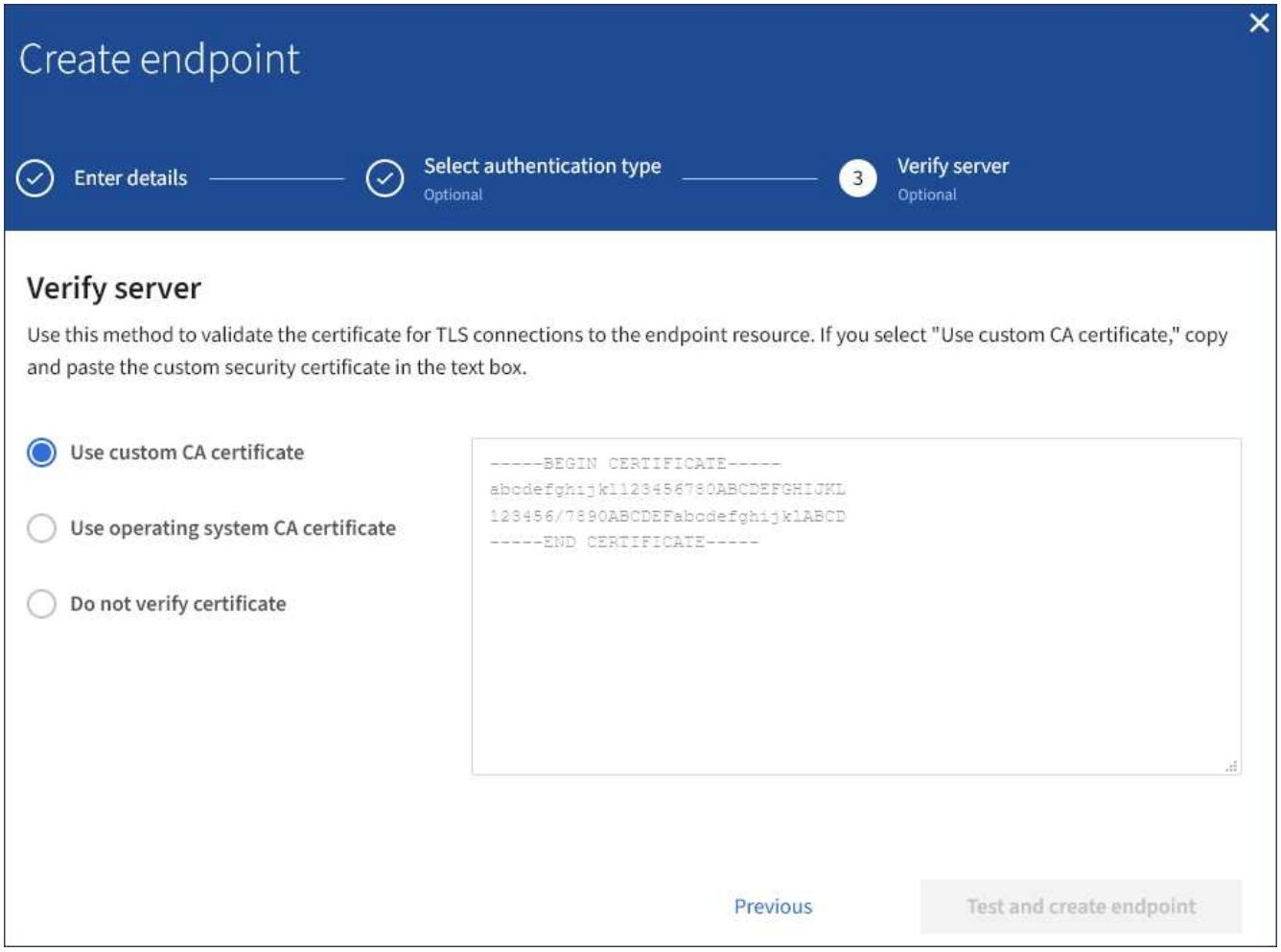
Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
SASL/PLAIN	Utiliza un nombre de usuario y una contraseña con texto sin formato para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña
SASL/SCRAM-SHA-256	Utiliza un nombre de usuario y una contraseña mediante un protocolo de respuesta de desafío y hash SHA-256 para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña
SASL/SCRAM-SHA-512	Utiliza un nombre de usuario y una contraseña mediante un protocolo de respuesta de desafío y hash SHA-512 para autenticar las conexiones al destino.	• Nombre de usuario • Contraseña

Seleccione **Usar la autenticación de delegación tomada** si el nombre de usuario y la contraseña se derivan de un token de delegación que se obtuvo de un clúster de Kafka.

8. Seleccione **continuar**.
9. Seleccione un botón de opción para **verificar servidor** para elegir cómo se verifica la conexión TLS con el

extremo.



Tipo de verificación del certificado	Descripción
Utilizar certificado de CA personalizado	Usar un certificado de seguridad personalizado. Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto **Certificado CA**.
Utilizar certificado de CA del sistema operativo	Utilice el certificado de CA de cuadrícula predeterminado instalado en el sistema operativo para asegurar las conexiones.
No verifique el certificado	El certificado utilizado para la conexión TLS no se verifica. Esta opción no es segura.

10. Seleccione **probar y crear punto final**.
    - Aparece un mensaje de éxito si se puede acceder al extremo con las credenciales especificadas. La conexión con el extremo se valida desde un nodo en cada sitio.
    - Aparece un mensaje de error si se produce un error en la validación del extremo. Si necesita modificar el punto final para corregir el error, seleccione **Volver a los detalles del punto final** y actualice la información. A continuación, seleccione **probar y crear punto final**.

La creación de punto final falla si los servicios de plataforma no están activados para su cuenta de inquilino. Póngase en contacto con el administrador de StorageGRID.

Una vez que haya configurado un extremo, puede utilizar su URN para configurar un servicio de plataforma.

Información relacionada

"Especifique URN para el extremo de servicios de la plataforma"

"Configure la replicación de CloudMirror"

"Configure las notificaciones de eventos"

"Configure el servicio de integración de búsqueda"

Probar la conexión para el extremo de servicios de la plataforma

Si la conexión a un servicio de plataforma ha cambiado, puede probar la conexión del extremo para validar que el recurso de destino existe y que se puede acceder a él utilizando las credenciales especificadas.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestionar puntos finales o permisos de acceso raíz".

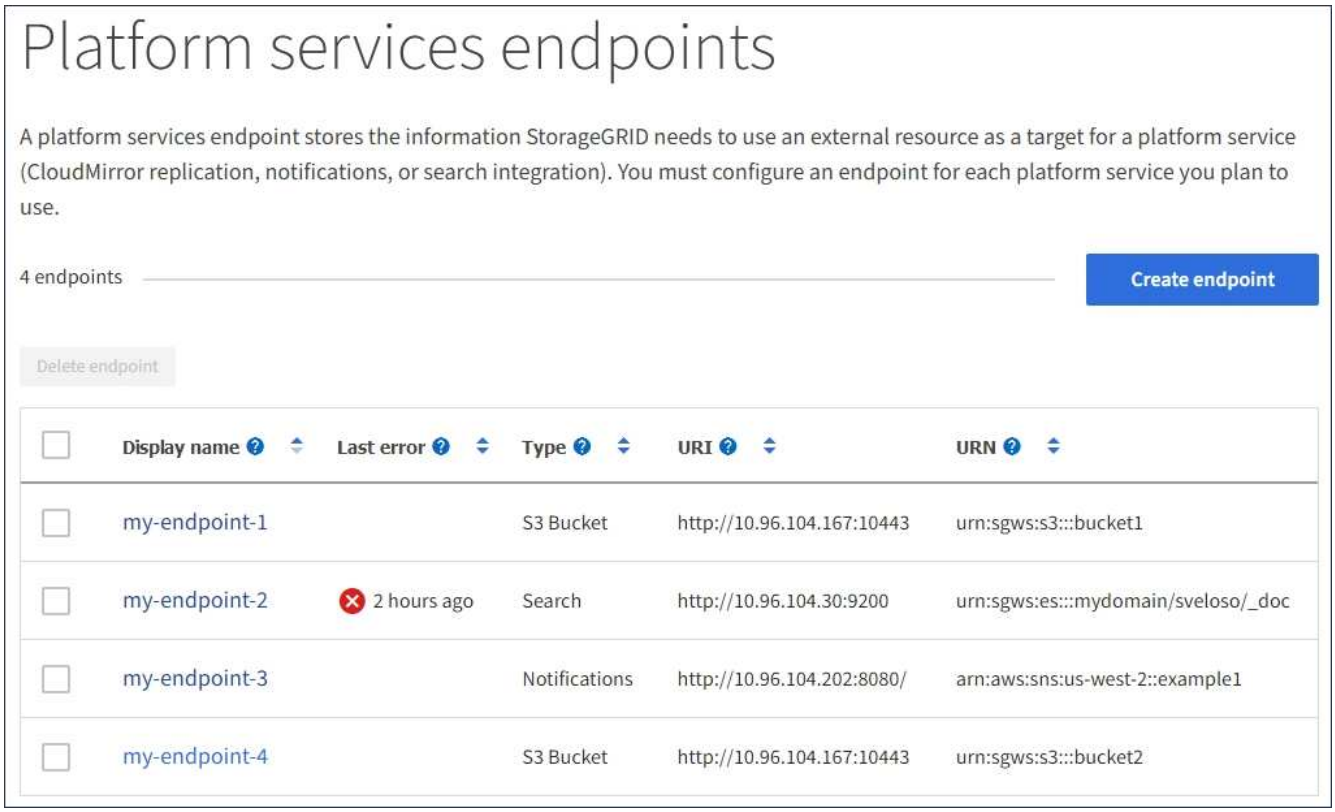
Acerca de esta tarea

StorageGRID no valida que las credenciales tengan los permisos correctos.

Pasos

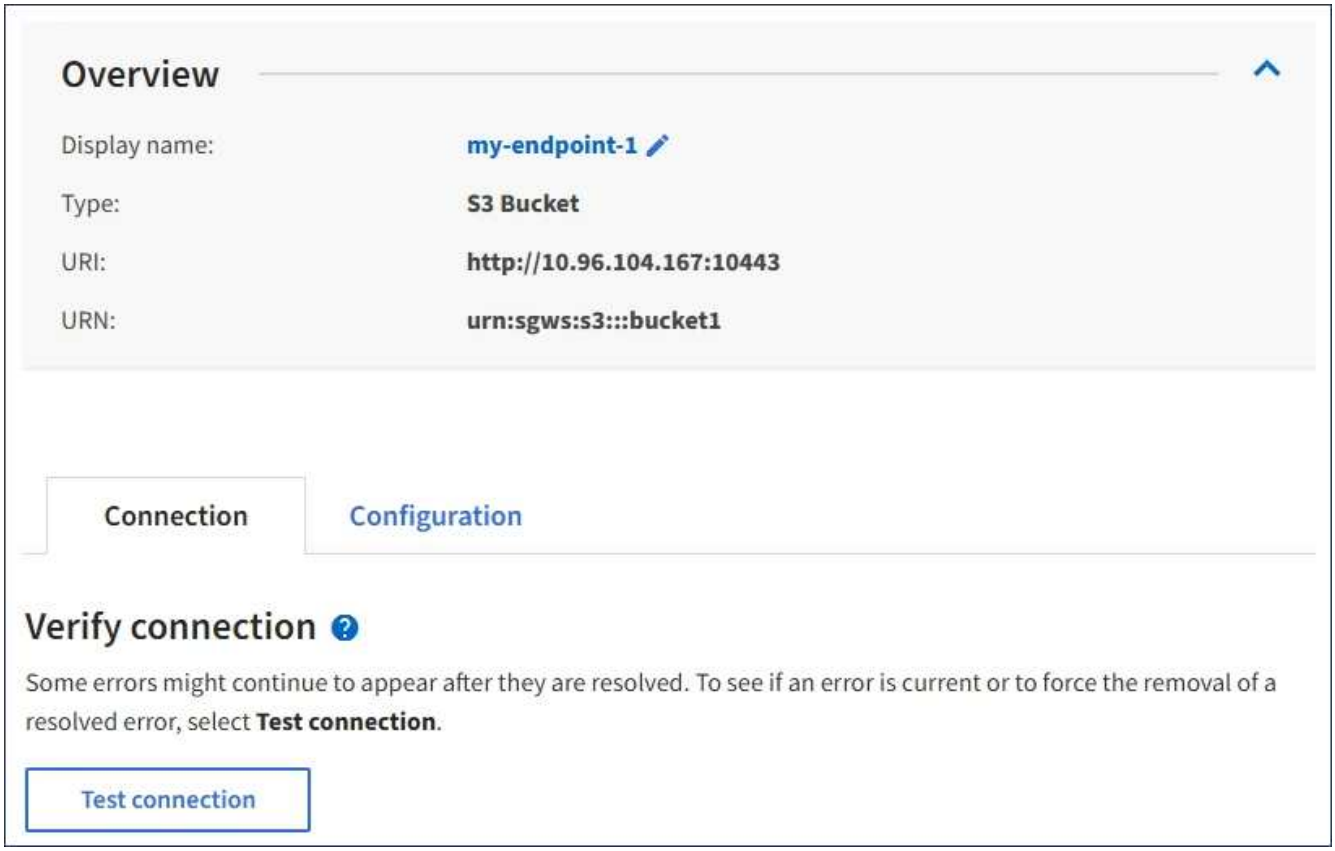
1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**.

   Aparece la página de extremos de servicios de plataforma y muestra la lista de extremos de servicios de plataforma que ya se han configurado.



2. Seleccione el extremo cuya conexión desea probar.

   Aparece la página de detalles del extremo.



3. Seleccione **probar conexión**.

- Aparece un mensaje de éxito si se puede acceder al extremo con las credenciales especificadas. La conexión con el extremo se valida desde un nodo en cada sitio.
- Aparece un mensaje de error si se produce un error en la validación del extremo. Si necesita modificar el extremo para corregir el error, seleccione **Configuración** y actualice la información. A continuación, seleccione **probar y guardar los cambios**.

Editar extremo de servicios de plataforma

Puede editar la configuración de un extremo de servicios de plataforma para cambiar su nombre, URI u otros detalles. Por ejemplo, es posible que deba actualizar las credenciales caducadas o cambiar el URI para apuntar a un índice de Elasticsearch de backup para la conmutación por error. No puede cambiar el URN para un punto final de servicios de plataforma.

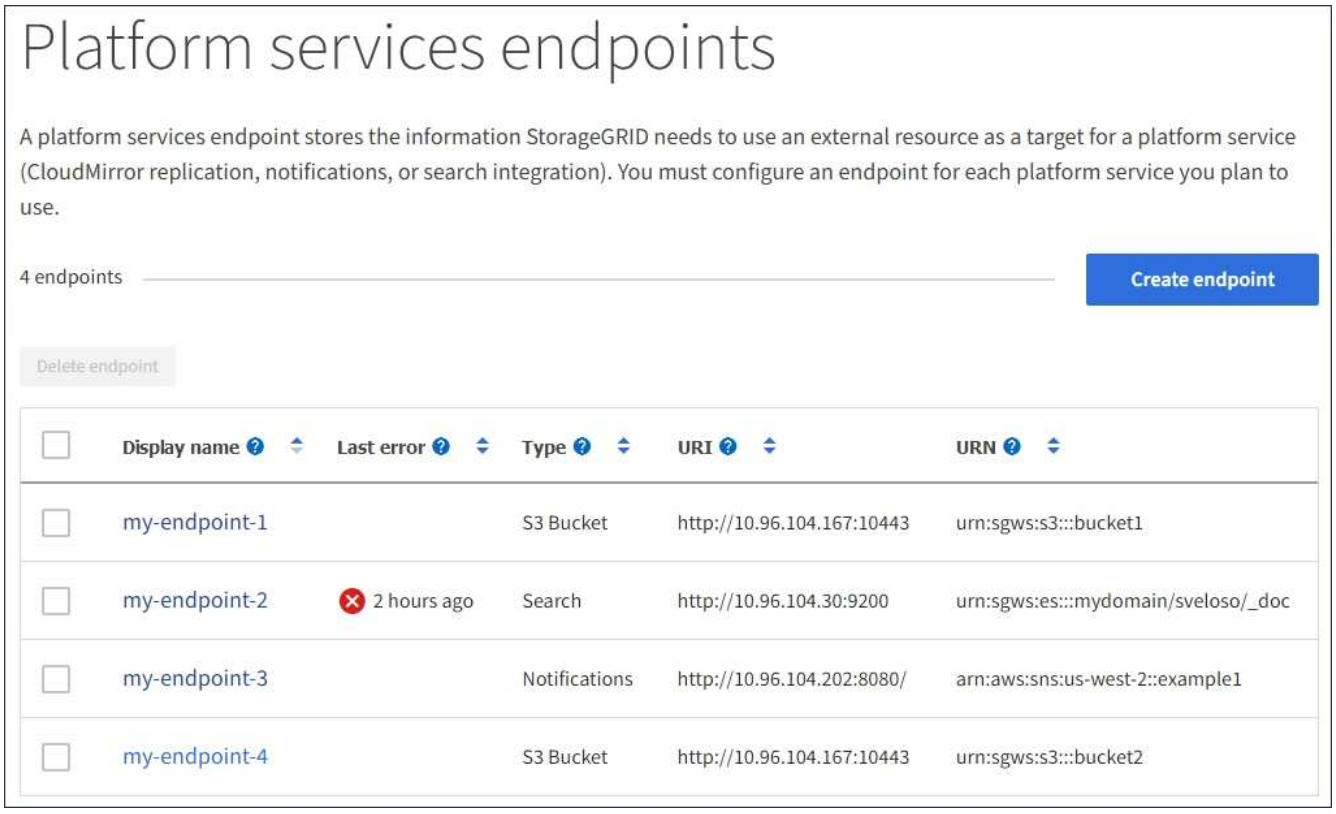
Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestionar puntos finales o permisos de acceso raíz".

Pasos

1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**.

   Aparece la página de extremos de servicios de plataforma y muestra la lista de extremos de servicios de plataforma que ya se han configurado.



2. Seleccione el extremo que desea editar.

   Aparece la página de detalles del extremo.

3. Seleccione **Configuración**.
4. Según sea necesario, cambie la configuración del extremo.

   No puede cambiar el URN de un punto final después de crear el punto final.

   a. Para cambiar el nombre para mostrar del extremo, seleccione el icono de edición .
   b. Según sea necesario, cambie el URI.
   c. Según sea necesario, cambie el tipo de autenticación.
      - Para la autenticación de la clave de acceso, cambie la clave según sea necesario seleccionando **Editar clave S3** y pegando un nuevo ID de clave de acceso y una clave de acceso secreta. Si necesita cancelar los cambios, seleccione **Revert S3 key EDIT**.
      - Para la autenticación CAP (C2S Access Portal), cambie la URL de las credenciales temporales o la frase de contraseña de la clave privada del cliente opcional y cargue nuevos archivos de certificado y claves según sea necesario.

        La clave privada del cliente debe estar en formato cifrado OpenSSL o en formato de clave privada no cifrada.

   d. Según sea necesario, cambie el método para verificar el servidor.
5. Seleccione **probar y guardar los cambios**.
   - Aparece un mensaje de éxito si se puede acceder al extremo con las credenciales especificadas. La conexión al extremo se verifica desde un nodo en cada sitio.
   - Aparece un mensaje de error si se produce un error en la validación del extremo. Modifique el extremo para corregir el error y, a continuación, seleccione **probar y guardar los cambios**.

Eliminar extremo de servicios de plataforma

Puede eliminar un extremo si ya no desea utilizar el servicio de plataforma asociado.

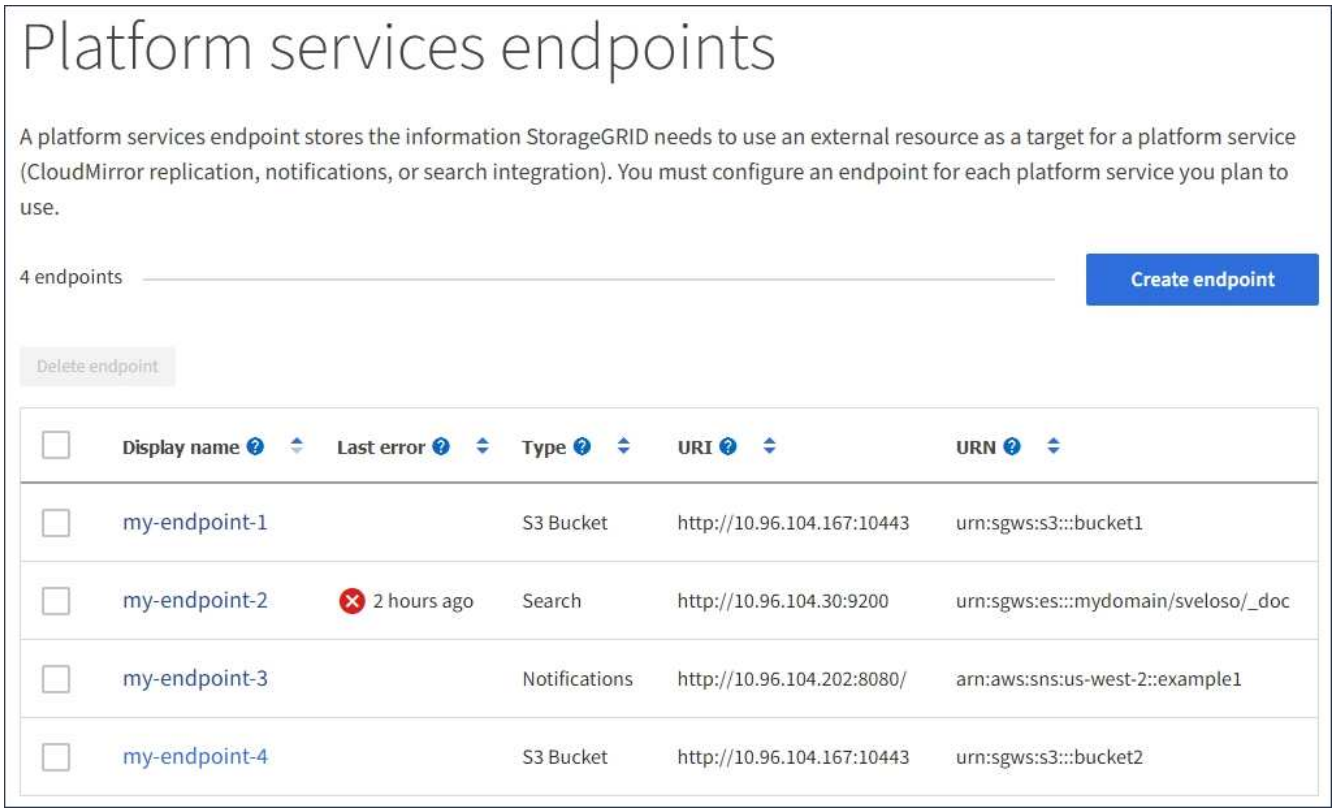
Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestionar puntos finales o permisos de acceso raíz".

Pasos

1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**.

   Aparece la página de extremos de servicios de plataforma y muestra la lista de extremos de servicios de plataforma que ya se han configurado.

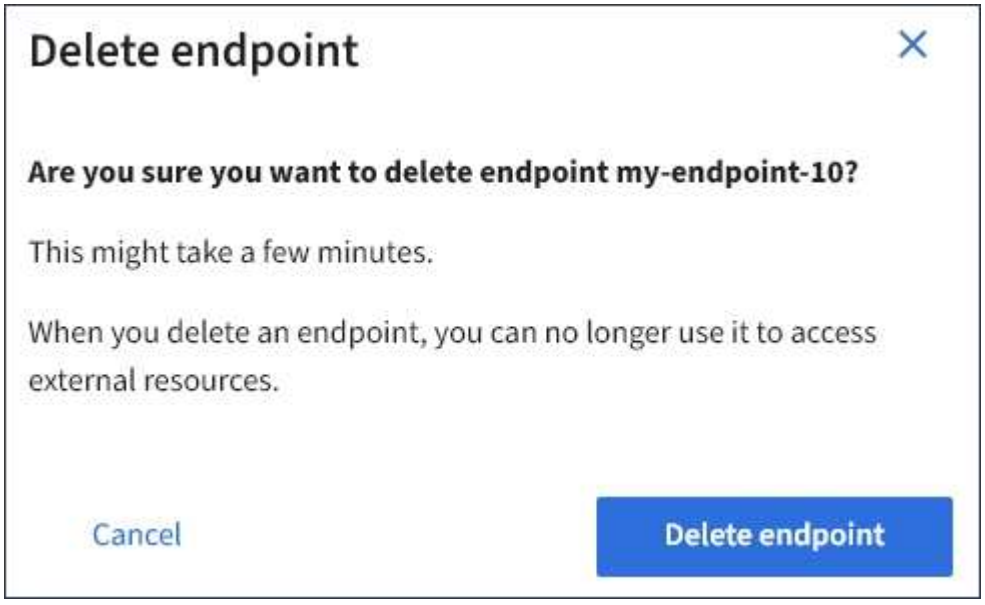


2. Seleccione la casilla de verificación de cada punto final que desee suprimir.

> Si elimina un extremo de servicios de plataforma que está en uso, el servicio de plataforma asociado se deshabilitará para todos los bloques que utilicen el extremo. Se descartarán las solicitudes que aún no se hayan completado. Se continuarán generando todas las solicitudes nuevas hasta que cambie la configuración de bloque para que ya no haga referencia a URN eliminado. StorageGRID informará de estas solicitudes como errores irrecuperables.

3. Seleccione **acciones** > **Eliminar punto final**.

   Aparecerá un mensaje de confirmación.



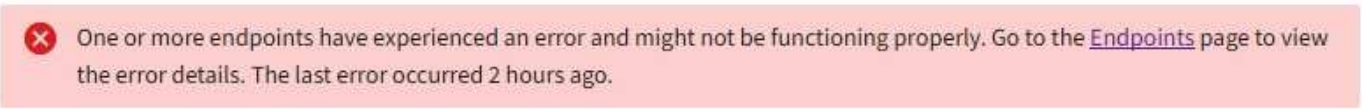
4. Seleccione **Eliminar punto final**.

Solucionar errores de extremos de servicios de plataforma

Si se produce un error cuando StorageGRID intenta comunicarse con un punto final de servicios de plataforma, se muestra un mensaje en el panel de control. En la página Platform Services Endpoints, la columna Last error indica durante cuánto tiempo se produjo el error. No se muestra ningún error si los permisos asociados con las credenciales de un extremo son incorrectos.

Determine si se ha producido un error

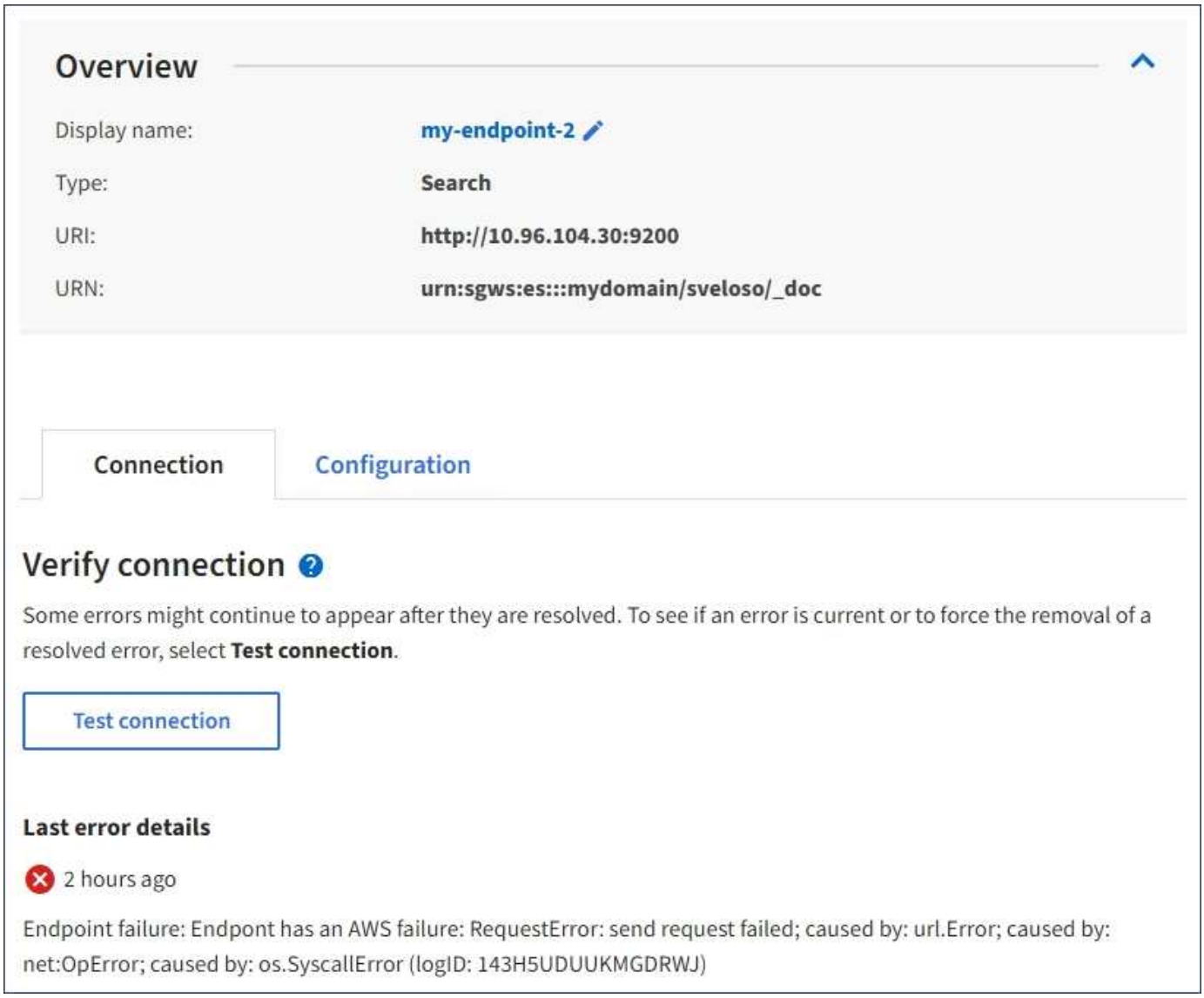
Si se ha producido algún error de punto final de servicios de plataforma en los últimos 7 días, el panel de control del gestor de inquilinos muestra un mensaje de alerta. Puede ir a la página de extremos de servicios de plataforma para ver más detalles sobre el error.



El mismo error que aparece en el panel de control también aparece en la parte superior de la página Puntos Finales de Servicios de Plataforma. Para ver un mensaje de error más detallado:

Pasos

1. En la lista de puntos finales, seleccione el extremo que tiene el error.
2. En la página de detalles del punto final, seleccione **Conexión**. Esta pestaña muestra sólo el error más reciente de un punto final e indica cuánto tiempo se produjo el error. Errores que incluyen el icono X rojo  ocurrió en los últimos 7 días.



Compruebe si el error sigue estando actualizado

Es posible que algunos errores sigan apareciendo en la columna **último error** incluso después de que se hayan resuelto. Para ver si un error es actual o para forzar la eliminación de un error resuelto de la tabla:

Pasos

1. Seleccione el extremo.

   Aparece la página de detalles del extremo.

2. Seleccione **Conexión** > **probar conexión**.

Al seleccionar **probar conexión**, StorageGRID valida que el extremo de servicios de la plataforma existe y que se puede alcanzar con las credenciales actuales. La conexión con el extremo se valida desde un nodo en cada sitio.

Resolver errores de punto final

Puede utilizar el mensaje **último error** de la página de detalles del punto final para ayudar a determinar qué está causando el error. Es posible que algunos errores requieran que edite el extremo para resolver el

problema. Por ejemplo, se puede producir un error CloudMirroring si StorageGRID no puede acceder al bloque de S3 de destino porque no tiene los permisos de acceso correctos o si la clave de acceso ha caducado. El mensaje es «Las credenciales del punto final o el acceso al destino deben actualizarse» y los detalles son «ACCESSDENIED» o «InvalidAccessKeyId».

Si necesita editar el extremo para resolver un error, al seleccionar **probar y guardar cambios** StorageGRID validará el extremo actualizado y confirmará que se puede alcanzar con las credenciales actuales. La conexión con el extremo se valida desde un nodo en cada sitio.

Pasos

1. Seleccione el extremo.
2. En la página de detalles del punto final, seleccione **Configuración**.
3. Edite la configuración del extremo según sea necesario.
4. Seleccione **Conexión** > **probar conexión**.

Credenciales de extremo con permisos insuficientes

Cuando StorageGRID valida un extremo de servicios de plataforma, confirma que las credenciales del extremo se pueden utilizar para ponerse en contacto con el recurso de destino y realiza una comprobación básica de permisos. Sin embargo, StorageGRID no valida todos los permisos necesarios para ciertas operaciones de servicios de plataforma. Por este motivo, si recibe un error al intentar utilizar un servicio de plataforma (como “403 Forbidden”), compruebe los permisos asociados con las credenciales del punto final.

Información relacionada

- **Administrar los servicios de plataforma de StorageGRID › Solucionar problemas**
- "Cree un extremo de servicios de plataforma"
- "Probar la conexión para el extremo de servicios de la plataforma"
- "Editar extremo de servicios de plataforma"

Configure la replicación de CloudMirror

La "Servicio de replicación de CloudMirror" Es uno de los tres servicios de plataforma de StorageGRID. Puede usar la replicación de CloudMirror para replicar automáticamente objetos en un bloque de S3 externo.

Antes de empezar

- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un bucket que actúa como origen de replicación.
- El punto final que pretende utilizar como destino para la replicación de CloudMirror ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

La replicación de CloudMirror copia los objetos de un bloque de origen en un bloque de destino que se especifique en un extremo.

La replicación de CloudMirror tiene similitudes y diferencias importantes con la función de replicación entre grid. Para obtener más información, consulte "Compare la replicación entre grid y la replicación de CloudMirror".

Para habilitar la replicación de CloudMirror para un bucket, debe crear y aplicar un XML de configuración de replicación de bucket válido. El XML de configuración de replicación debe usar la URN de un extremo de bloque de S3 para cada destino.

La replicación no es compatible con buckets de origen o destino con el bloqueo de objetos S3 habilitado.

Para obtener información general sobre la replicación de bloques y cómo configurarla, consulte "Documentación de Amazon Simple Storage Service (S3): Replicación de objetos". Para obtener información sobre cómo StorageGRID implementa GetBucketReplication, DeleteBucketReplication y PutBucketReplication, consulte "Operaciones en bloques".

Si habilita la replicación de CloudMirror en un bloque que contiene objetos, se replican los nuevos objetos agregados al bloque, pero los objetos existentes del bloque no se replican. Debe actualizar los objetos existentes para activar la replicación.

Si se especifica una clase de almacenamiento en el XML de configuración de replicación, StorageGRID utiliza esa clase al realizar operaciones en el extremo de S3 de destino. El extremo de destino también debe admitir la clase de almacenamiento especificada. Asegúrese de seguir las recomendaciones que proporciona el proveedor del sistema de destino.

Pasos

1. Habilite la replicación para su bloque de origen:

   Utilice un editor de texto para crear el XML de configuración de replicación necesario para habilitar la replicación, tal y como se especifica en la API de replicación de S3. Al configurar XML:

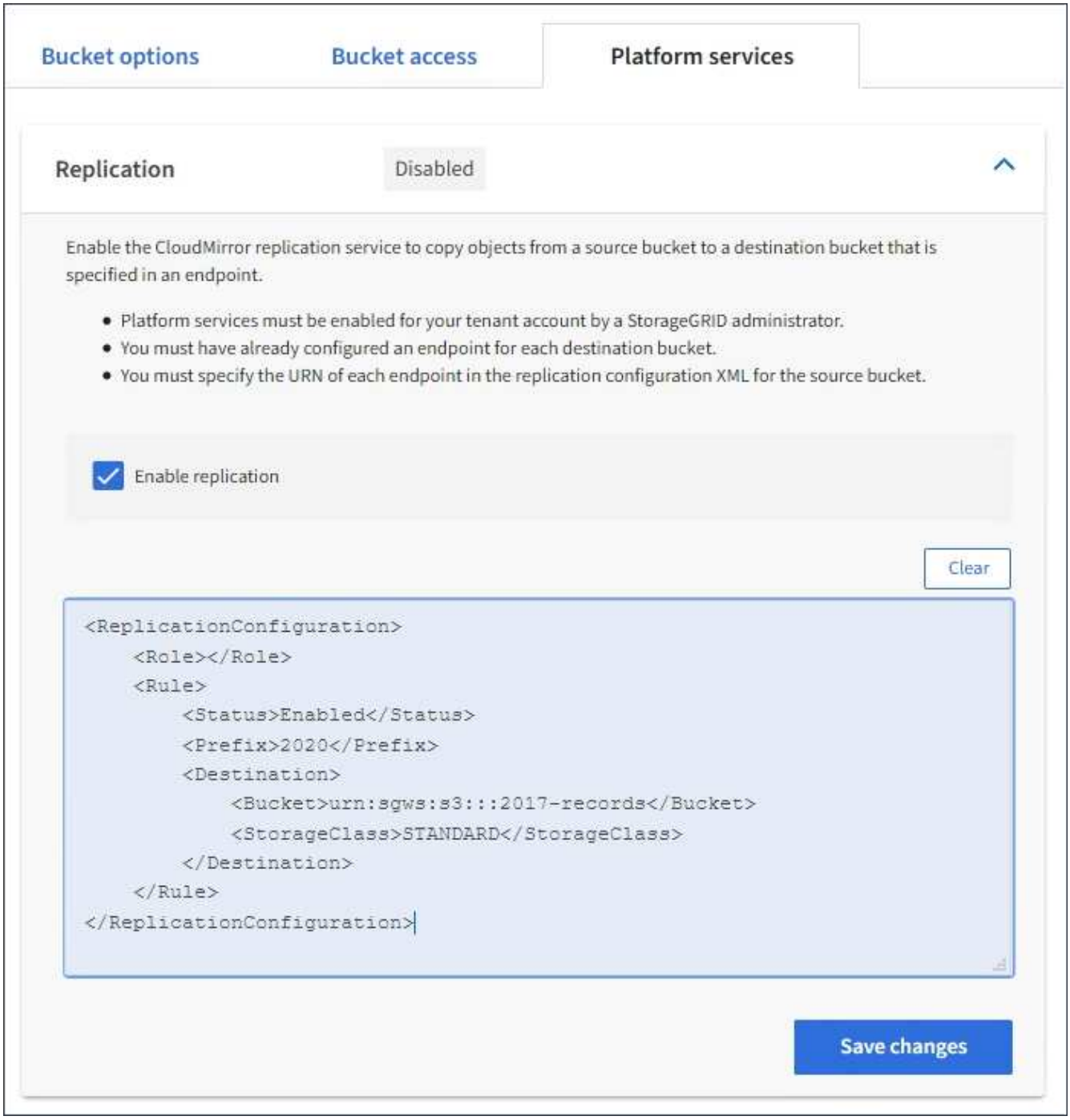
   - Tenga en cuenta que StorageGRID solo admite V1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso de `Filter` Elemento para reglas y sigue las convenciones V1 para eliminar versiones de objetos. Consulte la documentación de Amazon sobre la configuración de replicación para obtener más información.
   - Use el URN de un extremo de bloque de S3 como destino.
   - Si lo desea, puede agregar el `<StorageClass>` y especifique una de las siguientes opciones:
     - `STANDARD`: La clase de almacenamiento predeterminada. Si no especifica una clase de almacenamiento al cargar un objeto, el `STANDARD` se utiliza la clase de almacenamiento.
     - `STANDARD_IA`: (Estándar - acceso poco frecuente.) Utilice esta clase de almacenamiento para los datos a los que se accede con menor frecuencia; sin embargo, este proceso requiere un acceso rápido cuando sea necesario.
     - `REDUCED_REDUNDANCY`: Utilice esta clase de almacenamiento para datos no críticos y reproducibles que se pueden almacenar con menos redundancia que el `STANDARD` clase de almacenamiento.
   - Si especifica un `Role` En el XML de configuración se ignorará. StorageGRID no utiliza este valor.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Buckets**.
3. Seleccione el nombre del bloque de origen.

   Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma** > **replicación**.
5. Seleccione la casilla de verificación **Habilitar replicación**.
6. Pegue el XML de configuración de replicación en el cuadro de texto y seleccione **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de plataforma para cada cuenta de inquilino mediante Grid Manager o la API de gestión de grid. Póngase en contacto con el administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Compruebe que la replicación está configurada correctamente:
   a. Añada un objeto al bloque de origen que cumpla con los requisitos de replicación según se especifica en la configuración de replicación.

      En el ejemplo mostrado anteriormente, se replican los objetos que coincidan con el prefijo «2020».

   b. Confirme que el objeto se ha replicado en el bloque de destino.

En el caso de objetos pequeños, la replicación se realiza con rapidez.

Información relacionada

"Cree un extremo de servicios de plataforma"

Configure las notificaciones de eventos

El servicio de notificaciones es uno de los tres servicios de la plataforma StorageGRID. Puede habilitar las notificaciones de un depósito para enviar información sobre eventos especificados a un clúster Kafka de destino o servicio compatible con AWS Simple Notification Service (Amazon SNS).

Antes de empezar

- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Ya creó un bloque para que actúe como origen de notificaciones.
- El punto final que pretende utilizar como destino para las notificaciones de eventos ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar las notificaciones de eventos, cada vez que se produce un evento específico para un objeto en el depósito de origen, se genera una notificación y se envía al tema de Amazon SNS o Kafka utilizado como punto final de destino. Para habilitar las notificaciones para un bloque, debe crear y aplicar un XML de configuración de notificación válido. El XML de configuración de notificaciones debe usar el URN de un extremo de notificaciones de eventos para cada destino.

Para obtener información general sobre las notificaciones de eventos y cómo configurarlas, consulte la documentación de Amazon. Para obtener información sobre cómo StorageGRID implementa la API de configuración de notificación de bloques de S3, consulte la "Instrucciones para implementar aplicaciones cliente de S3".

Si habilita las notificaciones de eventos para un bloque que contiene objetos, las notificaciones se envían solo para las acciones que se realizan una vez guardada la configuración de notificación.

Pasos

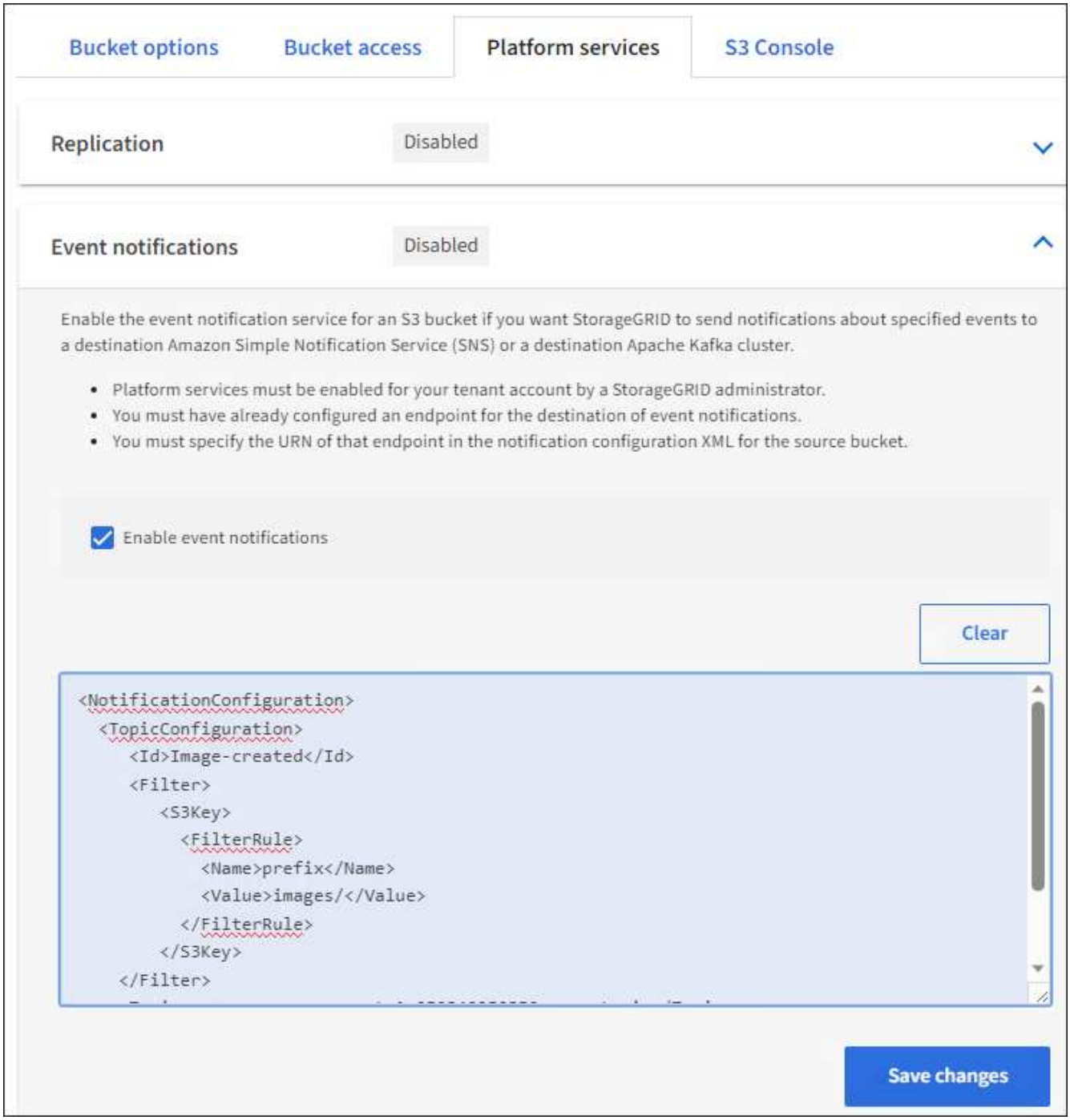
1. Habilite las notificaciones para su bloque de origen:
   - Use un editor de texto para crear el XML de configuración de notificaciones necesario para habilitar las notificaciones de eventos, como se especifica en la API de notificación de S3.
   - Al configurar XML, utilice URN de un extremo de notificaciones de eventos como tema de destino.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
3. Seleccione el nombre del bloque de origen.

   Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma** > **Notificaciones de eventos**.
5. Seleccione la casilla de verificación **Habilitar notificaciones de eventos**.
6. Pegue el XML de configuración de notificación en el cuadro de texto y seleccione **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de plataforma para cada cuenta de inquilino mediante Grid Manager o la API de gestión de grid. Póngase en contacto con el administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Compruebe que las notificaciones de eventos están configuradas correctamente:

   a. Realice una acción en un objeto del bloque de origen que cumpla los requisitos para activar una notificación tal y como se ha configurado en el XML de configuración.

      En el ejemplo, se envía una notificación de evento cada vez que se crea un objeto con el `images/` prefijo.

b. Confirme que se ha entregado una notificación al tema de destino de Amazon SNS o Kafka.

   Por ejemplo, si el tema de destino está alojado en Amazon SNS, puede configurar el servicio para que le envíe un correo electrónico cuando se entregue la notificación.


```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```


+
Si se recibe la notificación en el tema de destino, ha configurado correctamente el bloque de origen para las notificaciones StorageGRID.

Información relacionada

"Comprender las notificaciones para bloques"

"USE LA API DE REST DE S3"

"Cree un extremo de servicios de plataforma"

Utilice el servicio de integración de búsqueda

El servicio de integración de búsqueda es uno de los tres servicios de la plataforma StorageGRID. Este servicio puede habilitar el envío de metadatos de objetos a un índice de búsqueda de destino siempre que se cree, se elimine o actualice los metadatos o las etiquetas de un objeto.

Puede configurar la integración de búsqueda mediante el Administrador de inquilinos para aplicar XML de configuración de StorageGRID personalizado a un bloque.

> Debido a que el servicio de integración de búsqueda hace que los metadatos de objeto se envíen a un destino, su XML de configuración se denomina XML_ de configuración de notificación de metadatos. Este XML de configuración es diferente al *notification Configuration XML* utilizado para habilitar las notificaciones de eventos.

Consulte "Instrucciones para implementar aplicaciones cliente de S3" Para obtener detalles sobre las siguientes operaciones personalizadas de la API de REST de StorageGRID S3:

- DELETE bucket metadata notification Configuration
- OBTENGA la configuración de notificación de metadatos del bloque de datos
- Configuración de notificaciones de metadatos de PUT Bucket

Información relacionada

"XML de configuración para la integración de búsqueda"

"Metadatos de objetos incluidos en las notificaciones de metadatos"

"JSON generado por el servicio de integración de búsqueda"

"Configure el servicio de integración de búsqueda"

"USE LA API DE REST DE S3"

XML de configuración para la integración de búsqueda

El servicio de integración de búsqueda se configura mediante un conjunto de reglas contenidas en `<MetadataNotificationConfiguration>` y.. `</MetadataNotificationConfiguration>` etiquetas. Cada regla especifica los objetos a los que se aplica la regla y el destino al que StorageGRID debe enviar los metadatos de esos objetos.

Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, puede enviar metadatos de los objetos con el prefijo `images` en un destino y los metadatos de los objetos con el prefijo `videos` a otro. Las configuraciones que tienen prefijos superpuestos no son válidas y se rechazan cuando se envían. Por

ejemplo, una configuración que incluye una regla para objetos con el prefijo `test` y una segunda regla para los objetos con el prefijo `test2` no está permitido.

Los destinos deben especificarse mediante el URN de un extremo de StorageGRID que se ha creado para el servicio de integración de búsqueda. Estos extremos se refieren a un índice y tipo definidos en un clúster de Elasticsearch.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

En la tabla se describen los elementos del XML de configuración de notificaciones de metadatos.

Nombre	Descripción	Obligatorio
MetadataNotificationConfiguration	Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos Regla.	Sí
Regla	Código de contenedor de una regla que identifica los objetos cuyos metadatos deben agregarse a un índice especificado. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
ID	Identificador único de la regla. Incluido en el elemento Regla.	No

Nombre	Descripción	Obligatorio
Estado	El estado puede ser "activado" o "desactivado". No se toman medidas para las reglas que están desactivadas. Incluido en el elemento Regla.	Sí
Prefijo	Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado. Para hacer coincidir todos los objetos, especifique un prefijo vacío. Incluido en el elemento Regla.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Regla.	Sí
No	URN del destino donde se envían los metadatos del objeto. Debe ser URN de un extremo de StorageGRID con las siguientes propiedades: • `es` debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo donde se almacenan los metadatos, en el formulario `domain-name/myindex/mytype`. Los extremos se configuran con el administrador de inquilinos o la API de gestión de inquilinos. Tienen el siguiente formato: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` El punto final debe estar configurado antes de enviar el XML de configuración o la configuración fallará con un error 404. EL VALOR DE URN se incluye en el elemento Destination.	Sí

Utilice el XML de configuración de notificación de metadatos de ejemplo para aprender a crear su propio XML.

La configuración de notificaciones de metadatos se aplica a todos los objetos

En este ejemplo, los metadatos de objeto de todos los objetos se envían al mismo destino.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Configuración de notificaciones de metadatos con dos reglas

En este ejemplo, metadatos de objeto para objetos que coinciden con el prefijo `/images` se envía a un destino, mientras que los metadatos de objetos de los objetos que coinciden con el prefijo `/videos` se envía a un segundo destino.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Información relacionada

"USE LA API DE REST DE S3"

"Metadatos de objetos incluidos en las notificaciones de metadatos"

"JSON generado por el servicio de integración de búsqueda"

"Configure el servicio de integración de búsqueda"

Configure el servicio de integración de búsqueda

El servicio de integración de búsqueda envía metadatos de objetos a un índice de búsqueda de destino cada vez que se crea, se elimina o se actualizan sus metadatos o etiquetas.

Antes de empezar

- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un bucket S3 cuyo contenido desea indexar.
- El punto final que pretende utilizar como destino para el servicio de integración de búsqueda ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene el "Gestione todos los bloques o permisos de acceso raíz". Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar el servicio de integración de búsqueda para un bloque de origen, al crear un objeto o actualizar los metadatos o las etiquetas de un objeto se activan los metadatos de objeto que se enviarán al extremo de destino. Si habilita el servicio de integración de búsqueda para un depósito que ya contiene objetos, las notificaciones de metadatos no se envían automáticamente para los objetos existentes. Debe actualizar estos objetos existentes para asegurarse de que sus metadatos se agregan al índice de búsqueda de destino.

Pasos

1. Utilice un editor de texto para crear el XML de notificación de metadatos necesario para habilitar la integración de búsqueda.
   - Consulte la información sobre XML de configuración para la integración de búsquedas.
   - Al configurar XML, utilice URN de un extremo de integración de búsqueda como destino.

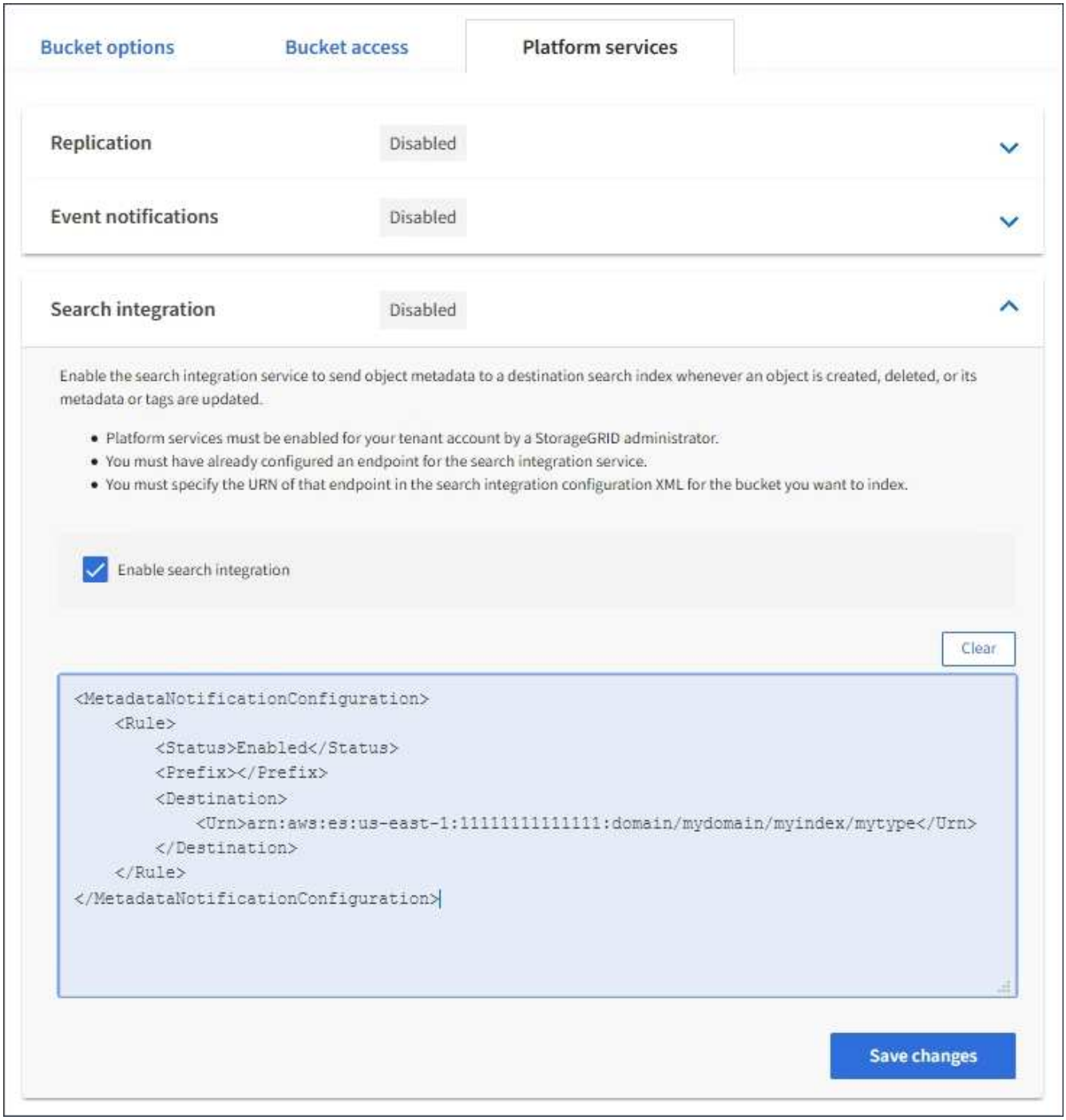
```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
3. Seleccione el nombre del bloque de origen.

   Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma** > **integración de búsqueda**
5. Seleccione la casilla de verificación **Habilitar integración de búsqueda**.

6. Pegue la configuración de notificación de metadatos en el cuadro de texto y seleccione **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de plataforma para cada cuenta de inquilino mediante Grid Manager o la API de gestión. Póngase en contacto con el administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Compruebe que el servicio de integración de búsqueda está configurado correctamente:
   a. Añada un objeto al bloque de origen que cumpla los requisitos para activar una notificación de metadatos tal y como se especifica en el XML de configuración.

      En el ejemplo mostrado anteriormente, todos los objetos añadidos al bloque activan una notificación de metadatos.

b. Confirme que se ha agregado un documento JSON que contiene los metadatos y las etiquetas del objeto al índice de búsqueda especificado en el extremo.

Después de terminar

Según sea necesario, se puede deshabilitar la integración de búsqueda para un bloque con cualquiera de los siguientes métodos:

- Seleccione **STORAGE (S3)** > **Buckets** y desactive la casilla de verificación **Enable search integration**.
- Si utiliza la API de S3 directamente, utilice una solicitud de notificación DELETE Bucket. Consulte las instrucciones para implementar aplicaciones cliente de S3.

Información relacionada

"Comprender el servicio de integración de búsquedas"

"XML de configuración para la integración de búsqueda"

"USE LA API DE REST DE S3"

"Cree un extremo de servicios de plataforma"

JSON generado por el servicio de integración de búsqueda

Al habilitar el servicio de integración de búsqueda para un bloque, se genera un documento JSON y se envía al extremo de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas del objeto.

Este ejemplo muestra un ejemplo de JSON que se podría generar cuando un objeto con la clave `SGWS/Tagging.txt` se crea en un bloque llamado `test`. La `test` el bloque no tiene versiones, por lo que el `versionId` la etiqueta está vacía.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadatos de objetos incluidos en las notificaciones de metadatos

En la tabla se enumeran todos los campos que se incluyen en el documento JSON que se envían al extremo de destino cuando la integración de búsqueda está habilitada.

El nombre del documento incluye el nombre del bloque, el nombre del objeto y el ID de versión, si existe.

Tipo	Nombre y descripción del artículo
Información sobre bloques y objetos	`bucket`: Nombre del cubo
`key`: Nombre de clave de objeto	`versionID`: Versión de objeto, para objetos en cubos con versiones
`region`: Región de cucharón, por ejemplo `us-east-1`	Metadatos del sistema
`size`: Tamaño del objeto (en bytes) visible para un cliente HTTP	`md5`: Hash de objeto
Metadatos del usuario	`metadata`: Todos los metadatos de usuario del objeto, como pares clave-valor `key:value`
Etiquetas	`tags`: Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor `key:value`

> Para las etiquetas y los metadatos de usuario, StorageGRID pasa las fechas y los números a Elasticsearch como cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para interpretar estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para la asignación dinámica de campos y para asignar formatos de fecha. Debe habilitar las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Después de indexar un documento, no puede editar los tipos de campo del documento en el índice.

USE LA API DE REST DE S3

Versiones y actualizaciones compatibles con la API de REST DE S3

StorageGRID admite la API de simple Storage Service (S3), que se implementa como un conjunto de servicios web de transferencia de estado de representación (REST).

La compatibilidad con la API REST DE S3 permite conectar las aplicaciones orientadas a servicios desarrolladas para servicios web S3 con el almacenamiento de objetos en las instalaciones que utiliza el sistema StorageGRID. Se requieren cambios mínimos en el uso actual de llamadas API DE REST DE S3 en una aplicación cliente.

Versiones compatibles

StorageGRID admite las siguientes versiones específicas de S3 y HTTP.

Elemento	Versión
Especificación de la API S3	"Documentación de Amazon Web Services (AWS): Referencia de API de Amazon simple Storage Service"
HTTP	1,1 Para obtener más información acerca de HTTP, vea HTTP/1.1 (RFC 7230-35). "RFC de IETF 2616: Protocolo de transferencia de hipertexto (HTTP/1.1)" **Nota**: StorageGRID no admite canalización HTTP/1.1.

Actualizaciones del soporte de la API de REST DE S3

Liberar	Comentarios
11,8	Se han actualizado los nombres de las operaciones S3 para que coincidan con los nombres utilizados en el "Documentación de Amazon Web Services (AWS): Referencia de API de Amazon simple Storage Service".
11,7	• Añadido "Referencia rápida: Solicitudes de API de S3 admitidas". • Se ha añadido soporte para el uso del modo de GOBIERNO con S3 Object Lock. • Se añadió compatibilidad con productos específicos de StorageGRID `x-ntap-sg-cgr-replication-status` Cabecera de respuesta para las solicitudes de objetos GET y HEAD. Este encabezado proporciona el estado de replicación de un objeto para la replicación entre grid. • Las solicitudes SelectObjectContent ahora admiten objetos de Parquet.
11,6	• Se ha agregado soporte para utilizar `partNumber` Parámetro de solicitud en GET Object y HEAD Object peticiones. • Se añadió compatibilidad con un modo de retención predeterminado y un período de retención predeterminado en el nivel de bloque para S3 Object Lock. • Se ha añadido compatibilidad con `s3:object-lock-remaining-retention-days` clave de condición de política para configurar el rango de períodos de retención permitidos para los objetos. • Se ha cambiado el tamaño máximo de *recommended* para una única operación PUT Object a 5 GiB (5.368.709.120 bytes). Si tiene objetos que sean mayores de 5 GIB, utilice la carga de varias partes en su lugar.

Liberar	Comentarios
11,5	• Se ha agregado compatibilidad para gestionar el cifrado de bloques. • Se añadió compatibilidad con el bloqueo de objetos S3 y las solicitudes de cumplimiento heredadas obsoletas. • Se ha agregado soporte para el uso DE DELETE Multiple Objects en cubos con versiones. • La `Content-MD5` el encabezado de la solicitud ahora es correctamente compatible.
11,4	• Se añadió compatibilidad con el etiquetado DE bloques DE DELETE, GET Bucket y PUT Bucket. No se admiten etiquetas de asignación de costes. • En el caso de bloques creados en StorageGRID 11.4, ya no es necesario restringir los nombres de claves de objetos para cumplir con las prácticas recomendadas de rendimiento. • Se ha agregado compatibilidad con las notificaciones de bloques en la `s3:ObjectRestore:Post` tipo de evento. • Ahora se aplican los límites de tamaño de AWS para piezas multiparte. Cada parte de una carga de varias partes debe tener entre 5 MIB y 5 GIB. La última parte puede ser menor que 5 MIB. • Añadido soporte para TLS 1,3
11,3	• Se ha añadido compatibilidad con el cifrado en el servidor de los datos de objetos con las claves proporcionadas por el cliente (SSE-C). • Se ha añadido compatibilidad para operaciones DE ELIMINACIÓN, GET y PUT Bucket Lifecycle (solo acción de caducidad) y para el `x-amz-expiration` encabezado de respuesta. • Se han actualizado PUT Object, PUT Object - Copy y Multipart Upload para describir el impacto de las reglas de ILM que utilizan la colocación síncrona en el procesamiento. • Ya no se admiten los cifrados TLS 1.1.
11,2	Compatibilidad añadida para la restauración DE objetos POSTERIOR para uso con pools de almacenamiento en cloud. Se añadió compatibilidad con el uso de la sintaxis AWS para ARN, claves de condición de política y variables de política en políticas de grupos y bloques. Se seguirán soportando las políticas de grupo y bloque existentes que utilicen la sintaxis StorageGRID. **Nota:** los usos de ARN/URN en otra configuración JSON/XML, incluidos los utilizados en las características personalizadas de StorageGRID, no han cambiado.
11,1	Se ha añadido soporte para el uso compartido de recursos de origen cruzado (CORS), HTTP para conexiones de clientes S3 a nodos de grid y configuraciones de cumplimiento en bloques.

Liberar	Comentarios
11,0	Se añadió compatibilidad para configurar servicios de plataforma (replicación de CloudMirror, notificaciones e integración de búsqueda de Elasticsearch) para los bloques. También se ha agregado soporte para las restricciones de ubicación de etiquetado de objetos para bloques y la coherencia disponible.
10,4	Se ha agregado compatibilidad con los cambios de análisis de ILM en las versiones, las actualizaciones de página de nombres de dominio de extremo, las condiciones y variables en las directivas, los ejemplos de directivas y el permiso PutOverwriteObject.
10,3	Se ha añadido compatibilidad con las versiones.
10,2	Se ha añadido compatibilidad con las políticas de acceso a grupos y bloques y para la copia de varias partes (cargar artículo - copia).
10,1	Se añadió compatibilidad con la carga de varias partes, las solicitudes de estilo hospedado virtual y la autenticación v4.
10,0	Soporte inicial de la API DE REST de S3 por parte del sistema StorageGRID.la versión actualmente admitida de *simple Storage Service API Reference* es 2006-03-01.

Referencia rápida: Solicitudes de API de S3 admitidas

En esta página se resume cómo StorageGRID admite las API de Amazon Simple Storage Service (S3).

Esta página incluye solo las operaciones S3 compatibles con StorageGRID.

> Para ver la documentación de AWS para cada operación, seleccione el enlace en el encabezado.

Parámetros de consulta URI comunes y cabeceras de solicitud

A menos que se indique lo contrario, se soportan los siguientes parámetros de consulta de URI comunes:

- `versionId` (según sea necesario para las operaciones de objeto)

A menos que se indique lo contrario, se admiten las siguientes cabeceras de solicitud comunes:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`

- `Expect`
- `Host`
- `x-amz-date`

Información relacionada

- "S3 Detalles de implementación de la API de REST"
- "Referencia de API de Amazon Simple Storage Service: Encabezados de solicitud comunes"

"AbortMultipartUpload"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes Para esta solicitud, además de este parámetro de consulta URI adicional:

- `uploadId`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones para cargas de varias partes"

"CompleteMultipartUpload"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes Para esta solicitud, además de este parámetro de consulta URI adicional:

- `uploadId`

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

- `CompleteMultipartUpload`
- `ETag`
- `Part`
- `PartNumber`

Documentación de StorageGRID

"CompleteMultipartUpload"

"CopyObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de estos encabezados adicionales:

- `x-amz-copy-source`

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"CopyObject"

"CreateBucket"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de estos encabezados adicionales:

- `x-amz-bucket-object-lock-enabled`

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en bloques"

"CreateMultipartUpload"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de estos encabezados adicionales:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"CreateMultipartUpload"

"DeleteBucket"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Documentación de StorageGRID

"Operaciones en bloques"

"DeleteBucketCors"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"DeleteBucketEncryption"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"DeleteBucketLifecycle"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

- "Operaciones en bloques"
- "Cree una configuración del ciclo de vida de S3"

"DeleteBucketPolicy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"DeleteBucketReplication"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"DeleteBucketTagging"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"DeleteObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de esta cabecera de solicitud adicional:

- `x-amz-bypass-governance-retention`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en objetos"

"DeleteObjects"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de esta cabecera de solicitud adicional:

- `x-amz-bypass-governance-retention`

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en objetos"

"DeleteObjectTagging"

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en objetos"

"GetBucketAcl"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketCors"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketEncryption"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketLifecycleConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

- "Operaciones en bloques"
- "Cree una configuración del ciclo de vida de S3"

"GetBucketLocation"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketNotificationConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketPolicy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketReplication"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"Etiquetado de GetBucketTagging"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetBucketVersioning"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"GetObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes Para esta solicitud, además de estos parámetros de consulta URI adicionales:

- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

Y estos encabezados de solicitud adicionales:

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"GetObject"

"GetObjectAcl"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en objetos"

"GetObjectLegalHold"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

"GetObjectLockConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

"GetObjectRetention"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

"GetObjectEtiquetado"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en objetos"

"Segmento de cabeza"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"Objeto principal"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de estos encabezados adicionales:

- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Objeto principal"

"ListCuchers"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

Operaciones en el servicio › ListBuckets

"ListCargas multipartitas"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de estos parámetros adicionales:

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"ListCargas multipartitas"

"ListObjects"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de estos parámetros adicionales:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"ListObjectsV2"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de estos parámetros adicionales:

- `continuation-token`
- `delimiter`
- `encoding-type`

- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"ListObjectVersions"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de estos parámetros adicionales:

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"Operaciones en bloques"

"ListParts"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de estos parámetros adicionales:

- `max-parts`
- `part-number-marker`
- `uploadId`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"ListCargas multipartitas"

"A cargo de PutBucketCors"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en bloques"

"PutBucketEncryption"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

Documentación de StorageGRID

"Operaciones en bloques"

"PutBucketLifecycleConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

- `And`
- `Days`
- `Expiration`
- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`

- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

Documentación de StorageGRID

- "Operaciones en bloques"
- "Cree una configuración del ciclo de vida de S3"

"PutBucketNotificationConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Etiquetas XML de cuerpo de solicitud

StorageGRID soporta las siguientes etiquetas XML del cuerpo de la solicitud:

- `Event`
- `Filter`
- `FilterRule`
- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

Documentación de StorageGRID

"Operaciones en bloques"

"Política de PutBucketPolicy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Para obtener detalles sobre los campos del cuerpo JSON admitidos, consulte "Utilice las políticas de acceso de bloques y grupos".

"PutBucketReplication"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Etiquetas XML de cuerpo de solicitud

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

Documentación de StorageGRID

"Operaciones en bloques"

"PutBucketTagging"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en bloques"

"PutBucketVersioning"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Parámetros de cuerpo de solicitud

StorageGRID admite los siguientes parámetros de cuerpo de solicitud:

- `VersioningConfiguration`
- `Status`

Documentación de StorageGRID

"Operaciones en bloques"

"Objeto de puta"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de estos encabezados adicionales:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Solicitar el cuerpo

- Datos binarios del objeto

Documentación de StorageGRID

"Objeto de puta"

"PutObjectLegalHold"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

"PutObjectLockConfiguration"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

"PutObjectRetention"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud, además de esta cabecera adicional:

- `x-amz-bypass-governance-retention`

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

"PutObjectEtiquetado"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

StorageGRID admite todos los parámetros de cuerpo de solicitud definidos por la API de REST DE Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en objetos"

"RestoreObject"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Para obtener más información sobre los campos de cuerpo admitidos, consulte "RestoreObject".

"SelectObjectContent"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes para esta solicitud.

Solicitar el cuerpo

Para obtener más información sobre los campos de cuerpo admitidos, consulte lo siguiente:

- "Utilice S3 Select"
- "SelectObjectContent"

"UploadPart"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes Para esta solicitud, además de estos parámetros de consulta URI adicionales:

- `partNumber`
- `uploadId`

Y estos encabezados de solicitud adicionales:

- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Solicitar el cuerpo

- Datos binarios de la pieza

Documentación de StorageGRID

"UploadPart"

"UploadPartCopy"

Parámetros de consulta URI y cabeceras de solicitud

StorageGRID admite todos parámetros y cabeceras comunes Para esta solicitud, además de estos parámetros de consulta URI adicionales:

- `partNumber`
- `uploadId`

Y estos encabezados de solicitud adicionales:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

Solicitar el cuerpo

Ninguno

Documentación de StorageGRID

"UploadPartCopy"

Probar la configuración de la API de REST S3

Puede usar la interfaz de línea de comandos (CLI de AWS) de Amazon Web Services para probar la conexión con el sistema y verificar que puede leer y escribir objetos.

Antes de empezar

- Ha descargado e instalado la CLI de AWS desde "aws.amazon.com/cli".
- Opcionalmente, tienes "se ha creado un punto final de equilibrio de carga". De lo contrario, conoce la dirección IP del nodo de almacenamiento al que desea conectarse y el número de puerto que se va a utilizar. Consulte "Puertos y direcciones IP para las conexiones de cliente".
- Ya tienes "Se ha creado una cuenta de inquilino de S3".
- Ha iniciado sesión en el inquilino y. "se creó una clave de acceso".

Para obtener más información sobre estos pasos, consulte "Configurar conexiones de cliente".

Pasos

1. Configure los ajustes de la CLI de AWS para usar la cuenta que creó en el sistema StorageGRID:
   a. Entrar al modo de configuración: `aws configure`
   b. Introduzca el ID de clave de acceso de la cuenta que creó.
   c. Introduzca la clave de acceso secreta de la cuenta que creó.
   d. Introduzca la región por defecto que se va a utilizar. Por ejemplo: `us-east-1`.
   e. Introduzca el formato de salida predeterminado que se va a utilizar o pulse **Intro** para seleccionar JSON.
2. Crear un bucket.

   En este ejemplo se supone que ha configurado un punto final de equilibrio de carga para utilizar la dirección IP 10.96.101.17 y el puerto 10443.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443
   --no-verify-ssl create-bucket --bucket testbucket
   ```

   Si el bloque se crea correctamente, se devuelve la ubicación del bloque, como se puede ver en el ejemplo siguiente:

   ```
   "Location": "/testbucket"
   ```

3. Cargue un objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Si el objeto se carga correctamente, se devuelve un ETag que es un hash de los datos del objeto.

4. Enumere el contenido del cucharón para verificar que el objeto se ha cargado.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Elimine el objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Eliminar el bloque.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Cómo StorageGRID implementa la API DE REST de S3

Solicitudes de clientes en conflicto

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias".

El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.

Valores de coherencia

La consistencia proporciona un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en distintos nodos de almacenamiento y sitios. Puede cambiar la consistencia según lo requiera la aplicación.

De forma predeterminada, StorageGRID garantiza la coherencia de lectura tras escritura de los objetos recién creados. Cualquier OBTENER después de un PUESTO completado correctamente podrá leer los datos recién escritos. Las sobrescrituras de objetos existentes, actualizaciones de metadatos y eliminaciones son coherentes en la actualidad. Por lo general, las sobrescrituras tardan segundos o minutos en propagarse, pero pueden tardar hasta 15 días.

Si desea realizar operaciones de objeto en otra coherencia, puede:

- Especifique una consistencia para cada cucharón.
- Especifique una consistencia para Cada operación de API.
- Cambie la consistencia predeterminada en toda la cuadrícula realizando una de las siguientes tareas:
  - En Grid Manager, vaya a **CONFIGURACIÓN** > **Sistema** > **Ajustes de almacenamiento** > **Consistencia predeterminada**.
  - .

> Un cambio en la consistencia de toda la cuadrícula se aplica solo a los depósitos creados después de que se haya cambiado el valor. Para determinar los detalles de un cambio, consulte el registro de auditoría ubicado en `/var/local/log` (Busque **consistencyLevel**).

Valores de coherencia

La consistencia afecta a la forma en que los metadatos que StorageGRID utiliza para rastrear objetos se distribuyen entre nodos y, por lo tanto, la disponibilidad de los objetos para las solicitudes del cliente.

Puede establecer la coherencia de un bloque o una operación de API en uno de los valores siguientes:

- **Todos**: Todos los nodos reciben los datos inmediatamente, o la solicitud fallará.
- **Strong-global**: Garantiza la consistencia de lectura tras escritura para todas las solicitudes de los clientes en todos los sitios.
- **Strong-site**: Garantiza la consistencia de lectura después de escritura para todas las solicitudes de los clientes dentro de un sitio.
- **Read-after-new-write**: (Por defecto) proporciona consistencia de lectura después de escritura para nuevos objetos y consistencia eventual para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
- **Disponible**: Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

Utilice los elementos de consistencia «Read-after-new-write» y «available»

Cuando una operación de CABEZAL u OBTENCIÓN utiliza la consistencia de lectura después de nueva escritura, StorageGRID realiza la búsqueda en varios pasos de la siguiente manera:

- Primero busca el objeto con una baja consistencia.
- Si esa búsqueda falla, repite la búsqueda en el siguiente valor de consistencia hasta que alcanza una consistencia equivalente al comportamiento para strong-global.

Si una operación HEAD u GET utiliza la coherencia «Read-after-new-write» pero el objeto no existe, la búsqueda de objetos siempre alcanzará una coherencia equivalente al comportamiento de un nivel global sólido. Debido a que esta consistencia requiere que haya disponibles varias copias de los metadatos del objeto en cada sitio, puede recibir un número elevado de errores de servidor interno 500 si hay dos o más nodos de almacenamiento en el mismo sitio disponibles.

A menos que necesite garantías de consistencia similares a Amazon S3, puede evitar estos errores para las operaciones HEAD y GET estableciendo la consistencia en “Disponible”. Cuando una operación de CABEZAL u OBTENCIÓN utiliza la consistencia «disponible», StorageGRID solo proporciona consistencia eventual. No

vuelve a intentar una operación fallida en el aumento de la coherencia, por lo que no es necesario que haya varias copias de los metadatos del objeto disponibles.

Especifique la consistencia para el funcionamiento de la API

Para configurar la coherencia de una operación de API individual, los valores de coherencia deben ser compatibles con la operación y debe especificar la coherencia en el encabezado de solicitud. Este ejemplo establece la coherencia en «sitio fuerte» para una operación GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

Debe utilizar la misma consistencia para las operaciones PutObject y GetObject.

Especificar consistencia para el bloque

Para configurar la coherencia del bloque, puede usar StorageGRID "PONGA la consistencia del cucharón" solicitud. O usted puede "cambiar la consistencia de un cucharón" Del Gestor de inquilinos.

Al establecer la coherencia de un cucharón, tenga en cuenta lo siguiente:

- La configuración de la coherencia de un bloque determina la coherencia que se usa para las operaciones S3 realizadas en los objetos del bloque o en la configuración de bloque. No afecta a las operaciones del propio cucharón.
- La coherencia de una operación API individual anula la coherencia del bloque.
- En general, los bloques deben utilizar la consistencia predeterminada «Read-after-new-write». Si las solicitudes no funcionan correctamente, cambie el comportamiento del cliente de aplicación si es posible. O bien, configure el cliente para especificar la consistencia de cada solicitud API. Defina la consistencia en el nivel del cucharón sólo como último recurso.

Cómo interactúan las reglas de coherencia e ILM para afectar a la protección de datos

Tanto la elección de coherencia como la regla de ILM afectan al modo de protección de los objetos. Estos ajustes pueden interactuar.

Por ejemplo, la consistencia utilizada cuando se almacena un objeto afecta la ubicación inicial de los metadatos del objeto, mientras que el comportamiento de procesamiento seleccionado para la regla de ILM afecta la ubicación inicial de las copias de objetos. Dado que StorageGRID requiere acceso a los metadatos de un objeto y a sus datos para satisfacer las solicitudes de los clientes, seleccionar niveles de protección correspondientes para la coherencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas del sistema más predecibles.

Lo siguiente "opciones de procesamiento" Están disponibles para reglas de ILM:

Registro doble

StorageGRID realiza de inmediato copias provisionales del objeto y devuelve la operación correcta al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Estricto

Todas las copias especificadas en la regla de ILM deben realizarse antes de devolver correctamente al cliente.

Equilibrado

StorageGRID intenta realizar todas las copias especificadas en la regla de gestión del ciclo de vida de la información durante el procesamiento; si no es posible, se realizarán copias provisionales y se devolverán correctamente al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Ejemplo de cómo pueden interactuar la regla de consistencia e ILM

Suponga que tiene un grid de dos sitios con la siguiente regla de ILM y la siguiente consistencia:

- **Norma ILM**: Cree dos copias de objetos, una en el sitio local y otra en un sitio remoto. Use un comportamiento de ingesta estricto.
- **Consistencia**: Fuerte-global (los metadatos de objetos se distribuyen inmediatamente a todos los sitios).

Cuando un cliente almacena un objeto en el grid, StorageGRID realiza copias de objetos y distribuye los metadatos en ambos sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra la pérdida en el momento del mensaje de procesamiento correcto. Por ejemplo, si el sitio local se pierde poco después del procesamiento, seguirán existiendo copias de los datos del objeto y los metadatos del objeto en el sitio remoto. El objeto se puede recuperar completamente.

Si, en cambio, utiliza la misma regla de ILM y la coherencia del sitio fuerte, es posible que el cliente reciba un mensaje de éxito después de replicar los datos de objetos en el sitio remoto, pero antes de que los metadatos de los objetos se distribuyan allí. En este caso, el nivel de protección de los metadatos de objetos no coincide con el nivel de protección de los datos de objetos. Si el sitio local se pierde poco después del procesamiento, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre las reglas de coherencia y de ILM puede ser compleja. Póngase en contacto con NetApp si necesita ayuda.

Control de versiones de objetos

Puede establecer el estado de control de versiones de un bloque si desea conservar varias versiones de cada objeto. Habilitar el control de versiones de un bloque puede ayudar a protegerse contra la eliminación accidental de objetos y permite recuperar y restaurar versiones anteriores de un objeto.

El sistema StorageGRID implementa versiones con compatibilidad para la mayoría de las funciones y con algunas limitaciones. StorageGRID admite hasta 1,000 versiones de cada objeto.

El control de versiones de objetos puede combinarse con la gestión del ciclo de vida de la información (ILM) de StorageGRID o con la configuración del ciclo de vida de bloques de S3. Debe activar el control de versiones de forma explícita para cada bloque. Cuando se habilita el control de versiones para un bloque, a cada objeto agregado al bloque se le asigna un ID de versión, que genera el sistema StorageGRID.

No se admite el uso de la autenticación multifactor (MFA).

El control de versiones solo se puede habilitar en bloques creados con StorageGRID versión 10.3 o posterior.

ILM y versiones

Las políticas de ILM se aplican a cada versión de un objeto. Un proceso de análisis de ILM analiza continuamente todos los objetos y los vuelve a evaluar en relación con la política actual de ILM. Todos los cambios realizados en las políticas de ILM se aplican a todos los objetos procesados anteriormente. Esto incluye versiones que se han ingerido previamente si la versión está activada. El análisis de ILM aplica nuevos cambios de ILM a los objetos procesados previamente.

Para los objetos S3 en bloques con control de versiones, la compatibilidad con el control de versiones le permite crear reglas de ILM que utilicen “Tiempo no corriente” como tiempo de referencia (seleccione **Sí** para la pregunta, ¿Aplicar esta regla solo a versiones de objetos anteriores?” pulg "Paso 1 del asistente Crear una regla de ILM"). Cuando se actualiza un objeto, sus versiones anteriores se vuelven no actuales. El uso de un filtro de tiempo no corriente permite crear políticas que reduzcan el impacto en el almacenamiento de las versiones anteriores de objetos.

> Cuando se carga una nueva versión de un objeto mediante una operación de carga de varias partes, la hora no actual de la versión original del objeto se refleja cuando se creó la carga de varias partes para la nueva versión, no cuando se completó la carga de varias partes. En casos limitados, la hora no actual de la versión original puede ser horas o días antes de la hora de la versión actual.

Información relacionada

- "Cómo se eliminan los objetos con versiones de S3"
- "Reglas de ILM y políticas para objetos con versiones de S3 (ejemplo 4)".

Use la API REST DE S3 para configurar el bloqueo de objetos de S3

Si la configuración global Bloqueo de objetos S3 está habilitada para el sistema StorageGRID, puede crear depósitos con Bloqueo de objetos S3 habilitado. Puede especificar la retención predeterminada para cada bloque o la configuración de retención para cada versión de objeto.

Cómo habilitar S3 Object Lock para un bucket

Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, también puede habilitar el bloqueo de objetos S3 al crear cada bloque.

S3 Bloqueo de objetos es un ajuste permanente que solo se puede activar cuando se crea un depósito. No puede agregar o deshabilitar S3 Object Lock después de crear un bucket.

Para activar el bloqueo de objetos S3 para un depósito, utilice uno de estos métodos:

- Cree el bloque con el Administrador de arrendatarios. Consulte "Crear bloque de S3".
- Cree el depósito mediante una solicitud CreateBucket con el `x-amz-bucket-object-lock-enabled` solicite el encabezado. Consulte "Operaciones en bloques".

S3 Object Lock requiere el control de versiones de bloque, que se habilita automáticamente cuando se crea el bloque. No puede suspender el control de versiones del depósito. Consulte "Control de versiones de objetos".

Configuración de retención predeterminada para un bloque

Cuando S3 Object Lock está habilitado para un depósito, puede habilitar opcionalmente la retención predeterminada para el bloque y especificar un modo de retención predeterminado y un período de retención

predeterminado.

Modo de retención predeterminado

- En modo de CUMPLIMIENTO:
  - El objeto no se puede eliminar hasta que se alcance su fecha de retención hasta.
  - La fecha de retención del objeto se puede aumentar, pero no se puede reducir.
  - No se puede eliminar la fecha de retención del objeto hasta que se alcance esa fecha.
- En modo de GOBIERNO:
  - Usuarios con `s3:BypassGovernanceRetention` el permiso puede utilizar el `x-amz-bypass-governance-retention: true` solicitar cabecera para omitir la configuración de retención.
  - Estos usuarios pueden suprimir una versión de objeto antes de alcanzar su fecha de retención hasta la fecha.
  - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

Período de retención predeterminado

Cada depósito puede tener un período de retención predeterminado especificado en años o días.

Cómo establecer la retención predeterminada para un depósito

Para definir la retención predeterminada de un depósito, utilice uno de estos métodos:

- Gestione la configuración de bloques desde el Gestor de inquilinos. Consulte "Cree un bloque de S3" y.. "Actualizar S3 Retención predeterminada de bloqueo de objetos".
- Emita una solicitud PutObjectLockConfiguration para el depósito para especificar el modo por defecto y el número por defecto de días o años.

PutObjectLockConfiguration

La solicitud PutObjectLockConfiguration le permite establecer y modificar el modo de retención predeterminado y el período de retención predeterminado para un depósito que tiene S3 Object Lock activado. También es posible eliminar los ajustes de retención predeterminados previamente configurados.

Cuando se ingieren nuevas versiones de objetos en el bloque, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` y.. `x-amz-object-lock-retain-until-date` no se han especificado. El período de retención predeterminado se utiliza para calcular el valor de retener hasta la fecha if `x-amz-object-lock-retain-until-date` no se ha especificado.

Si el período de retención predeterminado se modifica tras recibir una versión de objeto, la fecha de retención hasta la de la versión del objeto sigue siendo la misma y no se vuelve a calcular con el nuevo período de retención predeterminado.

Debe tener la `s3:PutBucketObjectLockConfiguration` permiso, o be account root, para completar esta operación.

La `Content-MD5` La cabecera de la solicitud se debe especificar en la solicitud PUT.

Ejemplo de solicitud

Este ejemplo habilita el bloqueo de objetos S3 para un depósito y establece el modo de retención predeterminado en CUMPLIMIENTO DE NORMATIVAS y el período de retención predeterminado en 6 años.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Cómo determinar la retención predeterminada de un depósito

Para determinar si S3 Object Lock está activado para un depósito y para ver el modo de retención y el período de retención predeterminados, utilice uno de estos métodos:

- Ver el depósito en el Gestor de inquilinos. Consulte "Ver S3 cubos".
- Emitir una solicitud GetObjectLockConfiguration.

GetObjectLockConfiguration

La solicitud GetObjectLockConfiguration le permite determinar si el bloqueo de objetos S3 está habilitado para un depósito y, si está activado, consulte si hay un modo de retención predeterminado y un período de retención configurado para el depósito.

Cuando se ingieren nuevas versiones de objetos en el bloque, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` no se ha especificado. El período de retención predeterminado se utiliza para calcular el valor de retener hasta la fecha if `x-amz-object-lock-retain-until-date` no se ha especificado.

Debe tener la `s3:GetBucketObjectLockConfiguration` permiso, o be account root, para completar esta operación.

Ejemplo de solicitud

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Ejemplo de respuesta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Cómo especificar la configuración de retención para un objeto

Un bucket con S3 Object Lock habilitado puede contener una combinación de objetos con y sin la configuración de retención de S3 Object Lock.

La configuración de retención en el nivel de objeto se especifica mediante la API DE REST S3. La configuración de retención de un objeto anula cualquier configuración de retención predeterminada del bloque.

Puede especificar los siguientes ajustes para cada objeto:

- **Modo de retención**: Ya sea CUMPLIMIENTO o GOBIERNO.
- **Retain-until-date**: Una fecha que especifica cuánto tiempo la versión del objeto debe ser retenida por StorageGRID.

    - En el modo de CUMPLIMIENTO DE NORMATIVAS, si la fecha de retención hasta la fecha es posterior, el objeto se puede recuperar, pero no se puede modificar ni eliminar. Se puede aumentar la fecha de retención hasta la fecha, pero esta fecha no se puede reducir ni eliminar.
    - En el modo de GOBIERNO, los usuarios con permiso especial pueden omitir la configuración Retener hasta la fecha. Pueden eliminar una versión de objeto antes de que haya transcurrido su período de retención. También pueden aumentar, disminuir o incluso eliminar la fecha de retención hasta la fecha.
- **Retención legal**: La aplicación de una retención legal a una versión de objeto bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesite poner una retención legal en un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, pero permanece en su lugar hasta que se elimina explícitamente.

  La configuración de conservación legal de un objeto es independiente del modo de retención y la retención hasta la fecha. Si una versión de objeto está bajo una conservación legal, nadie puede eliminar esa versión.

Para especificar la configuración de bloqueo de objetos S3 al agregar una versión de objeto a un depósito, emita un "Objeto de puta", "CopyObject", o. "CreateMultipartUpload" solicitud.

Puede utilizar lo siguiente:

- `x-amz-object-lock-mode`, Que puede ser CUMPLIMIENTO o GOBERNANZA (distingue entre mayúsculas y minúsculas).

  > Si especifica `x-amz-object-lock-mode`, también debe especificar `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
    - El valor retener hasta la fecha debe tener el formato `2020-08-10T21:46:00Z`. Se permiten segundos fraccionarios, pero sólo se conservan 3 dígitos decimales (precisión de milisegundos). No se permiten otros formatos ISO 8601.
    - La fecha de retención debe ser futura.
- `x-amz-object-lock-legal-hold`

  Si la conservación legal está ACTIVADA (distingue entre mayúsculas y minúsculas), el objeto se colocará bajo una retención legal. Si se HA DESACTIVADO la retención legal, no se ha colocado ningún tipo de retención legal. Cualquier otro valor produce un error 400 Bad Request (InvalidArgument).

Si utiliza alguno de estos encabezados de solicitud, tenga en cuenta estas restricciones:

- La `Content-MD5` la cabecera de la solicitud es necesaria si la hay `x-amz-object-lock-*` La cabecera de solicitud está presente en la solicitud PutObject. `Content-MD5` No es necesario para CopyObject o CreateMultipartUpload.
- Si el bloque no tiene habilitado el bloqueo de objetos S3 y un `x-amz-object-lock-*` El encabezado de la solicitud está presente, se devuelve un error de solicitud incorrecta 400 (InvalidRequest).
- La solicitud PutObject admite el uso de `x-amz-storage-class: REDUCED_REDUNDANCY` Para igualar el comportamiento de AWS. Sin embargo, cuando un objeto se procesa en un bucket con el bloqueo de objetos S3 habilitado, StorageGRID siempre ejecuta un procesamiento de compromiso doble.
- Una respuesta posterior a la versión GET o HeadObject incluirá los encabezados `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, y. `x-amz-object-lock-legal-hold`, si está

configurado y si el remitente de la solicitud tiene el correcto `s3:Get*` permisos.

Puede utilizar el `s3:object-lock-remaining-retention-days` clave de condición de política para limitar los períodos de retención mínimos y máximos permitidos para los objetos.

Cómo actualizar la configuración de retención de un objeto

Si necesita actualizar la configuración de retención legal o retención para una versión de objeto existente, puede realizar las siguientes operaciones de subrecursos de objeto:

- `PutObjectLegalHold`

  Si el nuevo valor de retención legal está ACTIVADO, el objeto se colocará bajo una retención legal. Si el valor de la retención legal está DESACTIVADO, se levanta la retención legal.

- `PutObjectRetention`
  - El valor de modo puede ser CUMPLIMIENTO o GOBIERNO (distingue entre mayúsculas y minúsculas).
  - El valor retener hasta la fecha debe tener el formato `2020-08-10T21:46:00Z`. Se permiten segundos fraccionarios, pero sólo se conservan 3 dígitos decimales (precisión de milisegundos). No se permiten otros formatos ISO 8601.
  - Si una versión de objeto tiene una fecha de retención existente, sólo puede aumentarla. El nuevo valor debe ser el futuro.

Cómo utilizar el modo de GOBIERNO

Los usuarios que tienen el `s3:BypassGovernanceRetention` El permiso puede omitir la configuración de retención activa de un objeto que utiliza el modo de GOBIERNO. Cualquier operación DELETE u PutObjectRetention debe incluir la `x-amz-bypass-governance-retention:true` solicite el encabezado. Estos usuarios pueden realizar las siguientes operaciones adicionales:

- Realice las operaciones DeleteObject o DeleteObjects para eliminar una versión de objeto antes de que haya transcurrido su período de retención.

  Los objetos que están bajo una retención legal no se pueden eliminar. La conservación legal debe estar DESACTIVADA.

- Realice operaciones PutObjectRetention que cambian el modo de una versión de objeto de GOBIERNO a CUMPLIMIENTO antes de que haya transcurrido el período de retención del objeto.

  Cambiar el modo de CUMPLIMIENTO a GOBIERNO nunca está permitido.

- Realice operaciones PutObjectRetention para aumentar, disminuir o eliminar el período de retención de una versión de objeto.

Información relacionada

- "Gestione objetos con S3 Object Lock"
- "Utilice Bloqueo de objetos S3 para retener objetos"
- "Guía del usuario de Amazon simple Storage Service: Uso del bloqueo de objetos de S3"

Cree una configuración del ciclo de vida de S3

Puede crear una configuración del ciclo de vida de S3 para controlar cuándo se eliminan objetos específicos del sistema StorageGRID.

El ejemplo sencillo de esta sección muestra cómo puede controlar una configuración del ciclo de vida de S3 cuando se eliminan ciertos objetos (caducados) de bloques S3 específicos. El ejemplo de esta sección es solo con fines ilustrativos. Para obtener información completa sobre la creación de configuraciones del ciclo de vida de S3, consulte "Guía del usuario de Amazon Simple Storage Service: Gestión del ciclo de vida de los objetos". Tenga en cuenta que StorageGRID solo admite acciones de caducidad, no admite acciones de transición.

Qué es la configuración del ciclo de vida

Una configuración de ciclo de vida es un conjunto de reglas que se aplican a los objetos en bloques de S3 específicos. Cada regla especifica qué objetos se ven afectados y cuándo caducarán dichos objetos (en una fecha específica o después de un número determinado de días).

StorageGRID admite hasta 1,000 reglas de ciclo de vida en una configuración del ciclo de vida. Cada regla puede incluir los siguientes elementos XML:

- Caducidad: Elimine un objeto cuando se alcance una fecha especificada o cuando se alcance un número especificado de días, empezando desde el momento en que se ingirió el objeto.
- NoncurrentVersionExpiration: Elimine un objeto cuando se alcance un número especificado de días, empezando desde el momento en que el objeto se volvió no actual.
- Filtro (prefijo, etiqueta)
- Estado
- ID

Cada objeto sigue la configuración de retención de un ciclo de vida de bloques de S3 o una política de ILM. Cuando se configura el ciclo de vida de un bloque de S3, las acciones de caducidad del ciclo de vida anulan la política de ILM de los objetos que coinciden con el filtro de ciclo de vida del bloque. Los objetos que no coinciden con el filtro de ciclo de vida del bloque utilizan la configuración de retención de la política de ILM. Si un objeto coincide con un filtro de ciclo de vida del bloque y no se especifica ninguna acción de caducidad explícitamente, no se utiliza la configuración de retención de la política de ILM y se implica que las versiones de los objetos se retienen permanentemente. Consulte "Ejemplo de prioridades del ciclo de vida del bloque de S3 y de una política de ILM".

Como resultado, es posible que se elimine un objeto de la cuadrícula aunque las instrucciones de colocación de una regla de ILM aún se apliquen al objeto. O bien, es posible que un objeto se conserve en la cuadrícula incluso después de que hayan transcurrido las instrucciones de colocación de ILM para el objeto. Para obtener más información, consulte "Cómo funciona ILM durante la vida de un objeto".

> La configuración del ciclo de vida de bloques se puede usar con bloques que tienen habilitado el bloqueo de objetos S3, pero la configuración del ciclo de vida de bloques no se admite para bloques compatibles con versiones anteriores.

StorageGRID admite el uso de las siguientes operaciones de bloques para gestionar las configuraciones del ciclo de vida:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration

- PutBucketLifecycleConfiguration

Cree la configuración del ciclo de vida

Como primer paso en la creación de una configuración de ciclo de vida, se crea un archivo JSON que incluye una o varias reglas. Por ejemplo, este archivo JSON incluye tres reglas, de la siguiente manera:

1. La regla 1 sólo se aplica a los objetos que coinciden con el prefijo `category1/` y que tienen un `key2` valor de `tag2`. La `Expiration` Parámetro especifica que los objetos que coinciden con el filtro caducarán a medianoche el 22 de agosto de 2020.
2. La regla 2 se aplica sólo a los objetos que coinciden con el prefijo `category2/`. La `Expiration` el parámetro especifica que los objetos que coinciden con el filtro caducarán 100 días después de que se ingieran.

   > Las reglas que especifican un número de días son relativas al momento en que se ingirió el objeto. Si la fecha actual supera la fecha de ingesta más el número de días, es posible que algunos objetos se eliminen del bloque en cuanto se aplique la configuración del ciclo de vida.

3. La regla 3 se aplica sólo a los objetos que coinciden con el prefijo `category3/`. La `Expiration` parámetro especifica que cualquier versión no actual de objetos coincidentes caducará 50 días después de que se conviertan en no actualizados.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Aplicar la configuración del ciclo de vida al bloque

Después de crear el archivo de configuración de ciclo de vida, se aplica a un depósito emitiendo una solicitud PutBucketLifecycleConfiguration.

Esta solicitud aplica la configuración del ciclo de vida del archivo de ejemplo a los objetos de un bloque denominado `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar que una configuración del ciclo de vida se ha aplicado correctamente al bloque, emita una solicitud GetBucketLifecycleConfiguration. Por ejemplo:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Una respuesta correcta muestra la configuración del ciclo de vida que acaba de aplicar.

Validar que la caducidad del ciclo de vida del bloque se aplica al objeto

Puede determinar si una regla de caducidad en la configuración del ciclo de vida se aplica a un objeto específico al emitir una solicitud PutObject, HeadObject o GetObject. Si se aplica una regla, la respuesta incluye una `Expiration` parámetro que indica cuándo caduca el objeto y qué regla de caducidad se ha coincidido.

> Dado que el ciclo de vida de los bloques anula la gestión del ciclo de vida de `expiry-date` se muestra la fecha real en la que se eliminará el objeto. Para obtener más información, consulte "Cómo se determina la retención de objetos".

Por ejemplo, esta solicitud PutObject se emitió el 22 de junio de 2020 y coloca un objeto en el `testbucket` cucharón.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La respuesta correcta indica que el objeto caducará en 100 días (01 de octubre de 2020) y que coincide con la regla 2 de la configuración del ciclo de vida.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Por ejemplo, esta solicitud HeadObject se ha utilizado para obtener metadatos para el mismo objeto en el cubo de testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La respuesta correcta incluye los metadatos del objeto e indica que el objeto caducará en 100 días y que coincide con la regla 2.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Para bloques con control de versiones activado, el `x-amz-expiration` la cabecera de respuesta sólo se aplica a las versiones actuales de los objetos.

Recomendaciones para implementar la API REST de S3

Debe seguir estas recomendaciones al implementar la API DE REST de S3 para usar con StorageGRID.

Recomendaciones para las cabezas a los objetos no existentes

Si su aplicación comprueba de forma rutinaria si existe un objeto en una ruta en la que no espera que exista realmente, debe utilizar el objeto «disponible». "coherencia". Por ejemplo, deberías utilizar la consistencia «disponible» si tu aplicación dirige una ubicación antes de colocarla.

De lo contrario, si la OPERACIÓN de CABEZAL no encuentra el objeto, es posible que reciba una cantidad alta de errores de servidor interno 500 si dos o más nodos de almacenamiento del mismo sitio no están disponibles o no se puede acceder a un sitio remoto.

Puede establecer la consistencia «disponible» para cada cubo mediante el "PONGA la consistencia del cucharón" Solicite, o bien puede especificar la coherencia en el encabezado de solicitud para una operación

de API individual.

Recomendaciones para las claves de objeto

Siga estas recomendaciones para los nombres de clave del objeto, según cuándo se creó el bloque por primera vez.

Bloques creados en StorageGRID 11,4 o versiones anteriores

- No utilice valores aleatorios como los primeros cuatro caracteres de las claves de objeto. Esto contrasta con la anterior recomendación de AWS para prefijos clave. En su lugar, utilice prefijos no aleatorios y no únicos, como `image`.
- Si sigue la recomendación anterior de AWS para utilizar caracteres aleatorios y únicos en los prefijos de clave, coloque un prefijo en las claves de objeto con un nombre de directorio. Es decir, utilice este formato:

  `mybucket/mydir/f8e3-image3132.jpg`

  En lugar de este formato:

  `mybucket/f8e3-image3132.jpg`

Bloques creados en StorageGRID 11,4 o versiones posteriores

No es necesario restringir los nombres clave de objetos para cumplir con las prácticas recomendadas de rendimiento. En la mayoría de los casos, puede utilizar valores aleatorios para los primeros cuatro caracteres de nombres de clave de objeto.

> Una excepción a esto es una carga de trabajo S3 que elimina continuamente todos los objetos después de un breve periodo de tiempo. Para minimizar el impacto en el rendimiento de este caso de uso, varíe una parte inicial del nombre de la clave cada varios miles de objetos con algo similar a la fecha. Por ejemplo, suponga que un cliente S3 normalmente escribe 2.000 objetos por segundo y la política de ciclo de vida de la gestión de la vida útil de la información o del bloque elimina los objetos al cabo de tres días. Para minimizar el impacto en el rendimiento, puede asignar un nombre a las claves utilizando un patrón como el siguiente: `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Recomendaciones para lecturas de rango

Si la "opción global para comprimir objetos almacenados" Está activado, las aplicaciones cliente S3 deben evitar realizar operaciones GetObject que especifiquen un rango de bytes devueltos. Estas operaciones de «lectura de rango» son ineficientes, puesto que StorageGRID debe descomprimir los objetos de forma efectiva para acceder a los bytes solicitados. Las operaciones GetObject que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, no es eficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden tener un tiempo de espera.

> Si necesita comprimir objetos y su aplicación cliente debe utilizar lecturas de rango, aumente el tiempo de espera de lectura de la aplicación.

Soporte para la API de REST DE Amazon S3

S3 Detalles de implementación de la API de REST

El sistema StorageGRID implementa la API de servicio de almacenamiento simple (API 2006-03-01) con compatibilidad para la mayoría de las operaciones y con algunas limitaciones. Debe comprender los detalles de la implementación al integrar las aplicaciones cliente de la API DE REST de S3.

El sistema StorageGRID admite tanto solicitudes virtuales de tipo hospedado como solicitudes de tipo path.

Gestión de fechas

La implementación de StorageGRID de la API REST de S3 solo admite formatos de fecha HTTP válidos.

El sistema StorageGRID sólo admite formatos de fecha HTTP válidos para cualquier encabezado que acepte valores de fecha. La parte horaria de la fecha puede especificarse en formato de hora media de Greenwich (GMT) o en formato de hora universal coordinada (UTC) sin desplazamiento de zona horaria (se debe especificar +0000). Si incluye el `x-amz-date` Encabezado de la solicitud, anula cualquier valor especificado en el encabezado de solicitud de fecha. Al utilizar la versión 4 de la firma de AWS, el `x-amz-date` el encabezado debe estar presente en la solicitud firmada porque no se admite el encabezado de fecha.

Encabezados de solicitud comunes

El sistema StorageGRID soporta las cabeceras de solicitud comunes definidas por "Referencia de API de Amazon Simple Storage Service: Encabezados de solicitud comunes", con una excepción.

Solicite el encabezado	Implementación
Autorización	Compatibilidad completa con la firma AWS Versión 2 Compatibilidad con la versión 4 de la firma de AWS, con las siguientes excepciones: • El valor SHA256 no se calcula para el cuerpo de la solicitud. El valor enviado por el usuario se acepta sin validación, como si fuera el valor `UNSIGNED-PAYLOAD` se había proporcionado para el `x-amz-content-sha256` encabezado.
x-amz-token de seguridad	No implementada. Retornos `XNotImplemented`.

Encabezados de respuesta comunes

El sistema StorageGRID admite todos los encabezados de respuesta comunes definidos por *simple Storage Service API Reference*, con una excepción.

Encabezado de respuesta	Implementación
x-amz-id-2	No se utiliza

Autenticar solicitudes

El sistema StorageGRID admite el acceso autenticado y anónimo a objetos mediante la

API de S3.

La API S3 admite la versión 2 de Signature y la versión 4 de Signature para autenticar solicitudes de API S3.

Las solicitudes autenticadas deben firmarse mediante su ID de clave de acceso y su clave de acceso secreta.

El sistema StorageGRID admite dos métodos de autenticación: HTTP `Authorization` encabezado y uso de parámetros de consulta.

Utilice el encabezado autorización HTTP

HTTP `Authorization` Todas las operaciones de la API de S3 utilizan el encabezado excepto las solicitudes anónimas, donde lo permite la directiva de bloques. La `Authorization` encabezado contiene toda la información de firma necesaria para autenticar una solicitud.

Utilice los parámetros de consulta

Puede utilizar parámetros de consulta para agregar información de autenticación a una URL. Esto se conoce como firma previa de la dirección URL, que se puede utilizar para otorgar acceso temporal a recursos específicos. Los usuarios con la URL prefirmada no necesitan conocer la clave de acceso secreta para acceder al recurso, lo que permite proporcionar acceso restringido de terceros a un recurso.

Operaciones en el servicio

El sistema StorageGRID admite las siguientes operaciones en el servicio.

Funcionamiento	Implementación
ListCuchers (Anteriormente llamado GET Service)	Se implementa con todo el comportamiento de la API DE REST de Amazon S3. Reservado el derecho a realizar modificaciones.
Obtenga el uso del almacenamiento	El StorageGRID "Obtenga el uso del almacenamiento" la solicitud indica la cantidad total de almacenamiento que utiliza una cuenta y para cada depósito asociado a la cuenta. Se trata de una operación en el servicio con una ruta de / y un parámetro de consulta personalizado (`?x-ntap-sg-usage`) agregado.
OPCIONES /	Las aplicaciones cliente pueden emitir `OPTIONS /` Se solicita al puerto S3 en un nodo de almacenamiento, sin proporcionar credenciales de autenticación S3, para determinar si el nodo de almacenamiento está disponible. Puede usar esta solicitud para supervisar o para permitir que los equilibradores de carga externos identifiquen cuando un nodo de almacenamiento esté inactivo.

Operaciones en bloques

El sistema StorageGRID admite un máximo de 1,000 bloques para cada cuenta de inquilino de S3.

Las restricciones de nombre de bloque siguen las restricciones de región estándar de AWS EE.UU., pero debe

restringirlas a las convenciones de nomenclatura DNS para admitir solicitudes virtuales de estilo hospedado de S3.

En la siguiente sección, se ofrece más información:

- "Guía del usuario de Amazon Simple Storage Service: Restricciones y limitaciones de buckets"
- "Configure los nombres de dominio de punto final S3"

Las operaciones ListObjects (GET Bucket) y ListObjectVersions (GET Bucket object versions) admiten StorageGRID "valores de coherencia".

Puede comprobar si las actualizaciones a la hora del último acceso están habilitadas o deshabilitadas para grupos individuales. Consulte
"HORA de último acceso al bloque DE GET".

En la siguiente tabla se describe cómo StorageGRID implementa operaciones de bloque de API DE REST de S3. Para realizar alguna de estas operaciones, se deben proporcionar las credenciales de acceso necesarias para la cuenta.

Funcionamiento	Implementación
CreateBucket	Crea un nuevo cucharón. Al crear la cuchara, se convierte en el propietario de la cuchara. • Los nombres de los bloques deben cumplir con las siguientes reglas: ◦ Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta de inquilino). ◦ Debe ser compatible con DNS. ◦ Debe incluir al menos 3 y no más de 63 caracteres. ◦ Puede ser una serie de una o más etiquetas, con etiquetas adyacentes separadas por un punto. Cada etiqueta debe comenzar y terminar con una letra minúscula o un número y solo puede utilizar letras minúsculas, números y guiones. ◦ No debe ser una dirección IP con formato de texto. ◦ No debe utilizar periodos en solicitudes de estilo alojadas virtuales. Los períodos provocarán problemas en la verificación del certificado comodín del servidor. • De forma predeterminada, los bloques se crean en la `us-east-1` región; sin embargo, puede utilizar la `LocationConstraint` elemento de solicitud en el cuerpo de solicitud para especificar una región diferente. Cuando utilice la `LocationConstraint` Elemento, debe especificar el nombre exacto de una región que se ha definido mediante el Administrador de grid o la API de gestión de grid. Póngase en contacto con el administrador del sistema si no conoce el nombre de región que debe utilizar. **Nota**: Se producirá un error si su solicitud de CreateBucket utiliza una región que no se ha definido en StorageGRID. • Puede incluir el `x-amz-bucket-object-lock-enabled` Solicite el encabezado para crear un bucket con el bloqueo de objetos S3 habilitado. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3". Debe habilitar S3 Object Lock cuando crea el bloque. No puede agregar o deshabilitar S3 Object Lock después de crear un bucket. S3 Object Lock requiere el control de versiones de bloques, que se habilita automáticamente al crear el bloque.
DeleteBucket	Elimina el cucharón.
DeleteBucketCors	Elimina la configuración de CORS para el cucharón.
DeleteBucketEncryption	Elimina el cifrado predeterminado del depósito. Los objetos cifrados existentes permanecen cifrados, pero todos los objetos nuevos agregados al depósito no están cifrados.

Funcionamiento	Implementación
DeleteBucketLifecycle	Elimina la configuración del ciclo de vida del depósito. Consulte "Cree una configuración del ciclo de vida de S3".
DeleteBucketPolicy	Suprime la política asociada al depósito.
DeleteBucketReplication	Suprime la configuración de replicación asociada al depósito.
DeleteBucketTagging	Utiliza la `tagging` subrecurso para quitar todas las etiquetas de un bloque. **Precaución**: Si se establece una etiqueta de política de ILM no predeterminada para este depósito, habrá un `NTAP-SG-ILM-BUCKET-TAG` etiqueta de segmento con un valor asignado. No emita una solicitud DeleteBucketTagging si hay un `NTAP-SG-ILM-BUCKET-TAG` etiqueta del cucharón. En su lugar, emita una solicitud PutBucketTagging con solo el `NTAP-SG-ILM-BUCKET-TAG` etiqueta y su valor asignado para eliminar todas las demás etiquetas del depósito. No modifique ni elimine el `NTAP-SG-ILM-BUCKET-TAG` etiqueta del cucharón.
GetBucketAcl	Devuelve una respuesta positiva y el ID, DisplayName y el permiso del propietario del depósito, lo que indica que el propietario tiene acceso completo al depósito.
GetBucketCors	Devuelve el `cors` configuración del bloque.
GetBucketEncryption	Devuelve la configuración de cifrado predeterminada para el depósito.
GetBucketLifecycleConfiguration (Anteriormente llamado GET Bucket Lifecycle)	Devuelve la configuración del ciclo de vida del cucharón. Consulte "Cree una configuración del ciclo de vida de S3".
GetBucketLocation	Devuelve la región que se ha definido mediante el `LocationConstraint` En la solicitud CreateBucket. Si la región del cucharón es `us-east-1`, se devuelve una cadena vacía para la región.
GetBucketNotificationConfiguration (Con el nombre anterior, GET Bucket notification)	Devuelve la configuración de notificación adjunta al depósito.
GetBucketPolicy	Devuelve la política adjunta al depósito.
GetBucketReplication	Devuelve la configuración de replicación asociada al bloque.

Funcionamiento	Implementación
Etiquetado de GetBucketTagging	Utiliza la `tagging` subrecurso para devolver todas las etiquetas de un bloque. **Precaución**: Si se establece una etiqueta de política de ILM no predeterminada para este depósito, habrá un `NTAP-SG-ILM-BUCKET-TAG` etiqueta de segmento con un valor asignado. No modifique ni elimine esta etiqueta.
GetBucketVersioning	Esta implementación usa la `versioning` subrecurso para devolver el estado de control de versiones de un bloque. • *BLANK*: El control de versiones nunca se ha activado (el bloque no está versionado) • Activado: El control de versiones está activado • Suspendido: El control de versiones se ha habilitado anteriormente y se ha suspendido
GetObjectLockConfiguration	Devuelve el modo de retención predeterminado del depósito y el período de retención predeterminado, si está configurado. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3".
Segmento de cabeza	Determina si existe un bloque y tiene permiso para acceder a él. Esta operación devuelve: • `x-ntap-sg-bucket-id`: El UUID del bloque en formato UUID. • `x-ntap-sg-trace-id`: El ID de traza único de la solicitud asociada.
ListObjects y ListObjectsV2 (Anteriormente denominado GET Bucket)	Devuelve algunos o todos (hasta 1.000) de los objetos de un cubo. La clase de almacenamiento para los objetos puede tener cualquiera de dos valores, incluso si el objeto se ingirió con la `REDUCED_REDUNDANCY` opción de clase de almacenamiento: • `STANDARD`, Que indica que el objeto se almacena en una agrupación de almacenamiento que consta de nodos de almacenamiento. • `GLACIER`, Que indica que el objeto se ha movido al bloque externo especificado por el grupo de almacenamiento en la nube. Si el bloque contiene un gran número de claves eliminadas que tienen el mismo prefijo, la respuesta podría incluir algunas `CommonPrefixes` que no contienen claves.
ListObjectVersions (Versiones de objeto GET Bucket con nombre anterior)	Con acceso DE LECTURA en un bloque, usando esta operación con el `versions` subrecurso enumera los metadatos de todas las versiones de objetos del bloque.

Funcionamiento	Implementación
A cargo de PutBucketCors	Establece la configuración de CORS para un depósito para que éste pueda atender solicitudes de origen cruzado. El uso compartido de recursos de origen cruzado (CORS) es un mecanismo de seguridad que permite a las aplicaciones web de cliente de un dominio acceder a los recursos de un dominio diferente. Por ejemplo, supongamos que se utiliza un bloque de S3 llamado `images` para almacenar gráficos. Mediante el ajuste de la configuración de CORS para `images` bloque, puede permitir que las imágenes de ese bloque se muestren en el sitio web `http://www.example.com`.
PutBucketEncryption	Establece el estado de cifrado predeterminado de un depósito existente. Cuando se habilita el cifrado a nivel de bloque, se cifran todos los objetos nuevos que se añadan al bloque.StorageGRID admite el cifrado en el lado del servidor con claves gestionadas por StorageGRID. Al especificar la regla de configuración de cifrado del servidor, defina la `SSEAlgorithm` parámetro a. `AES256`, y no utilice el `KMSMasterKeyID` parámetro. La configuración de cifrado predeterminada de bloque se omite si la solicitud de carga de objeto ya especifica cifrado (es decir, si la solicitud incluye la `x-amz-server-side-encryption-*` encabezado de solicitud).
PutBucketLifecycleConfiguration (Anteriormente llamado PUT Bucket Lifecycle)	Crea una nueva configuración de ciclo de vida para el bloque o sustituye a una configuración de ciclo de vida existente. StorageGRID admite hasta 1,000 reglas de ciclo de vida en una configuración del ciclo de vida. Cada regla puede incluir los siguientes elementos XML: • Caducidad (días, fecha, ExpiredObjectDeleteMarker) • Caducidad de versiones sin corriente (NewerNoncurrentVersions, NoncurrentDays) • Filtro (prefijo, etiqueta) • Estado • ID StorageGRID no admite estas acciones: • AbortEncompleteMultipartUpload • Transición Consulte "Cree una configuración del ciclo de vida de S3". Para comprender cómo la acción de caducidad en un ciclo de vida de bloques interactúa con las instrucciones de ubicación de ILM, consulte "Cómo funciona ILM a lo largo de la vida de un objeto". **Nota**: La configuración del ciclo de vida de la cuchara se puede utilizar con cucharones que tengan habilitado el bloqueo de objetos S3, pero la configuración del ciclo de vida de la cuchara no es compatible con cucharones legados compatibles.

Funcionamiento	Implementación

PutBucketNotificationConfiguration
 	
(Anteriormente denominado notificación PUT Bucket)
	Configura las notificaciones para el depósito mediante el XML de configuración de notificación incluido en el cuerpo de la solicitud. Debe tener en cuenta los siguientes detalles de implementación:
	
	• StorageGRID admite los temas Kafka o Amazon Simple Notification Service (Amazon SNS) como destinos. No se admiten los puntos finales de Simple Queue Service (SQS) o Amazon Lambda.
	• El destino de las notificaciones debe especificarse como URN de un extremo de StorageGRID. Se pueden crear extremos con el administrador de inquilinos o la API de gestión de inquilinos.
	
	El extremo debe existir para que la configuración de la notificación se realice correctamente. Si el extremo no existe, un `400 Bad Request` se devuelve un error con el código `InvalidArgument`.
	
	• No puede configurar una notificación para los siguientes tipos de evento. Estos tipos de evento **no** son compatibles.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar, excepto que no incluyen algunas claves y utilizan valores específicos para otros, como se muestra en la lista siguiente:
	◦ **EventSource**
	
	`sgws:s3`
	
	◦ * AwsRegion*
	
	no incluido
	
	◦ **x-amz-id-2**
	
	no incluido
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

Política de PutBucketPolicy	Define la política asociada al depósito. Consulte "Utilice las políticas de acceso de bloques y grupos".

Funcionamiento	Implementación
PutBucketReplication	Configura "Replicación de CloudMirror de StorageGRID" Para el depósito que utiliza el XML de configuración de replicación proporcionado en el cuerpo de la solicitud. Para la replicación de CloudMirror, debe tener en cuenta los siguientes detalles de la implementación: • StorageGRID solo admite V1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso de `Filter` Elemento para reglas y sigue las convenciones V1 para eliminar versiones de objetos. Para obtener más información, consulte "Guía del usuario de Amazon Simple Storage Service: Configuración de replicación". • La replicación de bloques se puede configurar en bloques con versiones o sin versiones. • Puede especificar un segmento de destino diferente en cada regla del XML de configuración de replicación. Un bloque de origen puede replicar en más de un bloque de destino. • Los bloques de destino se deben especificar como URN de extremos StorageGRID tal y como se especifica en el administrador de inquilinos o la API de gestión de inquilinos. Consulte "Configure la replicación de CloudMirror". El extremo debe existir para que la configuración de replicación se complete correctamente. Si el extremo no existe, la solicitud falla como un `400 Bad Request`. El mensaje de error indica: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • No es necesario especificar un `Role` En el XML de configuración. StorageGRID no utiliza este valor y se ignorará si se envía. • Si omite la clase de almacenamiento del XML de configuración, StorageGRID utiliza `STANDARD` clase de almacenamiento de forma predeterminada. • Si elimina un objeto del bloque de origen o elimina el propio bloque de origen, el comportamiento de replicación entre regiones es el siguiente: ◦ Si elimina el objeto o bloque antes de que se haya replicado, el objeto o bloque no se replicará y no se le notificará. ◦ Si elimina el objeto o bloque después de haber sido replicado, StorageGRID sigue el comportamiento estándar de eliminación de Amazon S3 para V1 de replicación entre regiones.

Funcionamiento	Implementación
PutBucketTagging	Utiliza la `tagging` subrecurso para agregar o actualizar un conjunto de etiquetas para un bloque. Al añadir etiquetas de bloque, tenga en cuenta las siguientes limitaciones: • Tanto StorageGRID como Amazon S3 admiten hasta 50 etiquetas por cada bloque. • Las etiquetas asociadas con un bloque deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener hasta 128 caracteres Unicode de longitud. • Los valores de etiqueta pueden tener una longitud máxima de 256 caracteres Unicode. • La clave y los valores distinguen entre mayúsculas y minúsculas. **Precaución**: Si se establece una etiqueta de política de ILM no predeterminada para este depósito, habrá un `NTAP-SG-ILM-BUCKET-TAG` etiqueta de segmento con un valor asignado. Compruebe que la `NTAP-SG-ILM-BUCKET-TAG` La etiqueta de cubo se incluye con el valor asignado en todas las solicitudes de PutBucketTagging. No modifique ni elimine esta etiqueta. **Nota**: Esta operación sobrescribirá cualquier etiqueta actual que el cubo ya tenga. Si se omite alguna etiqueta existente del conjunto, esas etiquetas se eliminarán para el cucharón.
PutBucketVersioning	Utiliza la `versioning` subrecurso para establecer el estado de control de versiones de un bloque existente. Puede establecer el estado de control de versiones con uno de los siguientes valores: • Enabled: Activa el control de versiones de los objetos del bloque. Todos los objetos que se agregan al bloque reciben un ID de versión único. • Suspendido: Desactiva el control de versiones de los objetos del bloque. Todos los objetos agregados al bloque reciben el ID de versión `null`.
PutObjectLockConfiguration	Configura o elimina el modo de retención predeterminado y el período de retención predeterminado. Si se modifica el período de retención predeterminado, la fecha de retención hasta la de las versiones de objeto existentes seguirá siendo la misma y no se volverá a calcular utilizando el nuevo período de retención predeterminado. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" para obtener información detallada.

Operaciones en objetos

Operaciones en objetos

En esta sección se describe cómo el sistema StorageGRID implementa operaciones de la API DE REST de S3 para objetos.

Las siguientes condiciones se aplican a todas las operaciones de objeto:

- StorageGRID "valores de coherencia" son compatibles con todas las operaciones de los objetos, con la excepción de lo siguiente:
  - GetObjectAcl
  - `OPTIONS /`
  - PutObjectLegalHold
  - PutObjectRetention
  - SelectObjectContent
- Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.
- Todos los objetos de un bloque StorageGRID son propiedad del propietario del bloque, incluidos los objetos creados por un usuario anónimo o por otra cuenta.
- No se puede acceder a los objetos de datos procesados en el sistema de StorageGRID a través de Swift mediante S3.

En la siguiente tabla se describe cómo StorageGRID implementa operaciones de objetos API DE REST de S3.

Funcionamiento	Implementación
DeleteObject	Autenticación multifactor (MFA) y el encabezado de respuesta `x-amz-mfa` no son compatibles. Al procesar una solicitud DeleteObject, StorageGRID intenta eliminar inmediatamente todas las copias del objeto de todas las ubicaciones almacenadas. Si se realiza correctamente, StorageGRID devuelve una respuesta al cliente inmediatamente. Si no se pueden eliminar todas las copias en 30 segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y, a continuación, indica que se ha realizado correctamente al cliente. **Creación de versiones** Para eliminar una versión específica, el solicitante debe ser el propietario del bloque y utilizar el `versionId` subrecurso. El uso de este subrecurso elimina permanentemente la versión. Si la `versionId` corresponde a un marcador de borrado, el encabezado de respuesta `x-amz-delete-marker` se devuelve establecido en `true`. • Si se elimina un objeto sin el `versionId` subrecurso en un bloque habilitado para la versión, da como resultado la generación de un marcador de borrado. La `versionId` para el marcador de borrado se devuelve mediante `x-amz-version-id` encabezado de respuesta, y el `x-amz-delete-marker` el encabezado de la respuesta se devuelve establecido en `true`. • Si se elimina un objeto sin el `versionId` subrecurso en un bloque suspendido de la versión, se produce la eliminación permanente de una versión "nula" ya existente o un marcador de borrado "nula" y la generación de un nuevo marcador de borrado "nulo". La `x-amz-delete-marker` el encabezado de la respuesta se devuelve establecido en `true`. **Nota**: En algunos casos, pueden existir varios marcadores de borrado para un objeto. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" Para obtener información sobre cómo eliminar versiones de objetos en el modo de GOBIERNO.
DeleteObjects (Anteriormente denominado DELETE Múltiples Objetos)	Autenticación multifactor (MFA) y el encabezado de respuesta `x-amz-mfa` no son compatibles. Se pueden eliminar varios objetos en el mismo mensaje de solicitud. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3" Para obtener información sobre cómo eliminar versiones de objetos en el modo de GOBIERNO.

Funcionamiento	Implementación
DeleteObjectTagging	Utiliza la `tagging` subrecurso para quitar todas las etiquetas de un objeto. **Creación de versiones** Si la `versionId` el parámetro de consulta no se especifica en la solicitud, la operación elimina todas las etiquetas de la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de eliminación, se devuelve el estado MethodNotAllowed con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.
GetObject	"GetObject"
GetObjectAcl	Si se proporcionan las credenciales de acceso necesarias para la cuenta, la operación devuelve una respuesta positiva y el ID, DisplayName y permiso del propietario del objeto, lo que indica que el propietario tiene acceso completo al objeto.
GetObjectLegalHold	"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
GetObjectRetention	"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
GetObjectEtiquetado	Utiliza la `tagging` subrecurso para devolver todas las etiquetas de un objeto. **Creación de versiones** Si la `versionId` el parámetro de consulta no se especifica en la solicitud, la operación devuelve todas las etiquetas de la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de eliminación, se devuelve el estado MethodNotAllowed con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.
Objeto principal	"Objeto principal"
RestoreObject	"RestoreObject"
Objeto de puta	"Objeto de puta"
CopyObject (Anteriormente denominado Objeto PUT - Copiar)	"CopyObject"
PutObjectLegalHold	"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

Funcionamiento	Implementación
PutObjectRetention	"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
PutObjectEtiquetado	Utiliza la `tagging` subrecurso para agregar un conjunto de etiquetas a un objeto existente. **Límites de etiqueta de objeto** Puede agregar etiquetas a nuevos objetos cuando los cargue o puede agregarlos a objetos existentes. Tanto StorageGRID como Amazon S3 admiten hasta 10 etiquetas por cada objeto. Las etiquetas asociadas a un objeto deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener hasta 128 caracteres Unicode de longitud y los valores de etiqueta pueden tener hasta 256 caracteres Unicode de longitud. La clave y los valores distinguen entre mayúsculas y minúsculas. **Comportamiento de ingesta y actualizaciones de etiquetas** Cuando utiliza PutObjectTagging para actualizar las etiquetas de un objeto, StorageGRID no vuelve a ingerir el objeto. Esto significa que no se utiliza la opción de comportamiento de ingesta especificada en la regla de ILM que coincide. Cualquier cambio en la ubicación del objeto que se active por la actualización se realice cuando los procesos de ILM normales se reevalúan el ILM en segundo plano. Esto significa que si la regla ILM utiliza la opción estricta para el comportamiento de ingesta, no se realiza ninguna acción si no se pueden realizar las ubicaciones de objetos necesarias (por ejemplo, porque una nueva ubicación requerida no está disponible). El objeto actualizado conserva su ubicación actual hasta que sea posible la colocación requerida. **Resolución de conflictos** Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación. **Creación de versiones** Si la `versionId` el parámetro de consulta no se especifica en la solicitud, la operación agrega etiquetas a la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de eliminación, se devuelve el estado MethodNotAllowed con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.
SelectObjectContent	"SelectObjectContent"

StorageGRID admite las siguientes cláusulas, tipos de datos y operadores de Amazon S3 Select para "SelectObjectContent".

> No se admiten los elementos que no aparecen en la lista.

Para obtener sintaxis, consulte "SelectObjectContent". Para obtener más información acerca de S3 Select, consulte "Documentación de AWS para S3 Select".

Solo las cuentas de inquilino con S3 Select habilitado pueden emitir consultas de SelectObjectContent. Consulte "Consideraciones y requisitos para usar S3 Select".

Cláusulas

- SELECCIONAR lista
- CLÁUSULA FROM
- Cláusula WHERE
- Cláusula LIMIT

Tipos de datos

- bool
- entero
- cadena
- flotante
- decimal, numérico
- fecha/hora

Operadores

Operadores lógicos

- Y..
- NO
- O.

Operadores de comparación

- <
- >
- ⇐
- >=
- =
- =
- <>

- !=
- ENTRE
- PULG

Operadores de comparación de patrones

- COMO
- _
- %

Operadores unitarios

- ES NULL
- NO ES NULL

Operadores de matemáticas

- +
- -
- *
- /
- %

StorageGRID sigue la prioridad del operador de Amazon S3 Select.

Funciones de agregados

- MEDIA()
- RECUENTO (*)
- MÁX.()
- MIN()
- SUMA()

Funciones condicionales

- CASO
- COALCE
- NULLIF

Funciones de conversión

- CAST (para tipo de datos compatible)

Funciones de fecha

- FECHA_AÑADIR
- DIF_FECHA

- EXTRAER
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

Funciones de cadena

- CHAR_LENGTH, CHARACTER_LENGTH
- INFERIOR
- SUBCADENA
- RECORTE
- SUPERIOR

Usar cifrado del servidor

El cifrado del lado del servidor le permite proteger los datos de objetos en reposo. StorageGRID cifra los datos mientras escribe el objeto y descifra los datos cuando accede al objeto.

Si desea utilizar el cifrado en el servidor, puede elegir una de las dos opciones mutuamente excluyentes, basándose en cómo se administran las claves de cifrado:

- **SSE (cifrado del lado del servidor con claves administradas por StorageGRID)**: Cuando se emite una solicitud de S3 para almacenar un objeto, StorageGRID cifra el objeto con una clave única. Cuando emite una solicitud S3 para recuperar el objeto, StorageGRID utiliza la clave almacenada para descifrar el objeto.
- **SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente)**: Cuando se emite una solicitud S3 para almacenar un objeto, se proporciona su propia clave de cifrado. Cuando recupera un objeto, proporciona la misma clave de cifrado que parte de la solicitud. Si las dos claves de cifrado coinciden, el objeto se descifra y se devuelven los datos del objeto.

  Mientras que StorageGRID gestiona todas las operaciones de cifrado y descifrado de objetos, debe gestionar las claves de cifrado que proporcione.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente.

> Si un objeto está cifrado con SSE o SSE-C, se ignorará cualquier configuración de cifrado a nivel de bloque o de cuadrícula.

Utilice SSE

Para cifrar un objeto con una clave única administrada por StorageGRID, se utiliza el siguiente encabezado de solicitud:

```
x-amz-server-side-encryption
```

El encabezado de solicitud SSE es compatible con las siguientes operaciones de objeto:

- "Objeto de puta"
- "CopyObject"
- "CreateMultipartUpload"

Utilice SSE-C

Para cifrar un objeto con una clave única que administra, se utilizan tres encabezados de solicitud:

Solicite el encabezado	Descripción
`x-amz-server-side-encryption-customer-algorithm`	Especifique el algoritmo de cifrado. El valor de encabezado debe ser `AES256`.
`x-amz-server-side-encryption-customer-key`	Especifique la clave de cifrado que se utilizará para cifrar o descifrar el objeto. El valor de la clave debe estar codificado en base64 de 256 bits.
`x-amz-server-side-encryption-customer-key-MD5`	Especifique el resumen MD5 de la clave de cifrado según RFC 1321, que se utiliza para garantizar que la clave de cifrado se haya transmitido sin errores. El valor del resumen MD5 debe estar codificado en base64 de 128 bits.

Las siguientes operaciones de objeto admiten los encabezados de solicitud de SSE-C:

- "GetObject"
- "Objeto principal"
- "Objeto de puta"
- "CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Consideraciones para utilizar el cifrado del servidor con claves proporcionadas por el cliente (SSE-C)

Antes de utilizar SSE-C, tenga en cuenta las siguientes consideraciones:

- Debe usar https.

> StorageGRID rechaza todas las solicitudes realizadas sobre http cuando se utilice SSE-C. Por cuestiones de seguridad, debe tener en cuenta cualquier clave que envíe accidentalmente mediante http para que se vea comprometida. Deseche la llave y gírela según corresponda.

- La ETag en la respuesta no es la MD5 de los datos del objeto.
- Debe gestionar la asignación de claves de cifrado a objetos. StorageGRID no almacena claves de cifrado. Usted es responsable del seguimiento de la clave de cifrado que usted proporciona para cada objeto.
- Si su bloque está habilitado para versionado, cada versión de objeto debe tener su propia clave de cifrado.

Usted es responsable del seguimiento de la clave de cifrado utilizada para cada versión del objeto.

- Dado que gestiona las claves de cifrado en el cliente, también debe administrar cualquier protección adicional, como la rotación de claves, en el cliente.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente.

- Si la replicación entre grid o la replicación de CloudMirror están configuradas para el bucket, no se pueden ingerir objetos SSE-C. La operación de ingesta fallará.

Información relacionada

"Guía del usuario de Amazon S3: Uso del cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C)"

CopyObject

Puede utilizar la solicitud S3 CopyObject para crear una copia de un objeto que ya está almacenado en S3. Una operación CopyObject es la misma que realizar GetObject seguido de PutObject.

Resolver conflictos

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.

Tamaño del objeto

El tamaño máximo de *recommended* para una sola operación PutObject es de 5 GiB (5.368.709.120 bytes). Si tiene objetos con un tamaño superior a 5 GiB, utilice "carga de varias partes" en su lugar.

El tamaño máximo de *supported* para una sola operación PutObject es de 5 TiB (5.497.558.138.880 bytes).

> Si actualizó desde StorageGRID 11,6 o una versión anterior, se activará la alerta S3 PUT Object size too large si intenta cargar un objeto que supere los 5 GiB. Si tiene una instalación nueva de StorageGRID 11,7 o 11,8, la alerta no se activará en este caso. Sin embargo, para alinearse con el estándar AWS S3, las versiones futuras de StorageGRID no admitirán cargas de objetos de más de 5 GiB.

Caracteres UTF-8 en los metadatos de usuario

Si una solicitud incluye (no escapadas) valores UTF-8 en el nombre de clave o el valor de los metadatos definidos por el usuario, el comportamiento de StorageGRID no está definido.

StorageGRID no analiza ni interpreta los caracteres UTF-8 escapados incluidos en el nombre de clave o el valor de los metadatos definidos por el usuario. Los caracteres UTF-8 que se han escapado se tratan como caracteres ASCII:

- Las solicitudes se realizan correctamente si los metadatos definidos por el usuario incluyen caracteres UTF-8 que se han escapado.
- StorageGRID no devuelve el `x-amz-missing-meta` encabezado si el valor interpretado del nombre o

valor de clave incluye caracteres no imprimibles.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, seguido de un par nombre-valor que contiene metadatos definidos por el usuario
- `x-amz-metadata-directive`: El valor predeterminado es `COPY`, que permite copiar el objeto y los metadatos asociados.

  Puede especificar `REPLACE` para sobrescribir los metadatos existentes al copiar el objeto o actualizar los metadatos del objeto.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: El valor predeterminado es `COPY`, que le permite copiar el objeto y todas las etiquetas.

  Puede especificar `REPLACE` para sobrescribir las etiquetas existentes al copiar el objeto o actualizar las etiquetas.

- Encabezados de solicitud de bloqueo de objetos S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si se realiza una solicitud sin estas cabeceras, se utiliza la configuración de retención por defecto del depósito para calcular el modo de versión del objeto y retener hasta la fecha. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3".

- Encabezados de solicitud SSE:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

Consulte Solicitar encabezados para el cifrado del servidor

Encabezados de solicitud no compatibles

No se admiten las siguientes cabeceras de solicitud:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-website-redirect-location`

Opciones para clase de almacenamiento

La `x-amz-storage-class` Se admite el encabezado de solicitud y afecta al número de copias de objetos que crea StorageGRID si la regla de ILM coincidente utiliza el registro doble o el equilibrado "opción de ingesta".

- `STANDARD`

  (Predeterminado) especifica una operación de procesamiento de confirmación doble cuando la regla ILM utiliza la opción Commit doble o cuando la opción equilibrada vuelve a crear copias provisionales.

- `REDUCED_REDUNDANCY`

  Especifica una operación de procesamiento de confirmación única cuando la regla de ILM utiliza la opción Commit doble o cuando la opción equilibrada vuelve a crear copias provisionales.

> Si va a procesar un objeto en un bloque con el bloqueo de objetos S3 habilitado, el `REDUCED_REDUNDANCY` opción ignorada. Si está ingiriendo un objeto en un bloque compatible heredado, el `REDUCED_REDUNDANCY` opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Uso de x-amz-copy-source en CopyObject

Si el bloque de origen y la clave, especificados en la `x-amz-copy-source` header, son diferentes del bloque y la clave de destino, se escribe una copia de los datos del objeto de origen en el destino.

Si el origen y el destino coinciden, y la `x-amz-metadata-directive` el encabezado se especifica como `REPLACE`, los metadatos del objeto se actualizan con los valores de metadatos proporcionados en la solicitud. En este caso, StorageGRID no vuelve a procesar el objeto. Esto tiene dos consecuencias importantes:

- No puede utilizar CopyObject para cifrar un objeto existente en su lugar, o para cambiar el cifrado de un objeto existente en su lugar. Si proporciona el `x-amz-server-side-encryption` cabecera o la `x-amz-server-side-encryption-customer-algorithm` Encabezamiento, StorageGRID rechaza la solicitud y devuelve `XNotImplemented`.

- No se utiliza la opción de comportamiento de procesamiento especificado en la regla de ILM que coincida. Cualquier cambio en la ubicación del objeto que se active por la actualización se realice cuando los procesos de ILM normales se reevalúan el ILM en segundo plano.

  Esto significa que si la regla ILM utiliza la opción estricta para el comportamiento de ingesta, no se realiza ninguna acción si no se pueden realizar las ubicaciones de objetos necesarias (por ejemplo, porque una nueva ubicación requerida no está disponible). El objeto actualizado conserva su ubicación actual hasta que sea posible la colocación requerida.

Solicitar encabezados para el cifrado del servidor

Si usted "usar cifrado del lado del servidor", los encabezados de solicitud que proporcione dependen de si el objeto de origen está cifrado y de si planea cifrar el objeto de destino.

- Si el objeto de origen se cifra mediante una clave proporcionada por el cliente (SSE-C), debe incluir los siguientes tres encabezados en la solicitud CopyObject, para que el objeto se pueda descifrar y copiar:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especificar `AES256`.
  - `x-amz-copy-source-server-side-encryption-customer-key`: Especifique la clave de cifrado que proporcionó cuando creó el objeto de origen.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 que proporcionó cuando creó el objeto de origen.
- Si desea cifrar el objeto de destino (la copia) con una clave única que proporciona y administra, incluya los tres encabezados siguientes:
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Especifique una nueva clave de cifrado para el objeto de destino.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la nueva clave de cifrado.

  > Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones para "utilizando cifrado del lado del servidor".

- Si desea cifrar el objeto de destino (la copia) con una clave única administrada por StorageGRID (SSE), incluya este encabezado en la solicitud CopyObject:
  - `x-amz-server-side-encryption`

  > La `server-side-encryption` no se puede actualizar el valor del objeto. En su lugar, haga una copia con un nuevo `server-side-encryption` valor con `x-amz-metadata-directive`: `REPLACE`.

Creación de versiones

Si se crea una versión del contenedor de origen, puede utilizar `x-amz-copy-source` encabezado para copiar la versión más reciente de un objeto. Para copiar una versión específica de un objeto, debe especificar explícitamente la versión que desea copiar mediante `versionId` subrecurso. Si se crea una versión del bloque de destino, la versión generada se devuelve en el `x-amz-version-id` encabezado de respuesta. Si

se suspende el control de versiones para el bloque de destino, entonces `x-amz-version-id` devuelve un valor nulo.

GetObject

Puede usar la solicitud GetObject S3 para recuperar un objeto de un bucket S3.

Objetos GetObject y multipart

Puede utilizar el `partNumber` parámetro de solicitud para recuperar una parte específica de un objeto de varias partes o segmentado. La `x-amz-mp-parts-count` el elemento de respuesta indica cuántas partes tiene el objeto.

Puede ajustar `partNumber` a 1 para objetos segmentados/multiparte y objetos no segmentados/no multiparte; sin embargo, el `x-amz-mp-parts-count` el elemento de respuesta sólo se devuelve para objetos segmentados o multipartes.

Caracteres UTF-8 en los metadatos de usuario

StorageGRID no analiza ni interpreta caracteres UTF-8 escapados en los metadatos definidos por el usuario. Las solicitudes GET para un objeto con caracteres UTF-8 que se han escapado en los metadatos definidos por el usuario no devuelven el `x-amz-missing-meta` encabezado si el nombre o valor de clave incluye caracteres no imprimibles.

Encabezado de solicitud no compatible

El siguiente encabezado de solicitud no es compatible y devuelve `XNotImplemented`:

- `x-amz-website-redirect-location`

Creación de versiones

Si es un `versionId` no se especifica el subrecurso, la operación busca la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de borrado, se devuelve un estado de no encontrado con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.

Solicitar encabezados para el cifrado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)

Utilice los tres encabezados si el objeto está cifrado con una clave única que ha proporcionado.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique la clave de cifrado del objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la clave de cifrado del objeto.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones que se deben tener en "Usar cifrado del servidor".

Comportamiento de los objetos GetObject para Cloud Storage Pool

Si un objeto se ha almacenado en un "Pool de almacenamiento en cloud", El comportamiento de una solicitud GetObject depende del estado del objeto. Consulte "Objeto principal" para obtener más detalles.

> Si un objeto está almacenado en un Pool de almacenamiento en la nube y una o más copias del objeto también existen en la cuadrícula, las solicitudes de GetObject intentarán recuperar los datos de la cuadrícula, antes de recuperarlo del Pool de almacenamiento en la nube.

Estado del objeto	Comportamiento de GetObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un pool de almacenamiento tradicional o utilizando código de borrado	`200 OK` Se recupera una copia del objeto.
Objeto en el pool de almacenamiento en cloud pero todavía no ha realizado la transición a un estado no recuperable	`200 OK` Se recupera una copia del objeto.
Objeto que ha pasado a un estado no recuperable	`403 Forbidden`, `InvalidObjectState` Utilice un "RestoreObject" solicitud para restaurar el objeto a un estado recuperable.
Objeto en proceso de restauración a partir de un estado no recuperable	`403 Forbidden`, `InvalidObjectState` Espere a que finalice la solicitud RestoreObject.
Objeto completamente restaurado en el pool de almacenamiento en cloud	`200 OK` Se recupera una copia del objeto.

Objetos de varias partes o segmentados en un pool de almacenamiento en nube

Si cargó un objeto con varias partes o StorageGRID dividió un objeto grande en segmentos, StorageGRID determina si el objeto está disponible en el pool de almacenamiento en cloud al muestrear un subconjunto de las partes o segmentos del objeto. En algunos casos, una solicitud GetObject podría devolver incorrectamente `200 OK` cuando algunas partes del objeto ya se han trasladado a un estado no recuperable o cuando algunas partes del objeto aún no se han restaurado.

En estos casos:

- Es posible que la solicitud GetObject devuelva algunos datos, pero se detenga a mitad de la transferencia.
- Es posible que se devuelva una solicitud GetObject posterior `403 Forbidden`.

GetObject y replicación entre grid

Si está utilizando "federación de grid" y.. "replicación entre grid" Está activado para un depósito, el cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud GetObject. La respuesta incluye los recursos específicos de StorageGRID `x-ntap-sg-cgr-replication-status` cabecera de respuesta,

que tendrá uno de los siguientes valores:

Cuadrícula	Estado de replicación
Origen	• **ÉXITO**: La replicación fue exitosa. • **PENDIENTE**: El objeto aún no ha sido replicado. • **FALLO**: La replicación falló con un fallo permanente. Un usuario debe resolver el error.
Destino	**REPLICA**: El objeto fue replicado desde la cuadrícula de origen.

> StorageGRID no admite el `x-amz-replication-status` encabezado.

Objeto principal

Puede utilizar la solicitud S3 HeadObject para recuperar metadatos de un objeto sin devolver el objeto en sí. Si el objeto está almacenado en un Cloud Storage Pool, puede usar HeadObject para determinar el estado de transición del objeto.

HeadObject y objetos multiparte

Puede utilizar el `partNumber` parámetro de solicitud para recuperar metadatos de una parte específica de un objeto de varias partes o segmentado. La `x-amz-mp-parts-count` el elemento de respuesta indica cuántas partes tiene el objeto.

Puede ajustar `partNumber` a 1 para objetos segmentados/multiparte y objetos no segmentados/no multiparte; sin embargo, el `x-amz-mp-parts-count` el elemento de respuesta sólo se devuelve para objetos segmentados o multipartes.

Caracteres UTF-8 en los metadatos de usuario

StorageGRID no analiza ni interpreta caracteres UTF-8 escapados en los metadatos definidos por el usuario. Las solicitudes de CABECERA para un objeto con caracteres UTF-8 que se han escapado en los metadatos definidos por el usuario no devuelven el `x-amz-missing-meta` encabezado si el nombre o valor de clave incluye caracteres no imprimibles.

Encabezado de solicitud no compatible

El siguiente encabezado de solicitud no es compatible y devuelve `XNotImplemented`:

- `x-amz-website-redirect-location`

Creación de versiones

Si es un `versionId` no se especifica el subrecurso, la operación busca la versión más reciente del objeto en un bloque con versiones. Si la versión actual del objeto es un marcador de borrado, se devuelve un estado de no encontrado con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.

Solicitar encabezados para el cifrado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)

Utilice los tres encabezados si el objeto está cifrado con una clave única que ha proporcionado.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique la clave de cifrado del objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la clave de cifrado del objeto.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones que se deben tener en "Usar cifrado del servidor".

Respuestas HeadObject para objetos de Cloud Storage Pool

Si el objeto se almacena en un "Pool de almacenamiento en cloud", se devuelven las siguientes cabeceras de respuesta:

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Los encabezados de respuesta proporcionan información sobre el estado de un objeto a medida que se mueve a un pool de almacenamiento en cloud, y que, opcionalmente, se realiza la transición a un estado no recuperable y se restaura.

Estado del objeto	Respuesta a HeadObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un pool de almacenamiento tradicional o utilizando código de borrado	`200 OK` (No se devuelve ningún encabezado de respuesta especial).

Objeto en el pool de almacenamiento en cloud pero todavía no ha realizado la transición a un estado no recuperable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: Ongoing-request="false", expire-date="sáb, 23 de julio de 20 2030 00:00:00 GMT"`
	
	Hasta que el objeto se realice la transición a un estado no recuperable, el valor de `expiry-date` se configura a una hora distante en el futuro. El sistema StorageGRID no controla la hora exacta de la transición.

Estado del objeto	Respuesta a HeadObject

El objeto ha pasado a estar en estado no recuperable, pero también existe al menos una copia en la cuadrícula	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: Ongoing-request="false", expire-date="sáb, 23 de julio de 20 2030 00:00:00 GMT"`
	
	Valor para `expiry-date` se configura a una hora distante en el futuro.
	
	Nota: Si la copia en la cuadrícula no está disponible (por ejemplo, un nodo de almacenamiento está caído), debe emitir un "RestoreObject" Solicite restaurar la copia del Cloud Storage Pool antes de poder recuperar el objeto correctamente.

El objeto ha pasado a un estado que no se puede recuperar y no existe ninguna copia en la cuadrícula	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Objeto en proceso de restauración a partir de un estado no recuperable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	'x-amz-restore: ongoing-request= 'true'

Objeto completamente restaurado en el pool de almacenamiento en cloud	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: Ongoing-request="false", expire-date="sáb, 23 de julio de 20 2018 00:00:00 GMT"`
	
	La `expiry-date` Indica si el objeto del Cloud Storage Pool regresará a un estado no recuperable.

Objetos de varias partes o segmentos en el pool de almacenamiento en cloud

Si cargó un objeto con varias partes o StorageGRID dividió un objeto grande en segmentos, StorageGRID determina si el objeto está disponible en el pool de almacenamiento en cloud al muestrear un subconjunto de las partes o segmentos del objeto. En algunos casos, una solicitud HeadObject podría devolver incorrectamente `x-amz-restore: Ongoing-request="false" cuando algunas partes del objeto ya han sido transitadas a un estado no recuperable o cuando algunas partes del objeto aún no han sido restauradas.

HeadObject y replicación entre grid

Si está utilizando "federación de grid" y.. "replicación entre grid" Está habilitado para un depósito, el cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud HeadObject. La respuesta incluye los recursos específicos de StorageGRID `x-ntap-sg-cgr-replication-status` cabecera de respuesta,

que tendrá uno de los siguientes valores:

Cuadrícula	Estado de replicación
Origen	• **ÉXITO**: La replicación fue exitosa. • **PENDIENTE**: El objeto aún no ha sido replicado. • **FALLO**: La replicación falló con un fallo permanente. Un usuario debe resolver el error.
Destino	**REPLICA**: El objeto fue replicado desde la cuadrícula de origen.

> StorageGRID no admite el `x-amz-replication-status` encabezado.

Objeto de puta

Puede utilizar la solicitud PutObject S3 para agregar un objeto a un depósito.

Resolver conflictos

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.

Tamaño del objeto

El tamaño máximo de *recommended* para una sola operación PutObject es de 5 GiB (5.368.709.120 bytes). Si tiene objetos con un tamaño superior a 5 GiB, utilice "carga de varias partes" en su lugar.

El tamaño máximo de *supported* para una sola operación PutObject es de 5 TiB (5.497.558.138.880 bytes).

> Si actualizó desde StorageGRID 11,6 o una versión anterior, se activará la alerta S3 PUT Object size too large si intenta cargar un objeto que supere los 5 GiB. Si tiene una instalación nueva de StorageGRID 11,7 o 11,8, la alerta no se activará en este caso. Sin embargo, para alinearse con el estándar AWS S3, las versiones futuras de StorageGRID no admitirán cargas de objetos de más de 5 GiB.

Tamaño de los metadatos del usuario

Amazon S3 limita el tamaño de los metadatos definidos por el usuario dentro de cada encabezado de solicitud PUT a 2 KB. StorageGRID limita los metadatos de usuario a 24 KiB. El tamaño de los metadatos definidos por el usuario se mide tomando la suma del número de bytes de la codificación UTF-8 de cada clave y valor.

Caracteres UTF-8 en los metadatos de usuario

Si una solicitud incluye (no escapadas) valores UTF-8 en el nombre de clave o el valor de los metadatos definidos por el usuario, el comportamiento de StorageGRID no está definido.

StorageGRID no analiza ni interpreta los caracteres UTF-8 escapados incluidos en el nombre de clave o el valor de los metadatos definidos por el usuario. Los caracteres UTF-8 que se han escapado se tratan como caracteres ASCII:

- Las solicitudes PutObject, CopyObject, GetObject y HeadObject se realizan correctamente si los metadatos definidos por el usuario incluyen caracteres UTF-8 que se han escapado.
- StorageGRID no devuelve el `x-amz-missing-meta` encabezado si el valor interpretado del nombre o valor de clave incluye caracteres no imprimibles.

Límites de etiqueta de objeto

Puede agregar etiquetas a nuevos objetos cuando los cargue o puede agregarlos a objetos existentes. Tanto StorageGRID como Amazon S3 admiten hasta 10 etiquetas por cada objeto. Las etiquetas asociadas a un objeto deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener hasta 128 caracteres Unicode de longitud y los valores de etiqueta pueden tener hasta 256 caracteres Unicode de longitud. La clave y los valores distinguen entre mayúsculas y minúsculas.

Propiedad del objeto

En StorageGRID, todos los objetos son propiedad de la cuenta de propietario del bloque, incluidos los objetos creados por una cuenta que no sea propietaria o un usuario anónimo.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  Al especificar `aws-chunked` para `Content-Encoding`StorageGRID no verifica los siguientes elementos:

  - StorageGRID no verifica el `chunk-signature` contra los datos del fragmento.
  - StorageGRID no verifica el valor indicado para `x-amz-decoded-content-length` contra el objeto.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  La codificación de transferencia con chunked es compatible si `aws-chunked` también se utiliza la firma de carga útil.

- `x-amz-meta-`, seguido de un par nombre-valor que contiene metadatos definidos por el usuario.

  Cuando especifique la pareja nombre-valor para los metadatos definidos por el usuario, utilice este formato general:

  ```
  x-amz-meta-name: value
  ```

Si desea utilizar la opción **Tiempo de creación definido por el usuario** como Tiempo de referencia para una regla de ILM, debe utilizar `creation-time` como nombre de los metadatos que registran cuando se creó el objeto. Por ejemplo:

```
x-amz-meta-creation-time: 1443399726
```

Valor para `creation-time` Se evalúa como segundos desde el 1 de enero de 1970.

> Una regla de ILM no puede usar un **Tiempo de creación definido por el usuario** para el Tiempo de referencia y la opción de ingesta equilibrada o estricta. Se devuelve un error cuando se crea la regla de ILM.

- `x-amz-tagging`
- Encabezados de solicitud de bloqueo de objetos de S3
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si se realiza una solicitud sin estas cabeceras, se utiliza la configuración de retención por defecto del depósito para calcular el modo de versión del objeto y retener hasta la fecha. Consulte "Use la API REST DE S3 para configurar el bloqueo de objetos de S3".
- Encabezados de solicitud SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Consulte Solicitar encabezados para el cifrado del servidor

Encabezados de solicitud no compatibles

No se admiten las siguientes cabeceras de solicitud:

- La `x-amz-acl` no se admite el encabezado de la solicitud.
- La `x-amz-website-redirect-location` el encabezado de la solicitud no es compatible y devuelve `XNotImplemented`.

Opciones para clase de almacenamiento

La `x-amz-storage-class` se admite el encabezado de la solicitud. El valor enviado para `x-amz-storage-class` Afecta la forma en que StorageGRID protege los datos de objetos durante el procesamiento y no cuántas copias persistentes del objeto se almacenan en el sistema StorageGRID (determinado por ILM).

Si la regla de ILM que coincide con un objeto ingerido utiliza la opción strict ingest, el `x-amz-storage-class` el encabezado no tiene efecto.

Se pueden utilizar los siguientes valores para `x-amz-storage-class`:

- `STANDARD` (Predeterminado)
  - **Commit** doble: Si la regla ILM especifica la opción COMMIT doble para el comportamiento de procesamiento, tan pronto como un objeto se ingiere una segunda copia de ese objeto se crea y se distribuye a un nodo de almacenamiento diferente (COMMIT doble). Cuando se evalúa el ciclo de vida de la información, StorageGRID determina si estas copias provisionales iniciales cumplen las instrucciones de colocación que se indican en la regla. Si no es así, es posible que deban realizarse copias de objetos nuevas en ubicaciones diferentes y es posible que las copias provisionales iniciales deban eliminarse.
  - **Equilibrado**: Si la regla de ILM especifica la opción Equilibrada y StorageGRID no puede hacer inmediatamente todas las copias especificadas en la regla, StorageGRID hace dos copias provisionales en diferentes nodos de almacenamiento.

    Si StorageGRID puede crear inmediatamente todas las copias de objeto especificadas en la regla de ILM (ubicación síncrona), la `x-amz-storage-class` el encabezado no tiene efecto.
- `REDUCED_REDUNDANCY`
  - **Commit doble**: Si la regla ILM especifica la opción COMMIT doble para el comportamiento de la ingesta, StorageGRID crea una única copia provisional mientras se ingiere el objeto (COMMIT único).
  - **Equilibrado**: Si la regla de ILM especifica la opción Equilibrada, StorageGRID hace una sola copia provisional solo si el sistema no puede hacer inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar una colocación síncrona, este encabezado no tiene ningún efecto.
    La `REDUCED_REDUNDANCY` Se recomienda utilizar la opción cuando la regla de ILM que coincide con el objeto crea una única copia replicada. En este caso, utilizar `REDUCED_REDUNDANCY` elimina la creación y eliminación innecesarias de una copia de objetos adicional en cada operación de procesamiento.

  Con el `REDUCED_REDUNDANCY` la opción no se recomienda en otras circunstancias. `REDUCED_REDUNDANCY` aumenta el riesgo de pérdida de datos de objetos durante el procesamiento. Por ejemplo, puede perder datos si la única copia se almacena inicialmente en un nodo de almacenamiento que falla antes de que se pueda realizar la evaluación de ILM.

> Tener solo una copia replicada durante un periodo de tiempo pone los datos en riesgo de pérdida permanente. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

Especificando `REDUCED_REDUNDANCY` sólo afecta al número de copias que se crean cuando un objeto se ingiere por primera vez. No afecta a cuántas copias del objeto se realizan cuando el objeto se evalúa mediante las políticas de ILM activas y no da lugar a que los datos se almacenen en niveles más bajos de redundancia del sistema StorageGRID.

> Si va a procesar un objeto en un bloque con el bloqueo de objetos S3 habilitado, el `REDUCED_REDUNDANCY` opción ignorada. Si está ingiriendo un objeto en un bloque compatible heredado, el `REDUCED_REDUNDANCY` opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Solicitar encabezados para el cifrado del servidor

Puede utilizar los siguientes encabezados de solicitud para cifrar un objeto con cifrado del servidor. Las opciones SSE y SSE-C son mutuamente excluyentes.

- **SSE**: Utilice el siguiente encabezado si desea cifrar el objeto con una clave única gestionada por StorageGRID.
  - `x-amz-server-side-encryption`
- **SSE-C**: Utilice los tres encabezados si desea cifrar el objeto con una clave única que proporciona y administra.
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Especifique la clave de cifrado para el nuevo objeto.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones para "utilizando cifrado del lado del servidor".

> Si un objeto está cifrado con SSE o SSE-C, se ignorará cualquier configuración de cifrado a nivel de bloque o de cuadrícula.

Creación de versiones

Si el control de versiones está habilitado para un bloque, un valor único `versionId` se genera automáticamente para la versión del objeto almacenado. Este `versionId` también se devuelve en la respuesta mediante el `x-amz-version-id` encabezado de respuesta.

Si se suspende el control de versiones, la versión del objeto se almacena con un valor nulo `versionId` y si ya existe una versión nula, se sobrescribirá.

Cálculos de firma para la cabecera de autorización

Cuando utilice la `Authorization` Encabezado Para autenticar solicitudes, StorageGRID difiere de AWS de las siguientes maneras:

- StorageGRID no requiere `host` cabeceras que se incluirán en `CanonicalHeaders`.
- StorageGRID no requiere `Content-Type` para ser incluido dentro de `CanonicalHeaders`.
- StorageGRID no requiere `x-amz-*` cabeceras que se incluirán en `CanonicalHeaders`.

> Como práctica recomendada general, incluya siempre estos encabezados en él `CanonicalHeaders` Para asegurarse de que se verifican; sin embargo, si excluye estas cabeceras, StorageGRID no devuelve un error.

Para obtener más información, consulte "Cálculos de firma para la cabecera de autorización: Transferencia de carga útil en un solo fragmento (AWS Signature versión 4)".

Información relacionada

"Gestión de objetos con ILM"

RestoreObject

Puede utilizar la solicitud S3 RestoreObject para restaurar un objeto almacenado en un Cloud Storage Pool.

Tipo de solicitud admitido

StorageGRID solo admite solicitudes RestoreObject para restaurar un objeto. No admite la `SELECT` tipo de restauración. Seleccione solicitudes de devolución `XNotImplemented`.

Creación de versiones

Opcionalmente, especifique `versionId` para restaurar una versión específica de un objeto en un bloque con versiones. Si no especifica `versionId`, se restaura la versión más reciente del objeto

Comportamiento de RestoreObject en objetos de Cloud Storage Pool

Si un objeto se ha almacenado en un "Pool de almacenamiento en cloud", Una solicitud RestoreObject tiene el siguiente comportamiento, basado en el estado del objeto. Consulte "Objeto principal" para obtener más detalles.

> Si un objeto se almacena en un pool de almacenamiento en la nube y una o más copias del objeto también existen en la cuadrícula, no es necesario restaurar el objeto emitiendo una solicitud RestoreObject. En su lugar, la copia local se puede recuperar directamente mediante una solicitud GetObject.

Estado del objeto	Comportamiento de RestoreObject
El objeto se ingiere en StorageGRID pero aún no se ha evaluado por ILM, o el objeto no está en un pool de almacenamiento cloud	`403 Forbidden`, `InvalidObjectState`
Objeto en el pool de almacenamiento en cloud pero todavía no ha realizado la transición a un estado no recuperable	`200 OK` No se han realizado cambios. **Nota**: Antes de que un objeto haya pasado a un estado no recuperable, no puedes cambiarlo `expiry-date`.

Estado del objeto	Comportamiento de RestoreObject
Objeto que ha pasado a un estado no recuperable	`202 Accepted` Restaura una copia recuperable del objeto en el Pool de almacenamiento en la nube durante la cantidad de días especificada en el cuerpo de la solicitud. Al final de este período, el objeto se devuelve a un estado no recuperable. Opcionalmente, utilice la `Tier` solicitar elemento para determinar cuánto tiempo tardará el trabajo de restauración en finalizar (`Expedited`, `Standard`, o. `Bulk`). Si no especifica `Tier`, la `Standard` se utiliza el nivel. **Importante**: Si un objeto ha sido trasladado a S3 Glacier Deep Archive o el Cloud Storage Pool utiliza almacenamiento de Azure Blob, no puede restaurarlo con el `Expedited` nivel. Se devuelve el siguiente error `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class.`
Objeto en proceso de restauración a partir de un estado no recuperable	`409 Conflict`, `RestoreAlreadyInProgress`
Objeto completamente restaurado en el pool de almacenamiento en cloud	`200 OK` **Nota:** Si un objeto ha sido restaurado a un estado recuperable, usted puede cambiar su `expiry-date` Volviendo a emitir la solicitud RestoreObject con un nuevo valor para `Days`. La fecha de restauración se actualiza en relación con la hora de la solicitud.

SelectObjectContent

Puede utilizar la solicitud S3 SelectObjectContent para filtrar el contenido de un objeto S3 en función de una simple instrucción SQL.

Para obtener más información, consulte "Referencia de API de Amazon Simple Storage Service: SelectObjectContent".

Antes de empezar

- La cuenta de inquilino tiene el permiso de S3 Select.
- Ya tienes `s3:GetObject` permiso para el objeto al que desea consultar.
- El objeto que desea consultar debe tener uno de los siguientes formatos:
  - **CSV**. Se puede utilizar tal cual o comprimir en archivos GZIP o bzip2.
  - **Parquet**. Requisitos adicionales para objetos de parquet:
    - S3 Select solo admite la compresión en columnas usando GZIP o Snappy. S3 Select no admite la compresión de objetos completos para objetos de parquet.
    - S3 La selección no es compatible con la salida de parquet. Debe especificar el formato de salida como CSV o JSON.
    - El tamaño máximo del grupo de filas sin comprimir es de 512 MB.

        - Debe utilizar los tipos de dato especificados en el esquema del objeto.
        - No puede utilizar los tipos lógicos INTERVAL, JSON, LIST, TIME o UUID.
- La expresión SQL tiene una longitud máxima de 256 KB.
- Cualquier registro de la entrada o de los resultados tiene una longitud máxima de 1 MIB.

Ejemplo de sintaxis de solicitud CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Ejemplo de sintaxis de solicitud de parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Ejemplo de consulta SQL

Esta consulta obtiene el nombre del estado, 2010 poblaciones, 2015 poblaciones estimadas y el porcentaje de cambio con respecto a los datos del censo estadounidense. Los registros del archivo que no son estados se ignoran.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Las primeras líneas del archivo a consultar, `SUB-EST2020_ALL.csv`, mire como esto:

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

Ejemplo de uso de AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Las primeras líneas del archivo de salida, `changes.csv`, mire como esto:

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

Ejemplo de uso AWS-CLI (Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

Las primeras líneas del archivo de salida, changes.csv, se ven así:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Operaciones para cargas de varias partes

Operaciones para cargas de varias partes: Información general

En esta sección se describe cómo StorageGRID admite las operaciones para cargas de varias partes.

Las siguientes condiciones y notas se aplican a todas las operaciones de carga de varias partes:

- No debe superar las 1.000 cargas simultáneas de varias partes en un solo bloque porque los resultados de las consultas ListMultipartUploads de ese bloque podrían devolver resultados incompletos.
- StorageGRID aplica los límites de tamaño de AWS para piezas multiparte. Los clientes de S3 deben seguir estas directrices:
  - Cada parte de una carga de varias partes debe estar entre 5 MIB (5,242,880 bytes) y 5 GIB (5,368,709,120 bytes).
  - La última parte puede ser más pequeña que 5 MIB (5,242,880 bytes).
  - En general, los tamaños de las piezas deben ser lo más grandes posible. Por ejemplo, utilice tamaños de parte de 5 GIB para un objeto de 100 GIB. Debido a que cada parte se considera un objeto único, el uso de piezas de gran tamaño reduce la sobrecarga de metadatos de StorageGRID.
  - En el caso de objetos de menor tamaño de 5 GIB, considere usar la carga sin varias partes.
- ILM se evalúa para cada parte de un objeto de varias partes a medida que se procesa y para el objeto como un todo cuando se completa la carga de varias partes, si la regla de ILM utiliza el equilibrado o estricto "opción de ingesta". Debe saber cómo afecta esto a la ubicación de objetos y piezas:
  - Si el ILM cambia mientras se realiza una carga de varias partes de S3 GB, es posible que algunas partes del objeto no cumplan los requisitos del ILM actuales cuando se complete la carga de varias partes. Cualquier pieza que no se coloque correctamente se pondrá en cola para volver a evaluarla y

posteriormente se moverá a la ubicación correcta.

  - Al evaluar ILM para una pieza, StorageGRID filtra el tamaño de la pieza, no el tamaño del objeto. Esto significa que las partes de un objeto se pueden almacenar en ubicaciones que no cumplan con los requisitos de ILM para el objeto como un todo. Por ejemplo, si una regla especifica que todos los objetos de 10 GB o más se almacenan a DC1 mientras que todos los objetos más pequeños se almacenan a DC2, cada parte de 1 GB de una carga de varias partes de 10 partes se almacena a DC2 en el momento de la ingesta. Sin embargo, cuando se evalúa ILM para el objeto como un todo, todas las partes del objeto se mueven a DC1.

- Todas las operaciones de carga de varias partes admiten StorageGRID "valores de coherencia".
- Según sea necesario, puede utilizar "cifrado del lado del servidor" con cargas de varias partes. Para usar SSE (cifrado en el servidor con claves gestionadas por StorageGRID), incluye el `x-amz-server-side-encryption` Cabecera de solicitud sólo en la solicitud CreateMultipartUpload. Para utilizar SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente), debe especificar los mismos tres encabezados de solicitud de clave de cifrado en la solicitud CreateMultipartUpload y en cada solicitud subsiguiente UploadPart.

Funcionamiento	Implementación
AbortMultipartUpload	Se implementa con todo el comportamiento de la API DE REST de Amazon S3. Reservado el derecho a realizar modificaciones.
CompleteMultipartUpload	Consulte "CompleteMultipartUpload"
CreateMultipartUpload (Anteriormente denominado Iniciar carga de varias partes)	Consulte "CreateMultipartUpload"
ListCargas multipartitas	Consulte "ListCargas multipartitas"
ListParts	Se implementa con todo el comportamiento de la API DE REST de Amazon S3. Reservado el derecho a realizar modificaciones.
UploadPart	Consulte "UploadPart"
UploadPartCopy	Consulte "UploadPartCopy"

CompleteMultipartUpload

La operación CompleteMultipartUpload completa una carga de varias partes de un objeto mediante el ensamblaje de las piezas cargadas anteriormente.

Resolver conflictos

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de S3 comienzan una operación.

Solicitar encabezados

La `x-amz-storage-class` Se admite el encabezado de solicitud y afecta al número de copias de objeto que crea StorageGRID si la regla de ILM coincidente especifica el Confirmación doble o Equilibrado "opción de ingesta".

- `STANDARD`

  (Predeterminado) especifica una operación de procesamiento de confirmación doble cuando la regla ILM utiliza la opción Commit doble o cuando la opción equilibrada vuelve a crear copias provisionales.

- `REDUCED_REDUNDANCY`

  Especifica una operación de procesamiento de confirmación única cuando la regla de ILM utiliza la opción Commit doble o cuando la opción equilibrada vuelve a crear copias provisionales.

  > Si va a procesar un objeto en un bloque con el bloqueo de objetos S3 habilitado, el `REDUCED_REDUNDANCY` opción ignorada. Si está ingiriendo un objeto en un bloque compatible heredado, el `REDUCED_REDUNDANCY` opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

> Si no se completa una carga de varias partes en un plazo de 15 días, la operación se Marca como inactiva y todos los datos asociados se eliminan del sistema.

> La `ETag` El valor devuelto no es una suma MD5 de los datos, sino que sigue a la implementación de API de Amazon S3 de `ETag` valor para objetos de varias piezas.

Creación de versiones

Esta operación completa una carga de varias partes. Si el control de versiones está activado para un depósito, la versión del objeto se crea después de completar la carga de varias partes.

Si el control de versiones está habilitado para un bloque, un valor único `versionId` se genera automáticamente para la versión del objeto almacenado. Este `versionId` también se devuelve en la respuesta mediante el `x-amz-version-id` encabezado de respuesta.

Si se suspende el control de versiones, la versión del objeto se almacena con un valor nulo `versionId` y si ya existe una versión nula, se sobrescribirá.

> Cuando se habilita el control de versiones para un bloque, al completar una carga de varias partes siempre se crea una versión nueva, incluso si hay cargas simultáneas de varias partes completadas en la misma clave de objeto. Cuando el control de versiones no está habilitado para un bloque, es posible iniciar una carga de varias partes y, a continuación, hacer que se inicie y finalice otra carga de varias partes primero en la misma clave de objeto. En cubos sin versiones, la carga de varias partes que finaliza por última vez tiene prioridad.

Error en la replicación, notificación o notificación de metadatos

Si el bloque donde se produce la carga de varias partes está configurado para un servicio de plataforma, la carga de varias partes se realiza correctamente incluso si la acción de replicación o notificación asociada falla.

Si esto ocurre, se genera una alarma en el administrador de grid en eventos totales (SMTT). El último mensaje de evento muestra un error al publicar notificaciones para la clave bucket-nameobject para el último objeto cuya notificación falló. (Para ver este mensaje, seleccione **NODES** > ***Storage Node*** > **Events**. Ver último evento en la parte superior de la tabla). Los mensajes de eventos también se muestran en la `/var/local/log/bycast-err.log`.

Un inquilino puede activar la replicación o notificación con errores actualizando los metadatos o las etiquetas del objeto. Un arrendatario puede volver a enviar los valores existentes para evitar realizar cambios no deseados.

CreateMultipartUpload

La operación CreateMultipartUpload (anteriormente denominada Iniciar carga de varias partes) inicia una carga de varias partes para un objeto y devuelve un ID de carga.

La `x-amz-storage-class` se admite el encabezado de la solicitud. El valor enviado para `x-amz-storage-class` Afecta la forma en que StorageGRID protege los datos de objetos durante el procesamiento y no cuántas copias persistentes del objeto se almacenan en el sistema StorageGRID (determinado por ILM).

Si la regla de ILM que coincide con un objeto ingerido utiliza el estricto "opción de ingesta", la `x-amz-storage-class` el encabezado no tiene efecto.

Se pueden utilizar los siguientes valores para `x-amz-storage-class`:

- `STANDARD` (Predeterminado)
  - **Confirmación doble**: Si la regla ILM especifica la opción de ingesta de confirmación doble, tan pronto como se ingiere un objeto, se crea una segunda copia de ese objeto y se distribuye a un nodo de almacenamiento diferente (confirmación doble). Cuando se evalúa el ciclo de vida de la información, StorageGRID determina si estas copias provisionales iniciales cumplen las instrucciones de colocación que se indican en la regla. Si no es así, es posible que deban realizarse copias de objetos nuevas en ubicaciones diferentes y es posible que las copias provisionales iniciales deban eliminarse.
  - **Equilibrado**: Si la regla de ILM especifica la opción Equilibrada y StorageGRID no puede hacer inmediatamente todas las copias especificadas en la regla, StorageGRID hace dos copias provisionales en diferentes nodos de almacenamiento.

    Si StorageGRID puede crear inmediatamente todas las copias de objeto especificadas en la regla de ILM (ubicación síncrona), la `x-amz-storage-class` el encabezado no tiene efecto.
- `REDUCED_REDUNDANCY`
  - **Confirmación doble**: Si la regla de ILM especifica la opción Confirmación doble, StorageGRID crea una sola copia provisional a medida que se ingiere el objeto (confirmación única).
  - **Equilibrado**: Si la regla de ILM especifica la opción Equilibrada, StorageGRID hace una sola copia provisional solo si el sistema no puede hacer inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar una colocación síncrona, este encabezado no tiene ningún efecto.
    La `REDUCED_REDUNDANCY` Se recomienda utilizar la opción cuando la regla de ILM que coincide con el objeto crea una única copia replicada. En este caso, utilizar `REDUCED_REDUNDANCY` elimina la creación y eliminación innecesarias de una copia de objetos adicional en cada operación de procesamiento.

  Con el `REDUCED_REDUNDANCY` la opción no se recomienda en otras circunstancias.

`REDUCED_REDUNDANCY` aumenta el riesgo de pérdida de datos de objetos durante el procesamiento. Por ejemplo, puede perder datos si la única copia se almacena inicialmente en un nodo de almacenamiento que falla antes de que se pueda realizar la evaluación de ILM.

> Tener solo una copia replicada durante un periodo de tiempo pone los datos en riesgo de pérdida permanente. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

Especificando `REDUCED_REDUNDANCY` sólo afecta al número de copias que se crean cuando un objeto se ingiere por primera vez. No afecta a cuántas copias del objeto se realizan cuando el objeto se evalúa mediante las políticas de ILM activas y no da lugar a que los datos se almacenen en niveles más bajos de redundancia del sistema StorageGRID.

> Si va a procesar un objeto en un bloque con el bloqueo de objetos S3 habilitado, el `REDUCED_REDUNDANCY` opción ignorada. Si está ingiriendo un objeto en un bloque compatible heredado, el `REDUCED_REDUNDANCY` opción devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Se admiten los siguientes encabezados de solicitud:

- `Content-Type`
- `x-amz-meta-`, seguido de un par nombre-valor que contiene metadatos definidos por el usuario

  Cuando especifique la pareja nombre-valor para los metadatos definidos por el usuario, utilice este formato general:

  ```
  x-amz-meta-_name_: `value`
  ```

  Si desea utilizar la opción **Tiempo de creación definido por el usuario** como Tiempo de referencia para una regla de ILM, debe utilizar `creation-time` como nombre de los metadatos que registran cuando se creó el objeto. Por ejemplo:

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  Valor para `creation-time` Se evalúa como segundos desde el 1 de enero de 1970.

  > Adición `creation-time` Como metadatos definidos por el usuario no se permite si va a agregar un objeto a un bloque que tiene la conformidad heredada habilitada. Se devolverá un error.

- Encabezados de solicitud de bloqueo de objetos S3:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

Si se realiza una solicitud sin estos encabezados, la configuración de retención predeterminada del bloque se utiliza para calcular la versión del objeto mantener hasta la fecha.

"Use la API REST DE S3 para configurar el bloqueo de objetos de S3"

- Encabezados de solicitud SSE:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

  Solicitar encabezados para el cifrado del servidor

> Para obtener más información sobre cómo StorageGRID trata los caracteres UTF-8, consulte "Objeto de puta".

Solicitar encabezados para el cifrado del servidor

Puede utilizar los siguientes encabezados de solicitud para cifrar un objeto de varias partes con cifrado del servidor. Las opciones SSE y SSE-C son mutuamente excluyentes.

- **SSE**: Utilice el siguiente encabezado en la solicitud CreateMultipartUpload si desea cifrar el objeto con una clave única gestionada por StorageGRID. No especifique esta cabecera en ninguna de las solicitudes de artículo de carga.
  - `x-amz-server-side-encryption`
- **SSE-C**: Utilice los tres encabezados en la solicitud CreateMultipartUpload (y en cada solicitud subsiguiente UploadPart) si desea cifrar el objeto con una clave única que proporcione y administre.
  - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Especifique la clave de cifrado para el nuevo objeto.
  - `x-amz-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.

> Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones para "utilizando cifrado del lado del servidor".

Encabezados de solicitud no compatibles

El siguiente encabezado de solicitud no es compatible y devuelve `XNotImplemented`

- `x-amz-website-redirect-location`

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas,

cargar piezas, ensamblar las piezas cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

ListCargas multipartitas

La operación ListMultipartUploads muestra las cargas de varias partes en curso para un bloque.

Se admiten los siguientes parámetros de solicitud:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas, cargar piezas, ensamblar las piezas cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

UploadPart

La operación UploadPart carga una pieza en una carga de varias partes para un objeto.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `Content-Length`
- `Content-MD5`

Solicitar encabezados para el cifrado del servidor

Si especificó el cifrado SSE-C para la solicitud CreateMultipartUpload, también debe incluir los siguientes encabezados de solicitud en cada solicitud UploadPart:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique la misma clave de cifrado que proporcionó en la solicitud CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el mismo resumen de MD5 que proporcionó en la solicitud CreateMultipartUpload.

Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones que se deben tener en "Usar cifrado del servidor".

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas, cargar piezas, ensamblar las piezas cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

UploadPartCopy

La operación UploadPartCopy carga una parte de un objeto copiando datos de un objeto existente como origen de datos.

La operación UploadPartCopy se implementa con todo el comportamiento de la API DE REST DE Amazon S3. Reservado el derecho a realizar modificaciones.

Esta solicitud lee y escribe los datos del objeto especificados en `x-amz-copy-source-range` En el sistema StorageGRID.

Se admiten los siguientes encabezados de solicitud:

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Solicitar encabezados para el cifrado del servidor

Si especificó el cifrado SSE-C para la solicitud CreateMultipartUpload, también debe incluir los siguientes encabezados de solicitud en cada solicitud UploadPartCopy:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique la misma clave de cifrado que proporcionó en la solicitud CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el mismo resumen de MD5 que proporcionó en la solicitud CreateMultipartUpload.

Si el objeto de origen se cifra utilizando una clave proporcionada por el cliente (SSE-C), debe incluir los siguientes tres encabezados en la solicitud UploadPartCopy, para que el objeto se pueda descifrar y copiar:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: Especifique la clave de cifrado que proporcionó cuando creó el objeto de origen.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Especifique el resumen MD5 que proporcionó cuando creó el objeto de origen.

Las claves de cifrado que proporcione no se almacenan nunca. Si pierde una clave de cifrado, perderá el objeto correspondiente. Antes de utilizar las claves proporcionadas por el cliente para proteger los datos de objetos, revise las consideraciones que se deben tener en "Usar cifrado del servidor".

Creación de versiones

La carga de varias partes consiste en operaciones independientes para iniciar la carga, enumerar cargas, cargar piezas, ensamblar las piezas cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación CompleteMultipartUpload.

Respuestas de error

El sistema StorageGRID es compatible con todas las respuestas de error estándar de la API DE REST de S3 que se aplican. Además, la implementación de StorageGRID añade varias respuestas personalizadas.

códigos de error API de S3 admitidos

Nombre	Estado de HTTP
ACCESSDENIED	403 Prohibido
BadDigest	400 solicitud incorrecta
BucketAlreadyExists	409 conflicto
BucketNotEmpty	409 conflicto
IncompleteBody	400 solicitud incorrecta
Internalerror	500 error de servidor interno
InvalidAccessKeyId	403 Prohibido
InvalidArgument	400 solicitud incorrecta
InvalidBucketName	400 solicitud incorrecta
InvalidBucketState	409 conflicto
InvalidDigest	400 solicitud incorrecta
InvalidEncryptionAlgorithmError	400 solicitud incorrecta
InvalidPart	400 solicitud incorrecta

Nombre	Estado de HTTP
InvalidPartOrder	400 solicitud incorrecta
InvalidRange	416 rango solicitado no utilizable
InvalidRequest	400 solicitud incorrecta
InvalidStorageClass	400 solicitud incorrecta
InvalidTag	400 solicitud incorrecta
InvalidURI	400 solicitud incorrecta
KeyTooLong	400 solicitud incorrecta
MalformedXML	400 solicitud incorrecta
MetadataTooLarge	400 solicitud incorrecta
MethodNotAllowed	405 método no permitido
MissingContentLength	411 longitud requerida
MissingRequestBodyError	400 solicitud incorrecta
MissingSecurityHeader	400 solicitud incorrecta
NoSuchBucket	404 no encontrado
NoSuchKey	404 no encontrado
NoSuchUpload	404 no encontrado
NotImplimed	501 no implementada
NoSuchBucketPolicy	404 no encontrado
ObjectLockConfigurationNotFoundError	404 no encontrado
Error de precondiciónError	Error de condición 412
RequestTimeTooSowed	403 Prohibido
ServiceUnavailable	503 Servicio no disponible

Nombre	Estado de HTTP
SignatureDoesNotMatch	403 Prohibido
Cucharones TooMany	400 solicitud incorrecta
UserKeyMustBeSpecified	400 solicitud incorrecta

códigos de error personalizados de StorageGRID

Nombre	Descripción	Estado de HTTP
XBucketLifecycleNotAllowed	No se permite la configuración del ciclo de vida de los bloques en un bloque compatible heredado	400 solicitud incorrecta
XBucketPolicyParseException	Error al analizar la política JSON de bloques recibidos.	400 solicitud incorrecta
XCondit. Cumplimiento	Operación denegada debido a la configuración de cumplimiento anterior.	403 Prohibido
XDSLA ReducedRedundancyForbidden	No se permite una redundancia reducida en el bloque compatible con la tecnología heredada	400 solicitud incorrecta
XMaxBucketPolicyLengthExceeded	Su política supera la longitud máxima permitida de la política de bloques.	400 solicitud incorrecta
XMissingInternalRequestHeader	Falta un encabezado de una solicitud interna.	400 solicitud incorrecta
Cumplimiento de XNoSuchBucketCompliance	El bloque especificado no tiene la conformidad heredada activada.	404 no encontrado
XNotAcceptable	La solicitud contiene uno o más encabezados de aceptación que no se han podido satisfacer.	406 no aceptable
XNotImplemed	La solicitud que ha proporcionado implica una funcionalidad que no se ha implementado.	501 no implementada

Operaciones personalizadas de StorageGRID

Operaciones personalizadas de StorageGRID: Información general

El sistema StorageGRID admite operaciones personalizadas que se añaden a la API DE

REST DE la versión S3.

La siguiente tabla enumera las operaciones personalizadas que admite StorageGRID.

Funcionamiento	Descripción
"OBTENGA coherencia de bloques"	Devuelve la coherencia aplicada a un bloque determinado.
"PONGA la consistencia del cucharón"	Establece la coherencia aplicada a un bloque determinado.
"HORA de último acceso al bloque DE GET"	Devuelve si las actualizaciones del último tiempo de acceso están habilitadas o deshabilitadas para un bloque en particular.
"PUT Bucket última hora de acceso"	Permite habilitar o deshabilitar las actualizaciones del último tiempo de acceso para un bloque en particular.
"DELETE bucket metadata notification Configuration"	Elimina el XML de configuración de notificación de metadatos asociado a un bloque en particular.
"OBTENGA la configuración de notificación de metadatos del bloque de datos"	Devuelve el XML de configuración de notificación de metadatos asociado a un bloque determinado.
"Configuración de notificaciones de metadatos de PUT Bucket"	Configura el servicio de notificación de metadatos para un bloque.
"Obtenga el uso del almacenamiento"	Indica la cantidad total de almacenamiento que utiliza una cuenta y para cada depósito asociado a la cuenta.
"Obsoleto: CreateBucket con configuración de cumplimiento"	Obsoleto y no compatible: Ya no puede crear nuevos bloques con el cumplimiento de normativas habilitado.
"En desuso: OBTENGA el cumplimiento de normativas de bloques"	Obsoleto pero compatible: Devuelve la configuración de cumplimiento vigente para un bloque compatible existente.
"Obsoleto: PUT Bucket Compliance"	Obsoleto pero compatible: Permite modificar la configuración de cumplimiento de un bloque compatible heredado.

OBTENGA coherencia de bloques

La solicitud OBTENER coherencia de bloques permite determinar la coherencia que se aplica a un bloque en particular.

La consistencia predeterminada se establece en garantía de lectura tras escritura para los objetos recién creados.

Debe tener el permiso s3:GetBucketConsistency, o bien ser la raíz de la cuenta, para completar esta operación.

Ejemplo de solicitud

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Respuesta

En la respuesta XML, `<Consistency>` devolverá uno de los siguientes valores:

Coherencia	Descripción
todo	Todos los nodos reciben los datos inmediatamente o se produce un error en la solicitud.
fuerte en todo el mundo	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente en todos los sitios.
sitio seguro	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.
lectura-después-nueva-escritura	(Predeterminado) proporciona coherencia de lectura tras escritura para los nuevos objetos y coherencia final para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
disponible	Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

Ejemplo de respuesta

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Información relacionada

"Valores de coherencia"

PONGA la consistencia del cucharón

La solicitud COLOCAR coherencia de bloques permite especificar la coherencia que se debe aplicar a las operaciones realizadas en un bloque.

La consistencia predeterminada se establece en garantía de lectura tras escritura para los objetos recién creados.

Antes de empezar

Debe tener el permiso s3:PutBucketConsistency, o bien ser la raíz de la cuenta, para completar esta operación.

Solicitud

La `x-ntap-sg-consistency` el parámetro debe contener uno de los siguientes valores:

Coherencia	Descripción
todo	Todos los nodos reciben los datos inmediatamente o se produce un error en la solicitud.
fuerte en todo el mundo	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente en todos los sitios.
sitio seguro	Garantiza la coherencia de lectura tras escritura para todas las solicitudes del cliente dentro de un sitio.
lectura-después-nueva-escritura	(Predeterminado) proporciona coherencia de lectura tras escritura para los nuevos objetos y coherencia final para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.

Coherencia	Descripción
disponible	Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

Nota: En general, debes usar la consistencia de “Leer después de la nueva escritura”. Si las solicitudes no funcionan correctamente, cambie el comportamiento del cliente de aplicación si es posible. O bien, configure el cliente para especificar la consistencia de cada solicitud API. Defina la consistencia en el nivel del cucharón sólo como último recurso.

Ejemplo de solicitud

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Información relacionada

"Valores de coherencia"

HORA de último acceso al bloque DE GET

La solicitud DE tiempo DE acceso del último bloque DE GET Bucket permite determinar si las actualizaciones de la última hora de acceso están habilitadas o deshabilitadas para bloques individuales.

Para completar esta operación, debe tener el permiso s3:GetBucketLastAccessTime, o ser la raíz de la cuenta.

Ejemplo de solicitud

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ejemplo de respuesta

Este ejemplo muestra que las actualizaciones de la última hora de acceso están habilitadas para el bloque.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

PUT Bucket última hora de acceso

La solicitud DE la última hora de acceso al bloque DE PUT permite habilitar o deshabilitar las actualizaciones del último tiempo de acceso para bloques individuales. Al deshabilitar las actualizaciones de la última hora de acceso, se mejora el rendimiento, y es la configuración predeterminada para todos los bloques creados con la versión 10.3.0 o posterior.

Para completar esta operación, debe tener el permiso s3:PutBucketLastAccessTime para un bloque o ser raíz de cuenta.

> A partir de la versión 10.3 de StorageGRID, las actualizaciones de la última hora de acceso se deshabilitan de forma predeterminada para todos los bloques nuevos. Si tiene bloques que se crearon con una versión anterior de StorageGRID y desea coincidir con el nuevo comportamiento predeterminado, debe deshabilitar explícitamente las actualizaciones de la última hora de acceso para cada uno de esos bloques anteriores. Puede activar o desactivar las actualizaciones en la hora del último acceso mediante la solicitud de hora de último acceso de PUT Bucket o desde la página de detalles de un bucket en el gestor de inquilinos. Consulte "Activar o desactivar las actualizaciones de la hora del último acceso".

Si se desactivan las actualizaciones de la última hora de acceso para un bloque, se aplicará el siguiente comportamiento a las operaciones del bloque:

- Las solicitudes GetObject, GetObjectAcl, GetObjectTagging y HeadObject no actualizan la hora del último acceso. El objeto no se agrega a las colas para la evaluación de la gestión del ciclo de vida de la información (ILM).
- Las solicitudes CopyObject y PutObjectTagging que actualizan solo los metadatos también actualizan la hora de último acceso. El objeto se agrega a las colas para la evaluación de ILM.
- Si las actualizaciones de la hora del último acceso están deshabilitadas para el bloque de origen, las solicitudes de CopyObject no actualizan la hora del último acceso para el bloque de origen. El objeto que se copió no se agrega a colas para la evaluación de ILM para el bloque de origen. Sin embargo, para el destino, las solicitudes de CopyObject siempre actualizan la hora del último acceso. La copia del objeto se agrega a las colas para la evaluación de ILM.
- Las solicitudes de CompleteMultipartUpload actualizan la hora del último acceso. El objeto completado se agrega a las colas para la evaluación de ILM.

Solicitar ejemplos

En este ejemplo se habilita la hora de último acceso para un bloque.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

En este ejemplo se deshabilita la hora de último acceso para un bloque.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

DELETE bucket metadata notification Configuration

La solicitud de configuración DE notificación DE metadatos DELETE Bucket permite deshabilitar el servicio de integración de búsqueda para bloques individuales al eliminar el XML de configuración.

Para completar esta operación, debe tener el permiso s3:DeleteBucketMetadataNotification para un bloque o ser raíz de cuenta.

Ejemplo de solicitud

Este ejemplo muestra cómo deshabilitar el servicio de integración de búsqueda para un bloque.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

OBTENGA la configuración de notificación de metadatos del bloque de datos

La solicitud de configuración DE notificación DE metadatos GET Bucket permite recuperar el XML de configuración que se utiliza para configurar la integración de búsqueda de bloques individuales.

Para completar esta operación, debe tener el permiso s3:GetBucketMetadataNotification, o ser raíz de la cuenta.

Ejemplo de solicitud

Esta solicitud recupera la configuración de notificación de metadatos del bloque denominado `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Respuesta

El cuerpo de la respuesta incluye la configuración de notificación de metadatos para el bloque. La configuración de notificaciones de metadatos permite determinar cómo se configura el bloque para la integración de búsquedas. Es decir, permite determinar a qué objetos se indexan y a qué extremos se envían los metadatos de sus objetos.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Cada configuración de notificación de metadatos incluye una o varias reglas. Cada regla especifica los objetos a los que se aplica y el destino al que StorageGRID debe enviar metadatos de objetos. Los destinos se deben especificar con el URN de un extremo de StorageGRID.

Nombre	Descripción	Obligatorio
MetadataNotificationConfiguration	Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos Regla.	Sí

Nombre	Descripción	Obligatorio
Regla	Código de contenedor de una regla que identifica los objetos cuyos metadatos deben agregarse a un índice especificado. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
ID	Identificador único de la regla. Incluido en el elemento Regla.	No
Estado	El estado puede ser "activado" o "desactivado". No se toman medidas para las reglas que están desactivadas. Incluido en el elemento Regla.	Sí
Prefijo	Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado. Para hacer coincidir todos los objetos, especifique un prefijo vacío. Incluido en el elemento Regla.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Regla.	Sí

Nombre	Descripción	Obligatorio
No	URN del destino donde se envían los metadatos del objeto. Debe ser URN de un extremo de StorageGRID con las siguientes propiedades: • `es` debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo donde se almacenan los metadatos, en el formulario `domain-name/myindex/mytype`. Los extremos se configuran con el administrador de inquilinos o la API de gestión de inquilinos. Tienen el siguiente formato: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` El punto final debe estar configurado antes de enviar el XML de configuración o la configuración fallará con un error 404. El valor de urn se incluye en el elemento Destination.	Sí

Ejemplo de respuesta

El XML incluido entre `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags muestra cómo se configura la integración con un extremo de integración de búsqueda para el bloque. En este ejemplo, los metadatos del objeto se envían a un índice de Elasticsearch llamado `current` y escriba named `2017` Que se aloja en un dominio de AWS llamado `records`.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Información relacionada

"Usar una cuenta de inquilino"

Configuración de notificaciones de metadatos de PUT Bucket

La solicitud de configuración de notificación DE metadatos DE PUT Bucket permite habilitar el servicio de integración de búsqueda para bloques individuales. El XML de configuración de notificación de metadatos que se proporciona en el cuerpo de la solicitud especifica los objetos cuyos metadatos se envían al índice de búsqueda de destino.

Para completar esta operación, debe tener el permiso s3:PutBucketMetadataNotification para un bloque o ser raíz de la cuenta.

Solicitud

La solicitud debe incluir la configuración de notificación de metadatos en el cuerpo de la solicitud. Cada configuración de notificación de metadatos incluye una o varias reglas. Cada regla especifica los objetos a los que se aplica y el destino al que StorageGRID debe enviar metadatos de objetos.

Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, puede enviar metadatos de los objetos con el prefijo `/images` en un destino y objetos con el prefijo `/videos` a otro.

Las configuraciones que tienen prefijos superpuestos no son válidas y se rechazan cuando se envían. Por ejemplo, una configuración que incluía una regla para objetos con el prefijo `test` y una segunda regla para los objetos con el prefijo `test2` no se permitirá.

Los destinos se deben especificar con el URN de un extremo de StorageGRID. El extremo debe existir cuando

se envía la configuración de notificación de metadatos o la solicitud falla como un `400 Bad Request`. El mensaje de error indica: `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN`.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

En la tabla se describen los elementos del XML de configuración de notificaciones de metadatos.

Nombre	Descripción	Obligatorio
MetadataNotificationConfiguration	Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos Regla.	Sí
Regla	Código de contenedor de una regla que identifica los objetos cuyos metadatos deben agregarse a un índice especificado. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
ID	Identificador único de la regla. Incluido en el elemento Regla.	No

Nombre	Descripción	Obligatorio
Estado	El estado puede ser "activado" o "desactivado". No se toman medidas para las reglas que están desactivadas. Incluido en el elemento Regla.	Sí
Prefijo	Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado. Para hacer coincidir todos los objetos, especifique un prefijo vacío. Incluido en el elemento Regla.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Regla.	Sí
No	URN del destino donde se envían los metadatos del objeto. Debe ser URN de un extremo de StorageGRID con las siguientes propiedades: • `es` debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo donde se almacenan los metadatos, en el formulario `domain-name/myindex/mytype`. Los extremos se configuran con el administrador de inquilinos o la API de gestión de inquilinos. Tienen el siguiente formato: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` El punto final debe estar configurado antes de enviar el XML de configuración o la configuración fallará con un error 404. El valor de urn se incluye en el elemento Destination.	Sí

Solicitar ejemplos

Este ejemplo muestra habilitar la integración de búsqueda de un bloque. En este ejemplo, los metadatos de objeto de todos los objetos se envían al mismo destino.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

En este ejemplo, metadatos de objeto para objetos que coinciden con el prefijo `/images` se envía a un destino, mientras que los metadatos de objetos de los objetos que coinciden con el prefijo `/videos` se envía a un segundo destino.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

JSON generado por el servicio de integración de búsqueda

Al habilitar el servicio de integración de búsqueda para un bloque, se genera un documento JSON y se envía al extremo de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas del objeto.

Este ejemplo muestra un ejemplo de JSON que se podría generar cuando un objeto con la clave `SGWS/Tagging.txt` se crea en un bloque llamado `test`. La `test` el bloque no tiene versiones, por lo que el `versionId` la etiqueta está vacía.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadatos de objetos incluidos en las notificaciones de metadatos

En la tabla se enumeran todos los campos que se incluyen en el documento JSON que se envían al extremo de destino cuando la integración de búsqueda está habilitada.

El nombre del documento incluye el nombre del bloque, el nombre del objeto y el ID de versión, si existe.

Tipo	Nombre del elemento	Descripción
Información sobre bloques y objetos	cucharón	Nombre del bloque
Información sobre bloques y objetos	clave	Nombre de clave de objeto
Información sobre bloques y objetos	ID de versión	Versión de objeto, para objetos en bloques con versiones
Información sobre bloques y objetos	región	Región de bloque, por ejemplo `us-east-1`
Metadatos del sistema	tamaño	Tamaño del objeto (en bytes) visible para un cliente HTTP
Metadatos del sistema	md5	Hash de objeto
Metadatos del usuario	metadatos *`key:value`*	Todos los metadatos de usuario del objeto, como pares clave-valor

Tipo	Nombre del elemento	Descripción
Etiquetas	etiquetas *key:value*	Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor

> Para las etiquetas y los metadatos de usuario, StorageGRID pasa las fechas y los números a Elasticsearch como cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para interpretar estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para la asignación dinámica de campos y para asignar formatos de fecha. Debe habilitar las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Después de indexar un documento, no puede editar los tipos de campo del documento en el índice.

Información relacionada

"Usar una cuenta de inquilino"

OBTENGA la solicitud de uso del almacenamiento

La solicitud GET Storage Usage le indica la cantidad total de almacenamiento que está usando una cuenta y por cada bloque asociado con la cuenta.

La cantidad de almacenamiento utilizada por una cuenta y sus depósitos se puede obtener mediante una solicitud ListBuckets modificada con el `x-ntap-sg-usage` parámetro de consulta. Se realiza un seguimiento del uso del almacenamiento en bloques de forma independiente de las solicitudes DE PUT y DELETE procesadas por el sistema. Es posible que haya algún retraso antes de que los valores de uso coincidan con los valores esperados en función del procesamiento de las solicitudes, especialmente si el sistema está sometido a cargas pesadas.

De forma predeterminada, StorageGRID intenta recuperar la información de uso con una coherencia global fuerte. Si no se puede lograr una coherencia global fuerte, StorageGRID intenta recuperar la información de uso en una coherencia de sitio fuerte.

Debe tener el permiso s3:ListAllMyBuckets o ser la raíz de la cuenta para completar esta operación.

Ejemplo de solicitud

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ejemplo de respuesta

Este ejemplo muestra una cuenta que tiene cuatro objetos y 12 bytes de datos en dos bloques. Cada bloque contiene dos objetos y seis bytes de datos.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Creación de versiones

Cada versión de objeto almacenada contribuirá a la `ObjectCount` y.. `DataBytes` valores en la respuesta. Los marcadores de eliminación no se agregan a la `ObjectCount` total.

Información relacionada

"Valores de coherencia"

Solicitudes de bloque obsoletas para cumplimiento de normativas heredadas

Solicitudes de bloque obsoletas para cumplimiento de normativas heredadas

Es posible que deba utilizar la API DE REST de StorageGRID S3 para gestionar los bloques creados con la función de cumplimiento heredada.

Función de cumplimiento de normativas obsoleta

La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID quedó obsoleta y se reemplazó por el bloqueo de objetos de S3.

Si anteriormente habilitó la configuración de cumplimiento global, la opción de bloqueo de objetos S3 global se habilita en StorageGRID 11.6. Ya no se pueden crear nuevos bloques con la función de cumplimiento habilitada; sin embargo, según sea necesario, se puede utilizar la API DE REST de StorageGRID S3 para gestionar bloques existentes que cumplen las normativas.

- "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
- "Gestión de objetos con ILM"
- "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"

Solicitudes de cumplimiento de normativas obsoletas:

- "Obsoleto: PONGA modificaciones de solicitud de cucharón para el cumplimiento"

  El elemento XML de SGCompliance está obsoleto. Anteriormente, podría incluir este elemento personalizado de StorageGRID en el cuerpo de solicitud XML opcional de SOLICITUDES PUT Bucket para crear un bloque compatible.

- "Obsoleto: OBTENER cumplimiento de bloques"

  La solicitud de cumplimiento de normativas GET Bucket quedó obsoleta. Sin embargo, puede seguir utilizando esta solicitud para determinar la configuración de cumplimiento actual para un bloque compatible heredado existente.

- "Obsoleto: Cumplimiento de PUT Bucket"

  La solicitud DE cumplimiento PUT Bucket queda obsoleta. Sin embargo, puede seguir utilizando esta solicitud para modificar la configuración de cumplimiento de un bloque compatible heredado existente. Por ejemplo, puede colocar un bloque existente en la retención legal o aumentar su período de retención.

Obsoleto: Modificaciones de la solicitud de CreateBucket para el cumplimiento

El elemento XML de SGCompliance está obsoleto. Anteriormente, podía incluir este elemento personalizado de StorageGRID en el cuerpo de solicitud XML opcional de las solicitudes de CreateBucket para crear un depósito compatible.

> La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID quedó obsoleta y se reemplazó por el bloqueo de objetos de S3. En la siguiente sección, se ofrecen más detalles:
>
> - "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
> - "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"

Ya no se pueden crear bloques nuevos con el cumplimiento de normativas habilitado. Se devuelve el siguiente mensaje de error si intenta utilizar las modificaciones de solicitud de CreateBucket para la conformidad con el fin de crear un nuevo depósito compatible:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Obsoleto: OBTENER solicitud de cumplimiento de bloques

La solicitud de cumplimiento de normativas GET Bucket quedó obsoleta. Sin embargo, puede seguir utilizando esta solicitud para determinar la configuración de cumplimiento actual para un bloque compatible heredado existente.

> ⓘ La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID quedó obsoleta y se reemplazó por el bloqueo de objetos de S3. En la siguiente sección, se ofrecen más detalles:
>
> - "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
> - "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"

Para completar esta operación, debe tener el permiso s3:GetBucketCompliance o ser la raíz de la cuenta.

Ejemplo de solicitud

Esta solicitud de ejemplo le permite determinar la configuración de cumplimiento para el bloque denominado `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ejemplo de respuesta

En la respuesta XML, `<SGCompliance>` enumera la configuración de cumplimiento vigente para el bloque. Esta respuesta de ejemplo muestra la configuración de cumplimiento de un bloque en el que se conservará cada objeto durante un año (525,600 minutos), a partir del momento en que el objeto se ingiere en la cuadrícula. Actualmente, no existe ningún derecho legal en este segmento. Cada objeto se eliminará automáticamente después de un año.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nombre	Descripción
RetentionPeriodonMinutes	La duración del período de retención para los objetos que se añadió a este bloque, en minutos. El período de retención se inicia cuando el objeto se ingiere en la cuadrícula.
LegalHold	• Cierto: Este segmento está actualmente bajo un control legal. Los objetos de este depósito no se pueden eliminar hasta que se levante la conservación legal, incluso si ha caducado su período de retención. • Falso: Este segmento no está actualmente bajo un derecho. Los objetos de este bloque se pueden eliminar cuando expire su período de retención.
Eliminación automática	• True: Los objetos de este bloque se eliminarán automáticamente cuando expire su período de retención, a menos que el bloque se encuentre bajo una retención legal. • False: Los objetos de este bloque no se eliminarán automáticamente cuando finalice el período de retención. Debe eliminar estos objetos manualmente si necesita eliminarlos.

Respuestas de error

Si el bloque no se creó para ser compatible, el código de estado HTTP para la respuesta es `404 Not Found`, Con un código de error S3 de `XNoSuchBucketCompliance`.

Obsoleto: PUT Bucket Compliance Request

La solicitud DE cumplimiento PUT Bucket queda obsoleta. Sin embargo, puede seguir utilizando esta solicitud para modificar la configuración de cumplimiento de un bloque compatible heredado existente. Por ejemplo, puede colocar un bloque existente en la retención legal o aumentar su período de retención.

La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID quedó obsoleta y se reemplazó por el bloqueo de objetos de S3. En la siguiente sección, se ofrecen más detalles:

- "Use la API REST DE S3 para configurar el bloqueo de objetos de S3"
- "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"

Debe tener el permiso s3:PutBucketCompliance o ser la raíz de la cuenta para completar esta operación.

Debe especificar un valor para cada campo de la configuración de cumplimiento al emitir una solicitud DE cumplimiento PUT Bucket.

Ejemplo de solicitud

Esta solicitud de ejemplo modifica la configuración de cumplimiento del bloque denominado `mybucket`. En este ejemplo, los objetos de `mybucket` ahora se conservará durante dos años (1,051,200 minutos) en lugar de un año, a partir del momento en que el objeto se ingiere en la cuadrícula. No existe ningún derecho legal en este segmento. Cada objeto se eliminará automáticamente después de dos años.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nombre	Descripción
RetentionPeriodonMinutes	La duración del período de retención para los objetos que se añadió a este bloque, en minutos. El período de retención se inicia cuando el objeto se ingiere en la cuadrícula. **Importante** Al especificar un nuevo valor para RetentionPeriodMinutes, debe especificar un valor que sea igual o mayor que el período de retención actual del bucket. Después de definir el período de retención del depósito, no puede disminuir ese valor; solo puede aumentarlo.

Nombre	Descripción
LegalHold	• Cierto: Este segmento está actualmente bajo un control legal. Los objetos de este depósito no se pueden eliminar hasta que se levante la conservación legal, incluso si ha caducado su período de retención. • Falso: Este segmento no está actualmente bajo un derecho. Los objetos de este bloque se pueden eliminar cuando expire su período de retención.
Eliminación automática	• True: Los objetos de este bloque se eliminarán automáticamente cuando expire su período de retención, a menos que el bloque se encuentre bajo una retención legal. • False: Los objetos de este bloque no se eliminarán automáticamente cuando finalice el período de retención. Debe eliminar estos objetos manualmente si necesita eliminarlos.

Consistencia para la configuración de cumplimiento

Cuando se actualiza la configuración de cumplimiento de normativas para un bloque de S3 con una solicitud DE cumplimiento PUT Bucket, StorageGRID intenta actualizar los metadatos del bloque en el grid. De forma predeterminada, StorageGRID utiliza la consistencia **strong-global** para garantizar que todos los sitios del centro de datos y todos los nodos de almacenamiento que contienen metadatos del depósito tengan consistencia de lectura tras escritura para los ajustes de cumplimiento modificados.

Si StorageGRID no puede lograr la consistencia **fuerte-global** porque un sitio de centro de datos o varios nodos de almacenamiento en un sitio no están disponibles, el código de estado HTTP para la respuesta es `503 Service Unavailable.`

Si recibe esta respuesta, debe ponerse en contacto con el administrador de grid para garantizar que los servicios de almacenamiento requeridos estén disponibles en Lo antes posible.. Si el administrador de grid no puede poner a disposición suficientes nodos de almacenamiento en cada sitio, el soporte técnico puede indicarle que vuelva a intentar la solicitud fallida forzando la consistencia del **sitio fuerte**.

> Nunca fuerce la consistencia de **strong-site** para el cumplimiento de PUT bucket a menos que se le haya indicado hacerlo por el soporte técnico y a menos que comprenda las posibles consecuencias de usar este nivel.

Cuando la consistencia se reduce a **strong-site**, StorageGRID garantiza que la configuración de cumplimiento actualizada tendrá consistencia de lectura tras escritura solo para las solicitudes de los clientes dentro de un sitio. Esto significa que el sistema StorageGRID podría tener temporalmente varias configuraciones incoherentes para este bloque hasta que todos los sitios y nodos de almacenamiento estén disponibles. La configuración incoherente puede dar como resultado un comportamiento inesperado y no deseado. Por ejemplo, si va a colocar un bloque bajo una conservación legal y fuerza una menor coherencia, la configuración de cumplimiento anterior del bloque (es decir, la retención legal) puede seguir vigente en algunos sitios del centro de datos. Como resultado, los objetos que cree que están en retención legal se pueden eliminar cuando caduque su período de retención, ya sea por el usuario o por AutoDelete, si está activado.

Para forzar el uso de la consistencia **strong-site**, vuelva a emitir la solicitud de cumplimiento de PUT Bucket e incluya el `Consistency-Control` Encabezado de solicitud HTTP, de la siguiente manera:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Respuestas de error

- Si el bloque no se creó para ser compatible, el código de estado HTTP para la respuesta es `404 Not Found`.
- Si `RetentionPeriodMinutes` En la solicitud es inferior al período de retención actual del bloque, el código de estado HTTP es `400 Bad Request`.

Información relacionada

"Obsoleto: PONGA modificaciones de solicitud de cucharón para el cumplimiento"

Políticas de acceso a bloques y grupos

Utilice las políticas de acceso de bloques y grupos

StorageGRID utiliza el lenguaje de políticas de Amazon Web Services (AWS) para permitir que los inquilinos S3 controlen el acceso a bloques y objetos dentro de esos bloques. El sistema StorageGRID implementa un subconjunto del lenguaje de políticas de la API DE REST de S3. Las políticas de acceso para la API de S3 se escriben en JSON.

Información general sobre las políticas de acceso

Existen dos tipos de políticas de acceso compatibles con StorageGRID.

- **Políticas de cubo**, que se gestionan mediante las operaciones de la API GetBucketPolicy, PutBucketPolicy y DeleteBucketPolicy S3. Las políticas de bloque se asocian a bloques, por lo que se configuran para controlar el acceso de los usuarios de la cuenta de propietario del bloque u otras cuentas al bloque y a los objetos en él. La política de bloques se aplica únicamente a un bloque y, posiblemente, a varios grupos.
- **Políticas de grupo**, que se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Las directivas de grupo se asocian a un grupo de la cuenta, por lo que se configuran para permitir que dicho grupo tenga acceso a recursos específicos propiedad de dicha cuenta. La política de grupo se aplica únicamente a un grupo y, posiblemente, a varios bloques.

> ⓘ No hay ninguna diferencia de prioridad entre las políticas de grupo y de bloque.

Las políticas de bloque y grupo de StorageGRID siguen una gramática específica definida por Amazon. Dentro de cada política hay una serie de declaraciones de política y cada sentencia contiene los siguientes elementos:

- ID de sentencia (Sid) (opcional)
- Efecto
- Principal/NotPrincipal
- Recurso/NotResource

- Acción/NotAction
- Condición (opcional)

Las sentencias de directiva se crean utilizando esta estructura para especificar permisos: Conceda <Effect> para permitir/denegar que <Principal> ejecute <Action> en <Resource> cuando se aplique <Condition>.

Cada elemento de directiva se utiliza para una función específica:

Elemento	Descripción
SID	El elemento Sid es opcional. El Sid sólo se ha diseñado como una descripción para el usuario. El sistema StorageGRID lo almacena pero no lo interpreta.
Efecto	Utilice el elemento Effect para establecer si se permiten o deniegan las operaciones especificadas. Debe identificar las operaciones que permite (o deniega) en cubos u objetos utilizando las palabras clave del elemento Acción admitido.
Principal/NotPrincipal	Puede permitir a los usuarios, grupos y cuentas acceder a recursos específicos y realizar acciones específicas. Si no se incluye ninguna firma S3 en la solicitud, se permite el acceso anónimo especificando el carácter comodín (*) como principal. De forma predeterminada, sólo la raíz de la cuenta tiene acceso a los recursos que pertenecen a la cuenta. Sólo es necesario especificar el elemento Principal en una política de bloque. Para las directivas de grupo, el grupo al que se asocia la directiva es el elemento Principal implícito.
Recurso/NotResource	El elemento Resource identifica los bloques y los objetos. Puede permitir o denegar permisos para cubos y objetos utilizando el nombre de recurso de Amazon (ARN) para identificar el recurso.
Acción/NotAction	Los elementos Acción y efecto son los dos componentes de los permisos. Cuando un grupo solicita un recurso, se le concede o se le deniega el acceso al recurso. Se deniega el acceso a menos que asigne permisos de forma específica, pero puede utilizar Denegar explícito para anular un permiso otorgado por otra directiva.
Condición	El elemento Condition es opcional. Las condiciones permiten crear expresiones para determinar cuándo se debe aplicar una directiva.

En el elemento Action , puede utilizar el carácter comodín (*) para especificar todas las operaciones o un subconjunto de operaciones. Por ejemplo, esta acción coincide con permisos como s3:GetObject, s3:PutObject y s3:DeleteObject.

```
s3:*Object
```

En el elemento Resource , puede utilizar los caracteres comodín (*) y (?). Aunque el asterisco (*) coincide con

0 o más caracteres, el signo de interrogación (?) coincide con cualquier carácter.

En el elemento Principal, no se admiten caracteres comodín excepto para establecer el acceso anónimo, que otorga permiso a todos. Por ejemplo, el comodín (*) se establece como el valor Principal.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

En el ejemplo siguiente, la instrucción utiliza los elementos Effect, Principal, Acción y recurso. En este ejemplo se muestra una sentencia de directiva de bloque completa que utiliza el efecto "permitir" para dar a los principales, el grupo admin `federated-group/admin` y el grupo financiero `federated-group/finance`, Permisos para realizar la acción `s3:ListBucket` en el bloque llamado `mybucket` Y la Acción `s3:GetObject` en todos los objetos dentro de ese cucharón.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

La política de bloque tiene un límite de tamaño de 20,480 bytes y la política de grupo tiene un límite de tamaño de 5,120 bytes.

Coherencia de las políticas

De forma predeterminada, cualquier actualización que realice a las directivas de grupo será consistente. Cuando una normativa de grupo es coherente, los cambios pueden tardar 15 minutos adicionales en aplicarse debido al almacenamiento en caché de la política. Por defecto, cualquier actualización que realice en las políticas de depósito es fuertemente coherente.

Según sea necesario, puede cambiar las garantías de coherencia para las actualizaciones de la política de bloques. Por ejemplo, es posible que desee que un cambio en una política de bloque esté disponible durante una interrupción del servicio del sitio.

En este caso, puede ajustar la `Consistency-Control` Cabecera en la solicitud PutBucketPolicy, o puede utilizar la solicitud de coherencia PUT Bucket. Cuando una política de depósito es coherente, los cambios pueden tardar 8 segundos adicionales en aplicarse debido al almacenamiento en caché de la política.

> Si establece la consistencia en un valor diferente para resolver una situación temporal, asegúrese de volver a establecer el valor de nivel de cubo en su valor original cuando haya terminado. De lo contrario, todas las solicitudes de bloque futuras utilizarán la configuración modificada.

Utilice ARN en las declaraciones de política

En las declaraciones de política, el ARN se utiliza en los elementos Principal y Recursos.

- Utilice esta sintaxis para especificar el recurso ARN de S3:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilice esta sintaxis para especificar el recurso de identidad ARN (usuarios y grupos):

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Otras consideraciones:

- Puede utilizar el asterisco (*) como comodín para que coincida con cero o más caracteres dentro de la clave de objeto.
- Los caracteres internacionales, que se pueden especificar en la clave de objeto, deben codificarse mediante JSON UTF-8 o mediante secuencias de escape JSON \u. No se admite el porcentaje de codificación.

  "Sintaxis de URN RFC 2141"

  El cuerpo de la solicitud HTTP para la operación PutBucketPolicy debe estar codificado con charset=UTF-8.

Especifique recursos en una política

En las sentencias de directiva, puede utilizar el elemento Resource para especificar el bloque o el objeto para el que se permiten o deniegan los permisos.

- Cada instrucción de directiva requiere un elemento Resource. En una política, el elemento denota los recursos `Resource`o bien, `NotResource` para la exclusión.
- Se especifican recursos con un ARN de recurso S3. Por ejemplo:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- También puede usar variables de política dentro de la clave de objeto. Por ejemplo:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- El valor del recurso puede especificar un bucket que todavía no existe cuando se crea una política de grupo.

Especifique los principales en una directiva

Utilice el elemento Principal para identificar al usuario, grupo o cuenta de arrendatario que la sentencia de directiva permite o deniega el acceso al recurso.

- Cada sentencia de política de una política de bloque debe incluir un elemento Principal. Las sentencias de política de una política de grupo no necesitan el elemento Principal porque se entiende que el grupo es el principal.
- En una política, los principales se denotan por el elemento Principal o, alternativamente, NotPrincipal para la exclusión.
- Las identidades basadas en cuentas se deben especificar mediante un ID o un ARN:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- En este ejemplo se utiliza el ID de cuenta de inquilino 27233906934684427525, que incluye la raíz de la cuenta y todos los usuarios de la cuenta:

```
 "Principal": { "AWS": "27233906934684427525" }
```

- Puede especificar sólo la raíz de la cuenta:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Puede especificar un usuario federado específico ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- Puede especificar un grupo federado específico ("managers"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-group/Managers"  }
```

- Puede especificar un principal anónimo:

```
"Principal": "*"
```

- Para evitar ambigüedades, puede utilizar el UUID de usuario en lugar del nombre de usuario:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

  Por ejemplo, supongamos que Alex abandona la organización y el nombre de usuario `Alex` se ha eliminado. Si un nuevo Alex se une a la organización y se le asigna la misma `Alex` nombre de usuario, es posible que el nuevo usuario herede sin querer los permisos concedidos al usuario original.

- El valor principal puede especificar un nombre de grupo/usuario que aún no existe cuando se crea una directiva de bloque.

Especificar permisos en una directiva

En una directiva, el elemento Acción se utiliza para permitir/denegar permisos a un recurso. Hay un conjunto de permisos que puede especificar en una directiva, que se indican mediante el elemento "Acción" o, alternativamente, "NotAction" para la exclusión. Cada uno de estos elementos se asigna a operaciones de API de REST de S3 específicas.

En las tablas se enumeran los permisos que se aplican a los bloques y los permisos que se aplican a los objetos.

> Amazon S3 ahora usa el permiso S3:PutReplicationConfiguration para las acciones PutBucketReplication y DeleteBucketReplication. StorageGRID utiliza permisos independientes para cada acción, que coinciden con la especificación original de Amazon S3.

> Se realiza una supresión cuando se utiliza una PUT para sobrescribir un valor existente.

Permisos que se aplican a los bloques

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:CreateBucket	CreateBucket	Sí. **Nota**: Usar solo en la política de grupo.

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:DeleteBucket	DeleteBucket	
s3:DeleteBucketMetadataNotification	DELETE bucket metadata notification Configuration	Sí
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:DeleteReplicationConfiguration	DeleteBucketReplication	Sí, separe los permisos para PUT y DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	CUMPLIMIENTO de LA normativa GET Bucket (obsoleto)	Sí
s3:GetBucketConsistency	OBTENGA coherencia de bloques	Sí
s3: GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	HORA de último acceso al bloque DE GET	Sí
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataNotification	OBTENGA la configuración de notificación de metadatos del bloque de datos	Sí
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	Etiquetado de GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:ListAllMyBuckets	• ListCuchers • Obtenga el uso del almacenamiento	Sí, para OBTENER uso de almacenamiento. **Nota**: Usar solo en la política de grupo.
s3:ListBucket	• ListObjects • Segmento de cabeza • RestoreObject	
s3:ListBucketMultipartUploads	• ListCargas multipartitas • RestoreObject	
s3:ListBucketVersions	OBTENGA las versiones DE Bucket	
s3:PutBucketCompliance	CUMPLIMIENTO de PUT Bucket (obsoleto)	Sí
s3:PutBucketConsistency	PONGA la consistencia del cucharón	Sí
s3: PutBucketCORS	• DeleteBucketCors† • A cargo de PutBucketCors	
s3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
s3:PutBucketLastAccessTime	PUT Bucket última hora de acceso	Sí
s3:PutBucketMetadataNotification	Configuración de notificaciones de metadatos de PUT Bucket	Sí
s3:PutBucketNotification	PutBucketNotificationConfiguration	
s3:PutBucketObjectLockConfiguration	• CreateBucket con el `x-amz-bucket-object-lock-enabled: true` Encabezado de solicitud (también requiere el permiso s3:CreateBucket) • PutObjectLockConfiguration	
s3:PutBucketPolicy	Política de PutBucketPolicy	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:PutBucketEtiquetado	• DeleteBucketTagging† • PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLipeycleConfiguration	• DeleteBucketLifecycle† • PutBucketLifecycleConfiguration	
s3:PutReplicationConfiguration	PutBucketReplication	Sí, separe los permisos para PUT y DELETE

Permisos que se aplican a objetos

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:AbortMultipartUpload	• AbortMultipartUpload • RestoreObject	
s3:BypassGovernanceRetention	• DeleteObject • DeleteObjects • PutObjectRetention	
s3:DeleteObject	• DeleteObject • DeleteObjects • RestoreObject	
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging (una versión específica del objeto)	
s3:DeleteObjectVersion	DeleteObject (una versión específica del objeto)	
s3:GetObject	• GetObject • Objeto principal • RestoreObject • SelectObjectContent	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectEtiquetado	
s3:GetObjectVersionTagging	GetObjectTagging (una versión específica del objeto)	
s3:GetObjectVersion	GetObject (una versión específica del objeto)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• Objeto de puta • CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectEtiquetado	PutObjectEtiquetado	
s3:PutObjectVersionEtiquetado	PutObjectTagging (una versión específica del objeto)	
s3:PutOverwriteObject	• Objeto de puta • CopyObject • PutObjectEtiquetado • DeleteObjectTagging • CompleteMultipartUpload	Sí
s3:RestoreObject	RestoreObject	

Utilice el permiso PutOverwriteObject

el permiso s3:PutOverwriteObject es un permiso StorageGRID personalizado que se aplica a operaciones que crean o actualizan objetos. La configuración de este permiso determina si el cliente puede sobrescribir los datos de un objeto, metadatos definidos por el usuario o el etiquetado de objetos S3.

Entre los posibles ajustes para este permiso se incluyen:

- **Permitir**: El cliente puede sobrescribir un objeto. Esta es la configuración predeterminada.
- **Denegar**: El cliente no puede sobrescribir un objeto. Cuando se establece en Denegar, el permiso PutOverwriteObject funciona de la siguiente manera:
  - Si se encuentra un objeto existente en la misma ruta:
    - Los datos del objeto, los metadatos definidos por el usuario o el etiquetado de objetos S3 no se pueden sobrescribir.
    - Se cancela cualquier operación de ingesta en curso y se devuelve un error.
    - Si el control de versiones S3 está activado, la configuración Denegar impide que las operaciones PutObjectTagging o DeleteObjectTagging modifiquen el TagSet para un objeto y sus versiones no actuales.
  - Si no se encuentra un objeto existente, este permiso no tiene efecto.
- Cuando este permiso no está presente, el efecto es el mismo que si se estableció permitir.

> Si la directiva S3 actual permite la sobrescritura y el permiso PutOverwriteObject se establece en Deny, el cliente no puede sobrescribir los datos de un objeto, los metadatos definidos por el usuario ni el etiquetado de objetos. Además, si la casilla de verificación **Evitar modificación de cliente** está seleccionada (**CONFIGURACIÓN** > **Ajustes de seguridad** > **Red y objetos**), esa configuración anula la configuración del permiso PutOverwriteObject.

Especificar condiciones en una política

Las condiciones definen cuándo estará en vigor una política. Las condiciones consisten en operadores y pares clave-valor.

Condiciones Utilice pares clave-valor para la evaluación. Un elemento Condition puede contener varias condiciones y cada condición puede contener varios pares clave-valor. El bloque Condition utiliza el siguiente formato:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

En el ejemplo siguiente, la condición ipaddress utiliza la clave de condición SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Operadores de condición admitidos

Los operadores de condición se categorizan de la siguiente manera:

- Cadena
- Numérico
- Booleano
- Dirección IP
- Comprobación nula

Operadores de condición	Descripción
StringEquals	Compara una clave con un valor de cadena basado en la coincidencia exacta (distingue entre mayúsculas y minúsculas).
StringNotEquals	Compara una clave con un valor de cadena basado en la coincidencia negada (distingue entre mayúsculas y minúsculas).
StringEqualizsIgnoreCase	Compara una clave con un valor de cadena basado en la coincidencia exacta (omite Case).
StringNotEqualizsIgnoreCase	Compara una clave con un valor de cadena basado en la coincidencia negada (omite Case).
StringLike	Compara una clave con un valor de cadena basado en la coincidencia exacta (distingue entre mayúsculas y minúsculas). Puede incluir * y ? caracteres comodín.
StringNotLike	Compara una clave con un valor de cadena basado en la coincidencia negada (distingue entre mayúsculas y minúsculas). Puede incluir * y ? caracteres comodín.
Valores numéricos	Compara una clave con un valor numérico basado en la coincidencia exacta.
NumericNotEquals	Compara una clave con un valor numérico basado en la coincidencia negada.

Operadores de condición	Descripción
NumericGreatertan	Compara una clave con un valor numérico basado en la coincidencia mayor que.
NumericGreaterThanEquals	Compara una clave con un valor numérico en función de la coincidencia mayor o igual que.
NumericLessThan	Compara una clave con un valor numérico basado en la coincidencia menor que.
NumericLesThanEquals	Compara una clave con un valor numérico en función de la coincidencia menor o igual que.
Bool	Compara una clave con un valor booleano basado en la coincidencia “true o false”.
IPAddress	Compara una clave con una dirección IP o un rango de direcciones IP.
NotIpAddress	Compara una clave con una dirección IP o un intervalo de direcciones IP basándose en la coincidencia negada.
Nulo	Comprueba si hay una clave de condición en el contexto actual de la solicitud.

Teclas de condición compatibles

Teclas de condición	Acciones	Descripción
aws:SourceIp	Operadores IP	Comparará con la dirección IP desde la que se envió la solicitud. Se puede utilizar para operaciones de bloques u objetos. **Nota:** Si la solicitud S3 se envió a través del servicio Load Balancer en nodos Admin y nodos de Gpuertas de enlace, se comparará con la dirección IP anterior al servicio Load Balancer. **Nota**: Si se utiliza un equilibrador de carga no transparente de terceros, se comparará con la dirección IP de ese equilibrador de carga. Cualquiera `X-Forwarded-For` el encabezado se ignorará porque no se puede determinar su validez.
aws:nombre de usuario	Recurso/identidad	Comparará con el nombre de usuario del remitente desde el que se envió la solicitud. Se puede utilizar para operaciones de bloques u objetos.

Teclas de condición	Acciones	Descripción
s3:delimitador	s3:ListBucket y. s3:ListBucketVersions permisos	Se comparará con el parámetro delimitador especificado en una solicitud ListObjects o ListObjectVersions.
S3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl 3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging S3:PutObjectAcl s3:PutObjectEtiquetado S3:PutObjectVersionAcl s3:PutObjectVersionEtiquetado	Requerirá que el objeto existente tenga la clave de etiqueta y el valor específicos.
s3:max-keys	s3:ListBucket y. s3:ListBucketVersions permisos	Se compara con el parámetro max-keys especificado en una solicitud ListObjects o ListObjectVersions.
s3:retención-días restante del bloqueo de objetos	s3:PutObject	Compara con la fecha de retención hasta especificada en `x-amz-object-lock-retain-until-date` cabecera de solicitud o calculada desde el período de retención predeterminado de bloque para asegurarse de que estos valores están dentro del intervalo permitido para las siguientes solicitudes: • Objeto de puta • CopyObject • CreateMultipartUpload

Teclas de condición	Acciones	Descripción
s3:retención-días restante del bloqueo de objetos	s3:PutObjectRetention	Se compara con la fecha de retención especificada en la solicitud PutObjectRetention para asegurarse de que se encuentra dentro del rango permitido.
s3:prefijo	s3:ListBucket y. s3:ListBucketVersions permisos	Se comparará con el parámetro PreFIX especificado en una solicitud ListObjects o ListObjectVersions.
S3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectEtiquetado s3:PutObjectVersionEtiquetado	Requerirá una clave y un valor de etiqueta específicos cuando la solicitud del objeto incluya el etiquetado.

Especifique las variables en una política

Las variables de las directivas se pueden utilizar para rellenar la información de directivas cuando esté disponible. Se pueden usar variables de política en la `Resource` comparaciones entre elementos y cadenas en la `Condition` elemento.

En este ejemplo, la variable `${aws:username}` Forma parte del elemento Resource:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

En este ejemplo, la variable `${aws:username}` forma parte del valor de condición en el bloque de condición:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variable	Descripción
`${aws:SourceIp}`	Utiliza la clave SourceIp como la variable proporcionada.
`${aws:username}`	Utiliza la clave de nombre de usuario como la variable proporcionada.
`${s3:prefix}`	Utiliza la clave de prefijo específica del servicio como variable proporcionada.

Variable	Descripción
`${s3:max-keys}`	Utiliza la clave de max-keys específica del servicio como la variable proporcionada.
`${*}`	Carácter especial. Utiliza el carácter como carácter literal *.
`${?}`	Carácter especial. Utiliza el carácter como literal ? carácter.
`${$}`	Carácter especial. Utiliza el carácter como carácter literal $.

Crear directivas que requieran un manejo especial

A veces, una directiva puede otorgar permisos peligrosos para la seguridad o para operaciones continuas, como bloquear al usuario raíz de la cuenta. La implementación de la API REST de StorageGRID S3 es menos restrictiva durante la validación de políticas que Amazon, pero igual de estricta durante la evaluación de la política.

Descripción de la política	Tipo de política	Comportamiento de Amazon	Comportamiento de StorageGRID
Denegar a sí mismo cualquier permiso a la cuenta raíz	Cucharón	Válido y reforzado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bloques de S3	Igual
Denegar a sí mismo cualquier permiso al usuario o grupo	Grupo	Válido y reforzado	Igual
Permitir cualquier permiso para un grupo de cuentas externo	Cucharón	Principal no válido	Válidos, pero los permisos para todas las operaciones de política de bloques de S3 devuelven un método 405 no permitido cuando lo permite una política
Permitir cualquier permiso para una raíz de cuenta externa o para un usuario	Cucharón	Válidos, pero los permisos para todas las operaciones de política de bloques de S3 devuelven un método 405 no permitido cuando lo permite una política	Igual

Descripción de la política	Tipo de política	Comportamiento de Amazon	Comportamiento de StorageGRID
Permitir que todos tengan permisos para todas las acciones	Cucharón	Válido, pero los permisos para todas las operaciones de política de bloques de S3 devuelven un error de método 405 no permitido para la raíz de cuenta externa y los usuarios	Igual
Denegar a todos los permisos a todas las acciones	Cucharón	Válido y reforzado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bloques de S3	Igual
Principal es un usuario o grupo inexistente	Cucharón	Principal no válido	Válido
El recurso es un bloque de S3 que no existe	Grupo	Válido	Igual
El director es un grupo local	Cucharón	Principal no válido	Válido
Policy otorga a una cuenta no propietaria (incluidas las cuentas anónimas) permisos para colocar objetos.	Cucharón	Válido. Los objetos son propiedad de la cuenta creadora y la política de bucket no se aplica. La cuenta de creador debe otorgar permisos de acceso al objeto mediante ACL de objeto.	Válido. Los objetos son propiedad de la cuenta de propietario del bloque. Se aplica la política de bloques.

Protección WORM (escritura única lectura múltiple)

Se pueden crear bloques DE escritura única y lectura múltiple (WORM) para proteger los datos, los metadatos de objetos definidos por el usuario y el etiquetado de objetos de S3. Puede configurar los bloques WORM para permitir la creación de objetos nuevos y evitar sobrescrituras o eliminaciones del contenido existente. Utilice uno de los enfoques aquí descritos.

Para asegurarse de que las sobrescrituras se deniegan siempre, puede:

- En Grid Manager, vaya a **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD** > **RED AND OBJECTS** y seleccione la casilla de verificación **Evitar modificación del cliente**.
- Aplique las siguientes reglas y políticas de S3:
  - Agregue una operación PUTOVERWRITEOBJECT DENY a la directiva S3.
  - Agregue una operación DeleteObject DENY a la directiva S3.
  - Agregue una operación PutObject ALLOW a la política S3.

Si se configura DeleteObject como DENEGADO en una política de S3, ILM no impide que elimine objetos cuando existe una regla como «copias cero tras 30 días».

Incluso cuando se aplican todas estas reglas y políticas, no protegen frente a escrituras simultáneas (consulte la situación A). Protegen contra sobrescrituras completadas secuenciales (consulte la situación B).

Situación A: Escrituras simultáneas (no protegidas contra)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situación B: Sobrescrituras completadas secuenciales (protegidas contra)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Información relacionada

- "Cómo gestionan las reglas de ILM de StorageGRID los objetos"
- "Ejemplo de políticas de bloque"
- "Ejemplo de políticas de grupo"
- "Gestión de objetos con ILM"
- "Usar una cuenta de inquilino"

Ejemplo de políticas de bloque

Utilice los ejemplos de esta sección para crear políticas de acceso StorageGRID para buckets.

Las políticas de bloque especifican los permisos de acceso para el bloque al que está asociada la directiva. Las políticas de bloque se configuran mediante la API de S3 PutBucketPolicy. Consulte "Operaciones en bloques".

Se puede configurar una política de bloques mediante la CLI de AWS según el siguiente comando:

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Ejemplo: Permitir que todos tengan acceso de solo lectura a un bloque

En este ejemplo, a todos, incluido el anónimo, se les permite enumerar objetos en el depósito y realizar operaciones GetObject en todos los objetos del depósito. Se denegarán todas las demás operaciones. Tenga en cuenta que esta política puede no ser particularmente útil porque nadie, excepto la raíz de la cuenta, tiene permisos para escribir en el depósito.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Ejemplo: Permitir que todos en una cuenta tengan acceso total y que todas las personas de otra cuenta tengan acceso de solo lectura a un bloque

En este ejemplo, se permite a todos los integrantes de una cuenta especificada el acceso completo a un bloque, mientras que a todos los miembros de otra cuenta especificada sólo se les permite enumerar el bloque y realizar operaciones GetObject en los objetos del bloque empezando por el `shared/` prefijo de clave de objeto.

> En StorageGRID, los objetos creados por una cuenta que no es propietaria (incluidas las cuentas anónimas) son propiedad de la cuenta de propietario del bloque. La política de bloque se aplica a estos objetos.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Ejemplo: Permitir que todo el mundo tenga acceso de solo lectura a un bloque y acceso completo por un grupo especificado

En este ejemplo, todos, incluidos los anónimos, pueden enumerar el depósito y realizar operaciones GetObject en todos los objetos del depósito, mientras que solo los usuarios que pertenecen al grupo `Marketing` en la cuenta especificada se permite el acceso completo.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Ejemplo: Permitir que todo el mundo tenga acceso de lectura y escritura a un bloque si un cliente se encuentra en el rango de IP

En este ejemplo, todos, incluido el anónimo, pueden enumerar el bloque y realizar cualquier operación Object en todos los objetos del bloque, siempre que las solicitudes provengan de un intervalo IP especificado (54.240.143.0 a 54.240.143.255, excepto 54.240.143.188). Se denegarán todas las demás operaciones y se denegarán todas las solicitudes que estén fuera del rango de IP.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Ejemplo: Permitir el acceso completo a un bloque exclusivamente por un usuario federado especificado

En este ejemplo, el usuario federado Alex tiene permiso de acceso completo al `examplebucket` cucharón y sus objetos. A todos los demás usuarios, incluido "root", se les deniega explícitamente todas las operaciones. Tenga en cuenta, sin embargo, que "root" nunca se le deniegan los permisos para poner/obtener/DeleteBucketPolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Ejemplo: Permiso PutOverwriteObject

En este ejemplo, la `Deny` Effect para PutOverwriteObject y DeleteObject garantiza que nadie puede sobrescribir ni eliminar los datos del objeto, los metadatos definidos por el usuario y el etiquetado de objetos S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Ejemplo de políticas de grupo

Utilice los ejemplos de esta sección para crear políticas de acceso StorageGRID para grupos.

Las directivas de grupo especifican los permisos de acceso para el grupo al que está asociada la directiva. No existe `Principal` elemento de la política porque está implícito. Las políticas de grupo se configuran con el administrador de inquilinos o la API.

Ejemplo: Establecer la directiva de grupo mediante el Administrador de inquilinos

Al agregar o editar un grupo en el Gestor de inquilinos, puede seleccionar una política de grupo para determinar qué permisos de acceso S3 tendrán los miembros de este grupo. Consulte "Cree grupos para un inquilino de S3".

- **Sin acceso S3**: Opción predeterminada. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que el acceso se conceda con una política de bloque. Si selecciona esta opción, de forma predeterminada, solo el usuario raíz tendrá acceso a recursos de S3.
- **Acceso de sólo lectura**: Los usuarios de este grupo tienen acceso de sólo lectura a los recursos S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puede editar esta cadena.
- **Acceso completo**: Los usuarios de este grupo tienen acceso completo a los recursos S3, incluidos los bloques. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puede editar esta cadena.
- **Ransomware Mitigation**: Esta política de muestra se aplica a todos los cubos para este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden suprimir de forma permanente objetos de los bloques que tienen activado el control de versiones de objetos.

  Los usuarios del gestor de inquilinos que tengan el permiso Gestionar todos los bloques pueden sustituir esta política de grupo. Limite el permiso Gestionar todos los buckets a usuarios de confianza y use la autenticación multifactor (MFA) cuando esté disponible.

- **Personalizado**: A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto.

Ejemplo: Permite el acceso total de grupos a todos los bloques

En este ejemplo, a todos los miembros del grupo se les permite el acceso completo a todos los segmentos que pertenecen a la cuenta de inquilino, a menos que la política de bloque lo deniegue explícitamente.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Ejemplo: Permitir el acceso de solo lectura de grupo a todos los bloques

En este ejemplo, todos los miembros del grupo tienen acceso de solo lectura a recursos S3, a menos que la política de bloque lo deniegue explícitamente. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Ejemplo: Permitir a los miembros del grupo acceso completo solo a su carpeta en un depósito

En este ejemplo, sólo se permite a los miembros del grupo que enumeren y tengan acceso a su carpeta específica (prefijo de clave) en el bloque especificado. Tenga en cuenta que los permisos de acceso de otras políticas de grupo y la directiva de bloque deben tenerse en cuenta al determinar la privacidad de estas carpetas.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

Los servicios de StorageGRID generan los mensajes de auditoría y se almacenan en archivos de registro de texto. Es posible revisar los mensajes de auditoría específicos de S3 en el registro de auditoría para obtener detalles sobre las operaciones de bloques y objetos.

Se realizó un seguimiento de las operaciones de bloque en los registros de auditoría

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- Etiquetado de GetBucketTagging
- Segmento de cabeza
- ListObjects
- ListObjectVersions
- CUMPLIR con la normativa de los bloques
- PutBucketTagging
- PutBucketVersioning

Se realizó un seguimiento de las operaciones de objetos en los registros de auditoría

- CompleteMultipartUpload
- CopyObject
- DeleteObject
- GetObject
- Objeto principal
- Objeto de puta
- RestoreObject
- Seleccionar objeto
- UploadPart (cuando una regla de ILM utiliza una ingesta equilibrada o estricta)
- UploadPartCopy (cuando una regla de ILM utiliza una ingesta equilibrada o estricta)

Información relacionada

- "Acceda al archivo de registro de auditoría"
- "El cliente escribe mensajes de auditoría"
- "El cliente lee los mensajes de auditoría"

Usar la API REST DE Swift (obsoleto)

Use la API de REST DE Swift: Información general

Las aplicaciones cliente pueden usar la API Swift de OpenStack para interactuar con el sistema StorageGRID.

Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.

StorageGRID admite las siguientes versiones específicas de Swift y HTTP.

Elemento	Versión
Especificación Swift	OpenStack Swift Object Storage API v1 a fecha de noviembre de 2015
HTTP	1,1 Para obtener más información acerca de HTTP, vea HTTP/1.1 (RFC 7230-35). **Nota**: StorageGRID no admite canalización HTTP/1.1.

Información relacionada

"OpenStack: API de almacenamiento de objetos"

Historial de soporte de la API de Swift en StorageGRID

Debe estar al tanto de los cambios en la compatibilidad del sistema StorageGRID con la API DE REST de Swift.

Liberar	Comentarios
11,8	
11,7	Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.
11,6	Cambios editoriales menores.
11,5	Se eliminó la consistencia débil. En su lugar, se utilizará la consistencia disponible.
11,4	Añadido soporte para TLS 1,3. Se ha añadido la descripción de la interrelación entre ILM y la consistencia.
11,3	Las operaciones de PUT Object actualizadas para describir el impacto de las reglas de ILM que utilizan la colocación síncrona en el procesamiento (las opciones equilibradas y estrictas del comportamiento de procesamiento). Se ha agregado una descripción de las conexiones de cliente que utilizan extremos de equilibrador de carga o grupos de alta disponibilidad. Ya no se admiten los cifrados TLS 1.1.
11,2	Cambios editoriales menores en el documento.
11,1	Se añadió compatibilidad con el uso de HTTP para conexiones de clientes Swift a los nodos de grid. Se han actualizado las definiciones de los valores de consistencia.
11,0	Se ha agregado soporte para 1,000 contenedores por cada cuenta de inquilino.
10,3	Actualizaciones administrativas y correcciones en el documento. Se han eliminado secciones para configurar certificados de servidor personalizados.
10,2	Soporte inicial de la API Swift por el sistema StorageGRID. La versión compatible actualmente es la API de almacenamiento de objetos Swift de OpenStack v1.

Cómo StorageGRID implementa la API DE REST de Swift

Una aplicación cliente puede usar llamadas API DE REST de Swift para conectarse a nodos de almacenamiento y nodos de puerta de enlace para crear contenedores, así como para almacenar y recuperar objetos. De este modo, las aplicaciones orientadas a los servicios desarrolladas para OpenStack Swift pueden conectarse con el almacenamiento de objetos en las instalaciones que proporciona el sistema

StorageGRID.

Gestión de objetos Swift

Una vez que los objetos de Swift se han ingerido en el sistema StorageGRID, se gestionan con las reglas de gestión de la vida útil de la información (ILM) de las políticas de ILM activas. "Reglas de ILM" y.. "Políticas de ILM" Determinar cómo crea y distribuye StorageGRID copias de datos de objetos y cómo administra esas copias con el tiempo. Por ejemplo, una regla de ILM puede aplicarse a los objetos en contenedores Swift específicos y puede especificar que se guarden varias copias de objetos en varios centros de datos durante un determinado número de años.

Póngase en contacto con su asesor de los servicios profesionales de NetApp o administrador de StorageGRID si tiene que comprender cómo las reglas y las políticas de ILM del grid afectan a los objetos de su cuenta de inquilino Swift.

Solicitudes de clientes en conflicto

Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de Swift inician una operación.

Garantías y controles de coherencia

De forma predeterminada, StorageGRID proporciona coherencia de lectura tras escritura para los objetos recién creados y coherencia eventual para las actualizaciones de objetos y operaciones DE CABECERA. Cualquiera "OBTENGA" después de un completado correctamente "PUESTO" podrá leer los datos recién escritos. Las sobrescrituras de objetos existentes, actualizaciones de metadatos y eliminaciones son coherentes en la actualidad. Por lo general, las sobrescrituras tardan segundos o minutos en propagarse, pero pueden tardar hasta 15 días.

StorageGRID también le permite controlar la coherencia de cada contenedor. Los valores de consistencia proporcionan un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en diferentes nodos de almacenamiento y sitios, según lo requiera la aplicación.

Recomendaciones para implementar la API DE REST de Swift

Debe seguir estas recomendaciones al implementar la API DE REST de Swift para usar con StorageGRID.

Recomendaciones para las cabezas a los objetos no existentes

Si su aplicación comprueba periódicamente si existe un objeto en una ruta en la que no espera que exista realmente, debe utilizar la consistencia «disponible». Por ejemplo, debe utilizar la consistencia «disponible» si su aplicación realiza una operación de CABECERA en una ubicación antes de realizar una operación DE COLOCACIÓN en esa ubicación.

De lo contrario, si la operación HEAD no encuentra el objeto, es posible que reciba un número elevado de 500 errores internos de Server si uno o más nodos de almacenamiento no están disponibles.

Puede establecer la consistencia «disponible» para cada contenedor mediante el "PONGA la solicitud de consistencia del contenedor". Puede definir la consistencia disponible para cada contenedor mediante el "OBTENGA la solicitud de consistencia del contenedor".

Recomendaciones para los nombres de objetos

En el caso de los contenedores creados en StorageGRID 11.4 o posteriores, ya no es necesario restringir los nombres de objetos para cumplir con las prácticas recomendadas de rendimiento. Por ejemplo, ahora puede utilizar valores aleatorios para los primeros cuatro caracteres de nombres de objetos.

Para los contenedores que se crearon en las versiones anteriores a StorageGRID 11.4, siga estas recomendaciones para los nombres de objetos:

- No debe utilizar valores aleatorios como los primeros cuatro caracteres de nombres de objetos. Esto contrasta con la anterior recomendación de AWS para prefijos de nombres. En su lugar, debe utilizar prefijos no aleatorios y no únicos, como `image`.
- Si sigue la recomendación anterior de AWS de utilizar caracteres aleatorios y únicos en prefijos de nombre, debe aplicar un prefijo a los nombres de objeto con un nombre de directorio. Es decir, utilice este formato:

```
mycontainer/mydir/f8e3-image3132.jpg
```

En lugar de este formato:

```
mycontainer/f8e3-image3132.jpg
```

Recomendaciones para lecturas de rango

Si la "opción global para comprimir objetos almacenados" Esté habilitada, las aplicaciones cliente de Swift deben evitar la realización de OPERACIONES GET object que especifican un rango de bytes. Estas operaciones de «lectura de rango» son ineficientes, puesto que StorageGRID debe descomprimir los objetos de forma efectiva para acceder a los bytes solicitados. LAS operaciones GET Object que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, es muy ineficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

Si se leen rangos de objetos comprimidos, las solicitudes del cliente pueden tener un tiempo de espera.

> Si necesita comprimir objetos y su aplicación cliente debe utilizar lecturas de rango, aumente el tiempo de espera de lectura de la aplicación.

Probar la configuración de la API de REST DE Swift

Puede usar la CLI de Swift para probar la conexión con el sistema StorageGRID y verificar que pueda leer y escribir objetos.

Antes de empezar

- Ha descargado e instalado el cliente de la línea de comandos de Swift: "SwiftStack: python-swiftclient"
- Opcionalmente, tienes "se ha creado un punto final de equilibrio de carga". De lo contrario, conoce la dirección IP del nodo de almacenamiento al que desea conectarse y el número de puerto que se va a utilizar. Consulte "Puertos y direcciones IP para las conexiones de cliente".
- Ya tienes "Se ha creado una cuenta de inquilino de Swift".

- Ha iniciado sesión en la cuenta de inquilino y ha creado al menos un grupo y un usuario. Consulte "Cree grupos para un inquilino de Swift".

> Los usuarios de inquilino de Swift deben tener el permiso del grupo de administrador para autenticarse en la API DE REST DE Swift.

Acerca de esta tarea

Si no ha configurado la seguridad, debe añadir el `--insecure` marque cada uno de estos comandos.

Pasos

1. Consulte la URL de información para la implementación de Swift de StorageGRID:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

   Esto es suficiente para probar que la implementación de Swift es funcional. Para seguir probando la configuración de la cuenta almacenando un objeto, continúe con los pasos adicionales.

2. Coloque un objeto en el contenedor:

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Obtenga el contenedor para verificar el objeto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Elimine el objeto:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Elimine el contenedor:

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

Operaciones compatibles con la API REST de Swift

El sistema StorageGRID admite la mayoría de operaciones en la API Swift de OpenStack. Antes de integrar clientes API DE REST de Swift con StorageGRID, revise los detalles de la implementación para las operaciones de la cuenta, el contenedor y el objeto.

Operaciones compatibles con StorageGRID

Se admiten las siguientes operaciones de API de Swift:

- "Operaciones de cuentas"
- "Operaciones de contenedor"
- "Operaciones de objeto"

Encabezados de respuesta comunes para todas las operaciones

El sistema StorageGRID implementa todos los encabezados comunes para las operaciones compatibles según lo definido por la API de almacenamiento de objetos Swift de OpenStack v1.

Información relacionada

"OpenStack: API de almacenamiento de objetos"

Extremos de API de Swift compatibles

StorageGRID admite los siguientes extremos de la API de Swift: La URL de la información, la URL de autenticación y la URL de almacenamiento.

URL de información

Puede determinar las capacidades y las limitaciones de la implementación de Swift de StorageGRID emitiendo una solicitud GET a la URL de la base de Swift con la ruta /info.

`https://FQDN | Node IP:Swift Port/info/`

En la solicitud:

- *`FQDN`* es el nombre de dominio completo.
- *`Node IP`* Es la dirección IP del nodo de almacenamiento o del nodo de puerta de enlace en la red de StorageGRID.
- *`Swift Port`* Es el número de puerto que se usa para las conexiones API de Swift en el nodo de almacenamiento o la puerta de enlace.

Por ejemplo, la siguiente URL de información solicita información desde un nodo de almacenamiento con la dirección IP 10.99.106.103 y mediante el puerto 18083.

`https://10.99.106.103:18083/info/`

La respuesta incluye las capacidades de la implementación Swift como diccionario JSON. Una herramienta cliente puede analizar la respuesta JSON para determinar las capacidades de la implementación y usarlas como restricciones para operaciones de almacenamiento subsiguientes.

La implementación de StorageGRID de Swift permite un acceso sin autenticar a la URL de información.

URL de autenticación

Un cliente puede utilizar la URL de autenticación de Swift para autenticarse como usuario de cuenta de inquilino.

`https://FQDN | Node IP:Swift Port/auth/v1.0/`

Se deben proporcionar el ID de cuenta de inquilino, el nombre de usuario y la contraseña como parámetros en el `X-Auth-User` y.. `X-Auth-Key` solicite los encabezados de la siguiente manera:

`X-Auth-User: Tenant_Account_ID:Username`

`X-Auth-Key: Password`

En los encabezados de la solicitud:

- *`Tenant_Account_ID`* Es el ID de cuenta que asigna StorageGRID cuando se creó el inquilino de Swift. Este es el mismo ID de cuenta de arrendatario que se utiliza en la página de inicio de sesión de Gestor de inquilinos.
- *`Username`* Es el nombre de un usuario arrendatario que se ha creado en el Administrador de arrendatarios. Este usuario debe pertenecer a un grupo con permiso de administrador de Swift. El usuario raíz del inquilino no puede configurarse para usar la API REST DE Swift.

  Si la Federación de identidades está habilitada para la cuenta de inquilino, proporcione el nombre de usuario y la contraseña del usuario federado desde el servidor LDAP. Como alternativa, proporcione el nombre de dominio del usuario LDAP. Por ejemplo:

  `X-Auth-User: Tenant_Account_ID:Username@Domain_Name`

- *`Password`* es la contraseña del usuario inquilino. Las contraseñas de usuario se crean y administran en el Administrador de inquilinos.

La respuesta a una solicitud de autenticación correcta devuelve una URL de almacenamiento y un token de autenticación, de la siguiente forma:

```
X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID

X-Auth-Token: token

X-Storage-Token: token
```

De forma predeterminada, el token es válido durante 24 horas desde el tiempo de generación.

Se generan tokens para una cuenta de arrendatario específica. Un token válido para una cuenta no autoriza a un usuario a acceder a otra cuenta.

URL de almacenamiento

Una aplicación cliente puede emitir llamadas a la API DE REST de Swift para realizar operaciones de cuenta, contenedor y objeto admitidas contra un nodo de puerta de enlace o un nodo de almacenamiento. Las solicitudes de almacenamiento se dirigen a la URL de almacenamiento que se devuelve en la respuesta de autenticación. La solicitud también debe incluir el encabezado X-Auth-Token y el valor devuelto por la solicitud auth.

```
https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID

[/container][/object]

X-Auth-Token: token
```

Es posible que algunos encabezados de respuesta del almacenamiento que contienen estadísticas de uso no reflejen números precisos de los objetos modificados recientemente. Puede que en estos encabezados se deban utilizar unos minutos para que aparezcan números precisos.

Los siguientes encabezados de respuesta para las operaciones de cuentas y contenedores son ejemplos de los que contienen estadísticas de uso:

- `X-Account-Bytes-Used`
- `X-Account-Object-Count`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`

Información relacionada

"Configure las conexiones y las cuentas de inquilino"

"Operaciones de cuentas"

"Operaciones de contenedor"

"Operaciones de objeto"

Operaciones de cuentas

Las siguientes operaciones de la API de Swift se realizan en las cuentas.

OBTENGA la cuenta

Esta operación recupera la lista de contenedores asociada a las estadísticas de uso de la cuenta y la cuenta.

Se requiere el siguiente parámetro request:

- `Account`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Los siguientes parámetros de consulta de solicitud admitidos son opcionales:

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Prefix`

Una ejecución correcta devuelve las siguientes cabeceras con una respuesta HTTP/1,1 204 sin contenido si la cuenta se encuentra y no tiene contenedores o la lista de contenedores está vacía; o una respuesta HTTP/1,1 200 correcta si se encuentra la cuenta y la lista de contenedores no está vacía:

- `Accept-Ranges`
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

CUENTA principal

Esta operación recupera información de la cuenta y estadísticas de una cuenta de Swift.

Se requiere el siguiente parámetro request:

- `Account`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 204 sin contenido":

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Información relacionada

"Se realizó un seguimiento de las operaciones de Swift en los registros de auditoría"

Operaciones de contenedor

StorageGRID admite un máximo de 1,000 contenedores por cuenta de Swift. Las siguientes operaciones de la API de Swift se realizan en contenedores.

ELIMINAR contenedor

Esta operación elimina un contenedor vacío de una cuenta de Swift en un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 204 sin contenido":

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

OBTENGA el contenedor

Esta operación recupera la lista de objetos asociada con el contenedor junto con las estadísticas y los metadatos del contenedor en un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Los siguientes parámetros de consulta de solicitud admitidos son opcionales:

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Path`
- `Prefix`

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 200 Success" o "HTTP/1.1 204 sin contenido":

- `Accept-Ranges`
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Contenedor DE LA CABEZA

Esta operación recupera las estadísticas y los metadatos del contenedor de un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 204 sin contenido":

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

COLOQUE el contenedor

Esta operación crea un contenedor para una cuenta en un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 201 creado" o "HTTP/1.1 202 aceptado" (si el contenedor ya existe bajo esta cuenta):

- `Content-Length`
- `Date`
- `X-Timestamp`
- `X-Trans-Id`

Un nombre de contenedor debe ser único en el espacio de nombres de StorageGRID. Si el contenedor existe en otra cuenta, se devuelve el siguiente encabezado: "Conflicto HTTP/1.1 409".

Información relacionada

"Supervisar y auditar operaciones"

Operaciones de objeto

Las siguientes operaciones de la API de Swift se realizan en objetos. Se puede realizar un seguimiento de estas operaciones en la "Registro de auditoría de StorageGRID".

ELIMINAR objeto

Esta operación elimina los metadatos y el contenido de un objeto del sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`

- `Container`
- `Object`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Una ejecución correcta devuelve los encabezados de respuesta siguientes con un `HTTP/1.1 204 No Content` respuesta:

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Al procesar una solicitud DE ELIMINACIÓN de objeto, StorageGRID intenta eliminar inmediatamente todas las copias del objeto de todas las ubicaciones almacenadas. Si se realiza correctamente, StorageGRID devuelve una respuesta al cliente inmediatamente. Si no se pueden eliminar todas las copias en 30 segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y, a continuación, indica que se ha realizado correctamente al cliente.

Para obtener más información, consulte "Cómo se eliminan los objetos".

OBJETO GET

Esta operación recupera el contenido de objetos y obtiene los metadatos de objetos de un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`
- `Object`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Los siguientes encabezados de solicitud son opcionales:

- `Accept-Encoding`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Una ejecución correcta devuelve los encabezados siguientes con un `HTTP/1.1 200 OK` respuesta:

- `Accept-Ranges`
- `Content-Disposition`, devuelto sólo si `Content-Disposition` se establecieron los metadatos
- `Content-Encoding`, devuelto sólo si `Content-Encoding` se establecieron los metadatos
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

OBJETO HEAD

Esta operación recupera los metadatos y las propiedades de un objeto ingerido desde un sistema StorageGRID.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`
- `Object`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 200 OK":

- `Accept-Ranges`
- `Content-Disposition`, devuelto sólo si `Content-Disposition` se establecieron los metadatos
- `Content-Encoding`, devuelto sólo si `Content-Encoding` se establecieron los metadatos
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

PONER objeto

Esta operación crea un objeto nuevo con datos y metadatos, o reemplaza un objeto existente con datos y metadatos en un sistema StorageGRID.

La StorageGRID admite objetos de hasta 5 TIB (5,497,558,138,880 bytes) con un tamaño.

> Las solicitudes de clientes en conflicto, como dos clientes que escriben en la misma clave, se resuelven en función de las "últimas victorias". El plazo para la evaluación de "logros más recientes" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes de Swift inician una operación.

Se requieren los siguientes parámetros de solicitud:

- `Account`
- `Container`
- `Object`

Se requiere el siguiente encabezado de solicitud:

- `X-Auth-Token`

Los siguientes encabezados de solicitud son opcionales:

- `Content-Disposition`
- `Content-Encoding`

  No utilice fragmentos `Content-Encoding` Si la regla de ILM que se aplica a un objeto filtra objetos según el tamaño y utiliza la ubicación síncrona durante el procesamiento (las opciones equilibradas o estrictas del comportamiento de ingesta).

- `Transfer-Encoding`

  No utilice comprimidos ni fragmentados `Transfer-Encoding` Si la regla de ILM que se aplica a un objeto filtra objetos según el tamaño y utiliza la ubicación síncrona durante el procesamiento (las opciones equilibradas o estrictas del comportamiento de ingesta).

- `Content-Length`

  Si una regla de ILM filtra objetos por tamaño y utiliza la ubicación síncrona durante el procesamiento, debe especificar `Content-Length`.

  > Si no sigue estas directrices para `Content-Encoding`, `Transfer-Encoding`, y. `Content-Length`, StorageGRID debe guardar el objeto para poder determinar el tamaño del objeto y aplicar la regla ILM. En otras palabras, StorageGRID debe crear de forma predeterminada copias provisionales de un objeto durante el procesamiento. Es decir, StorageGRID debe utilizar la opción Dual COMMIT para el comportamiento de procesamiento.

  Para obtener más información sobre la ubicación síncrona y las reglas de ILM, consulte "Opciones de protección de datos para consumo".

- `Content-Type`
- `ETag`
- `X-Object-Meta-<name\>` (metadatos relacionados con objetos)

  Si desea utilizar la opción **Tiempo de creación definido por el usuario** como tiempo de referencia para una regla de ILM, debe almacenar el valor en un encabezado definido por el usuario llamado `X-Object-Meta-Creation-Time`. Por ejemplo:

  ```
  X-Object-Meta-Creation-Time: 1443399726
  ```

  Este campo se evalúa como segundos desde el 1 de enero de 1970.

- `X-Storage-Class: reduced_redundancy`

  Este encabezado afecta al número de copias de objeto que crea StorageGRID si la regla de ILM que coincide con un objeto ingerido especifica un comportamiento de procesamiento de Doble COMMIT o equilibrado.

  - **Commit doble**: Si la regla ILM especifica la opción COMMIT doble para el comportamiento de la ingesta, StorageGRID crea una única copia provisional mientras se ingiere el objeto (COMMIT único).
  - **Equilibrado**: Si la regla de ILM especifica la opción Equilibrada, StorageGRID hace una sola copia provisional solo si el sistema no puede hacer inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar una colocación síncrona, este encabezado no tiene ningún efecto.

    La `reduced_redundancy` El encabezado se utiliza mejor cuando la regla de ILM que coincide con el objeto crea una única copia replicada. En este caso, utilizar `reduced_redundancy` elimina la creación y eliminación innecesarias de una copia de objetos adicional en cada operación de procesamiento.

    Con el `reduced_redundancy` la cabecera no se recomienda en otras circunstancias porque aumenta el riesgo de pérdida de datos de objetos durante el procesamiento. Por ejemplo, puede perder datos si la única copia se almacena inicialmente en un nodo de almacenamiento que falla antes de que se pueda realizar la evaluación de ILM.

    > Tener solo una copia replicada durante un periodo de tiempo pone los datos en riesgo de pérdida permanente. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

  Tenga en cuenta que especificar `reduced_redundancy` sólo afecta al número de copias que se crean cuando un objeto se ingiere por primera vez. No afecta a cuántas copias del objeto se realizan cuando se evalúan el objeto mediante las políticas de ILM activas y no dan como resultado el almacenamiento de los datos en niveles de redundancia más bajos del sistema StorageGRID.

Una ejecución correcta devuelve los siguientes encabezados con una respuesta "HTTP/1.1 201 creado":

- `Content-Length`

- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Trans-Id`

SOLICITUD DE OPCIONES

La solicitud DE OPCIONES comprueba la disponibilidad de un servicio Swift individual. El nodo de almacenamiento o el nodo de puerta de enlace especificado en la URL procesan la solicitud DE OPCIONES.

MÉTODO DE OPCIONES

Por ejemplo, las aplicaciones cliente pueden emitir una solicitud DE OPCIONES al puerto Swift en un nodo de almacenamiento sin proporcionar las credenciales de autenticación Swift para determinar si el nodo de almacenamiento está disponible. Puede usar esta solicitud para supervisar o para permitir que los equilibradores de carga externos identifiquen cuando un nodo de almacenamiento esté inactivo.

Cuando se utiliza con la URL de información o la URL de almacenamiento, el método OPTIONS devuelve una lista de verbos admitidos para la URL dada (por ejemplo, HEAD, GET, OPTIONS y PUT). El método de OPCIONES no se puede utilizar con la URL de autenticación.

Se requiere el siguiente parámetro request:

- `Account`

Los siguientes parámetros de solicitud son opcionales:

- `Container`
- `Object`

Una ejecución correcta devuelve las siguientes cabeceras con una respuesta de HTTP/1,1 204 sin contenido. La solicitud DE OPCIONES a la URL de almacenamiento no requiere que exista el destino.

- `Allow` (Una lista de verbos admitidos para la dirección URL dada, por ejemplo, CABEZA, OBTENER, OPCIONES, Y PUESTO)
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Información relacionada

"Extremos de API de Swift compatibles"

Respuesta de error a las operaciones de la API de Swift

Comprender las posibles respuestas de error puede ayudar a resolver las operaciones.

Pueden devolverse los siguientes códigos de estado HTTP cuando se produzcan errores durante una operación:

Nombre de error de Swift	Estado de HTTP
AccountNameTooLong, ContainerNameTooLong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameTooLong, MetadataValueTooBig, MissingSecurityHeader, ObjectNameTooLong, TooManyContainers, TooManyMetadataItems, TotalMetadataTooLarge	400 solicitud incorrecta
ACCESSDENIED	403 Prohibido
ContainerNotEmpty, ContainerAlreadyExists	409 conflicto
Internalerror	500 error de servidor interno
InvalidRange	416 rango solicitado no utilizable
MethodNotAllowed	405 método no permitido
MissingContentLength	411 longitud requerida
NOTFOUND	404 no encontrado
NotImplimed	501 no implementada
Error de precondiciónError	Error de condición 412
ResourceNotFound	404 no encontrado
No autorizado	401 no autorizado
Entidad no procesable	422 entidad no procesable

Operaciones de la API de REST de StorageGRID Swift

Existen operaciones que se añaden a la API DE REST de Swift que son específicas del sistema StorageGRID.

OBTENGA la solicitud de consistencia del contenedor

"Valores de coherencia" Proporcionar un equilibrio entre la disponibilidad de los objetos y la coherencia de

dichos objetos en distintos nodos de almacenamiento y sitios. La solicitud OBTENER consistencia de contenedor le permite determinar la consistencia que se aplica a un contenedor en particular.

Solicitud

Solicitar encabezado HTTP	Descripción
Token X-Auth	Especifica el token de autenticación Swift de la cuenta que se va a utilizar para la solicitud.
x-ntap-sg-consistency	Especifica el tipo de solicitud, donde `true` = OBTENER la consistencia del contenedor, y. `false` = OBTENER contenedor.
Host	El nombre de host al que se dirige la solicitud.

Ejemplo de solicitud

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Respuesta

Encabezado HTTP de respuesta	Descripción
Fecha	La fecha y la hora de la respuesta.
Conexión	Si la conexión con el servidor está abierta o cerrada.
X-Trans-ID	Identificador de transacción único para la solicitud.
Longitud de contenido	La longitud del cuerpo de respuesta.

Encabezado HTTP de respuesta	Descripción
x-ntap-sg-consistency	La consistencia que se aplica al contenedor. Se admiten los siguientes valores: **Todos**: Todos los nodos reciben los datos inmediatamente o la solicitud fallará. **Strong-global**: Garantiza la consistencia de lectura tras escritura para todas las solicitudes de los clientes en todos los sitios. **Strong-site**: Garantiza la consistencia de lectura después de escritura para todas las solicitudes de los clientes dentro de un sitio. **Read-after-new-write**: (Por defecto) proporciona consistencia de lectura después de escritura para nuevos objetos y consistencia eventual para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos. **Disponible**: Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

Ejemplo de respuesta

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

PONGA la solicitud de consistencia del contenedor

La solicitud de consistencia de contenedor PUT permite especificar la coherencia que se aplicará a las operaciones realizadas en un contenedor. De forma predeterminada, se crean nuevos contenedores con la consistencia de lectura tras nueva escritura.

Solicitud

Solicitar encabezado HTTP	Descripción
Token X-Auth	El token de autenticación Swift de la cuenta que se va a utilizar para la solicitud.

Solicitar encabezado HTTP	Descripción
x-ntap-sg-consistency	La coherencia que se debe aplicar a las operaciones en el contenedor. Se admiten los siguientes valores: **Todos**: Todos los nodos reciben los datos inmediatamente o la solicitud fallará. **Strong-global**: Garantiza la consistencia de lectura tras escritura para todas las solicitudes de los clientes en todos los sitios. **Strong-site**: Garantiza la consistencia de lectura después de escritura para todas las solicitudes de los clientes dentro de un sitio. **Read-after-new-write**: (Por defecto) proporciona consistencia de lectura después de escritura para nuevos objetos y consistencia eventual para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos. **Disponible**: Proporciona consistencia eventual tanto para nuevos objetos como para actualizaciones de objetos. Para los cubos S3, utilice solo según sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.
`Host`	El nombre de host al que se dirige la solicitud.

Cómo interactúan las reglas de coherencia e ILM para afectar a la protección de datos

Ambas opciones "valor de coherencia" Y la regla de ILM afectan a la forma en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, la consistencia utilizada cuando se almacena un objeto afecta la ubicación inicial de los metadatos del objeto, mientras que el "comportamiento de ingesta" Seleccionada para la regla de ILM afecta la ubicación inicial de las copias del objeto. Dado que StorageGRID requiere acceso a los metadatos de un objeto y a sus datos para satisfacer las solicitudes de los clientes, seleccionar niveles de protección correspondientes para la coherencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas del sistema más predecibles.

Un ejemplo de cómo pueden interactuar las reglas de coherencia e ILM

Suponga que tiene un grid de dos sitios con la siguiente regla de ILM y la siguiente consistencia:

- **Norma ILM**: Cree dos copias de objetos, una en el sitio local y otra en un sitio remoto. Se ha seleccionado el comportamiento de procesamiento estricto.
- **: “Strong-global” (los metadatos de objetos se distribuyen inmediatamente a todos los sitios.)

Cuando un cliente almacena un objeto en el grid, StorageGRID realiza copias de objetos y distribuye los metadatos en ambos sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra la pérdida en el momento del mensaje de procesamiento

correcto. Por ejemplo, si el sitio local se pierde poco después del procesamiento, seguirán existiendo copias de los datos del objeto y los metadatos del objeto en el sitio remoto. El objeto se puede recuperar completamente.

Si, en cambio, ha usado la misma regla de ILM y la coherencia de «sitio seguro», es posible que el cliente reciba un mensaje de éxito después de que los datos de objetos se repliquen en el sitio remoto, pero antes de que los metadatos de objetos se distribuyan allí. En este caso, el nivel de protección de los metadatos de objetos no coincide con el nivel de protección de los datos de objetos. Si el sitio local se pierde poco después del procesamiento, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre las reglas de coherencia y de ILM puede ser compleja. Póngase en contacto con NetApp si necesita ayuda.

Ejemplo de solicitud

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

Respuesta

Encabezado HTTP de respuesta	Descripción
`Date`	La fecha y la hora de la respuesta.
`Connection`	Si la conexión con el servidor está abierta o cerrada.
`X-Trans-Id`	Identificador de transacción único para la solicitud.
`Content-Length`	La longitud del cuerpo de respuesta.

Ejemplo de respuesta

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

Se realizó un seguimiento de las operaciones de Swift en los registros de auditoría

Se realiza un seguimiento de todas las operaciones DE ELIMINACIÓN, GET, HEAD, POST y PUT de almacenamiento correctamente en el registro de auditoría de StorageGRID. Los fallos y las solicitudes de información, autenticación u OPCIONES no se registran.

Operaciones de cuentas

- "OBTENGA la cuenta"
- "CUENTA principal"

Operaciones de contenedor

- "ELIMINAR contenedor"
- "OBTENGA el contenedor"
- "Contenedor DE LA CABEZA"
- "COLOQUE el contenedor"

Operaciones de objeto

- "ELIMINAR objeto"
- "OBJETO GET"
- "OBJETO HEAD"
- "PONER objeto"

Información relacionada

- "Acceda al archivo de registro de auditoría"
- "El cliente escribe mensajes de auditoría"
- "El cliente lee los mensajes de auditoría"

Supervisar y solucionar problemas de un sistema StorageGRID

Supervise el sistema StorageGRID

Supervisar un sistema StorageGRID: Descripción general

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya 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"
  - "Capacidad de archivado"
- "Gestionar alertas y alarmas heredadas"
- "Ver archivos de registro"
- "Configurar los mensajes de auditoría y los destinos de registro"
- "Use un servidor de syslog externo" para recopilar información de auditoría
- "Utilice SNMP para la supervisión"
- "Obtener más datos de StorageGRID", incluyendo métricas y diagnósticos

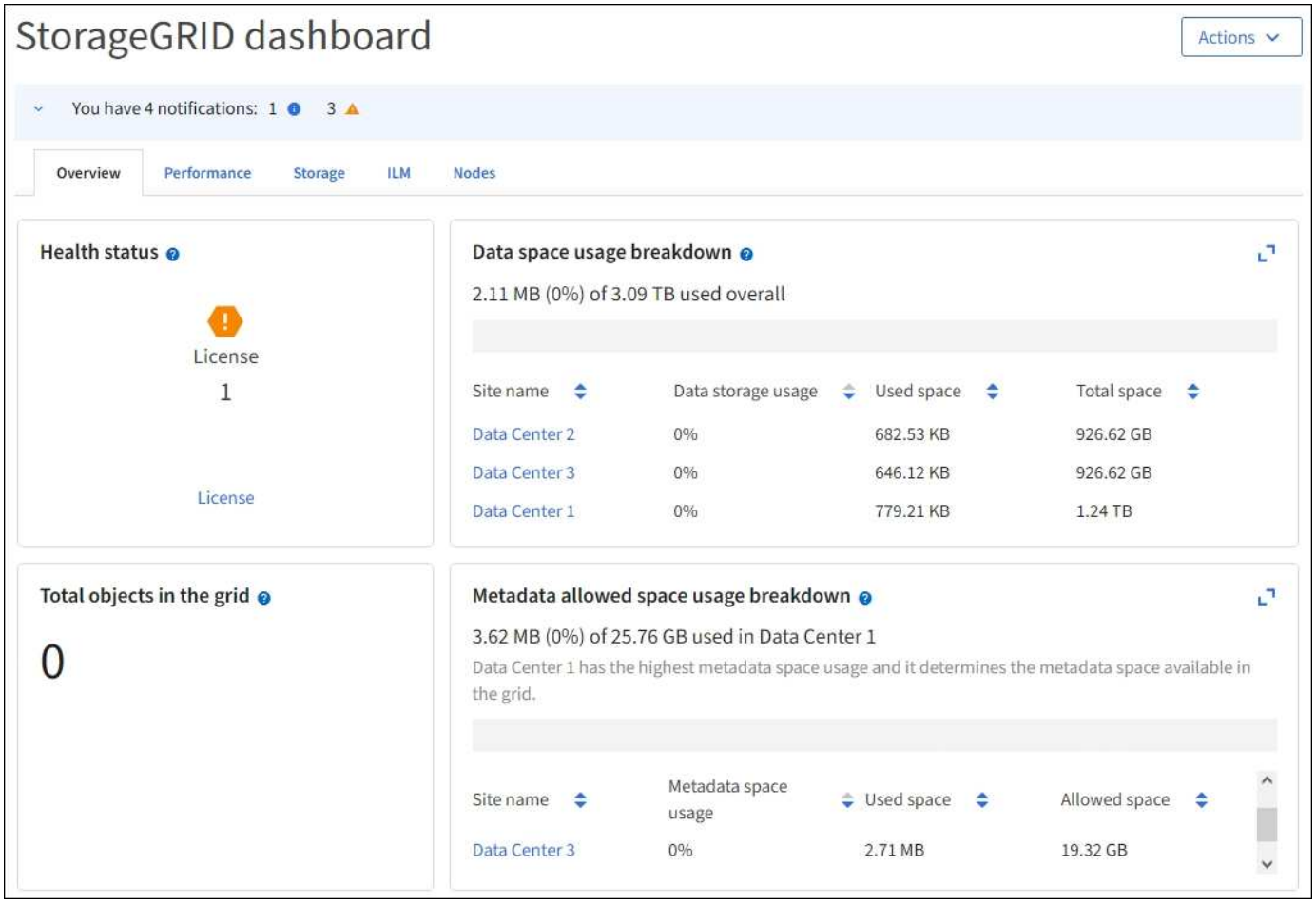
Permite ver y gestionar el panel de control

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.



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, operaciones S3 o Swift, 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. Operaciones S3 o Swift 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, seleccione el icono Minimizar O seleccione **Cerrar**.

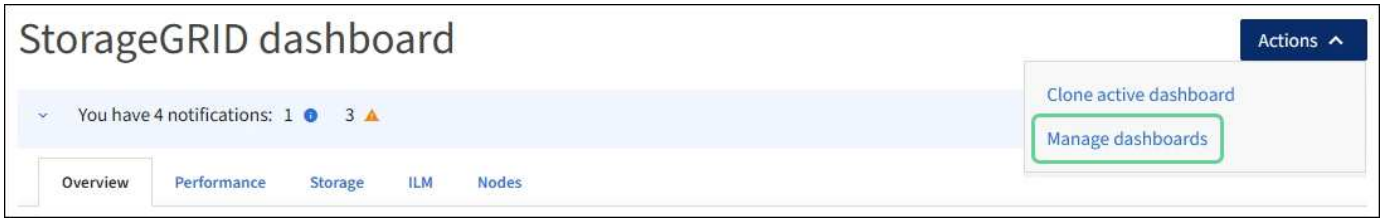
Gestionar paneles

Si tiene 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**.



Configurar paneles de control

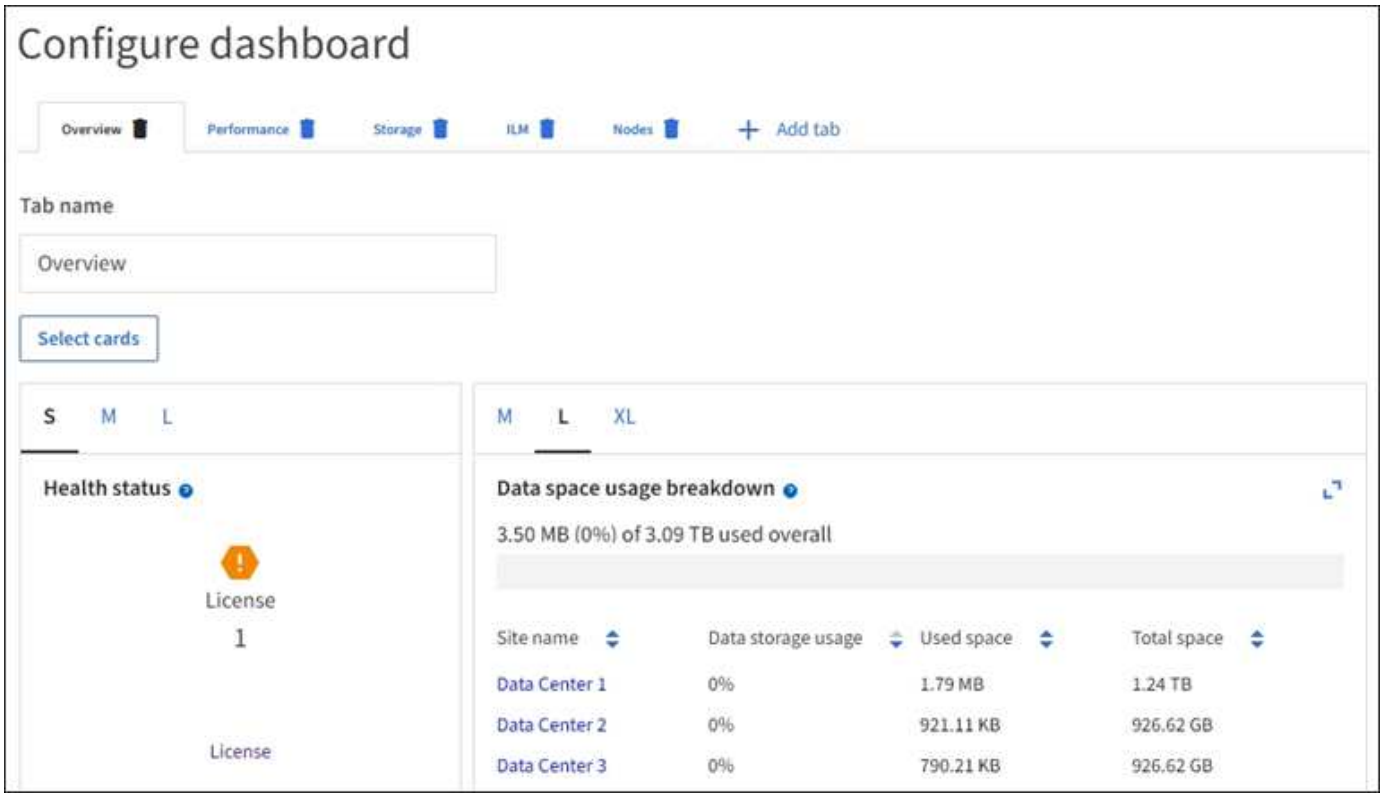
Para crear un nuevo panel clonando el panel activo, seleccione **Acciones** > **Clonar panel activo**.

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



Vea la página Nodes

Consulte la página Nodos: Información general

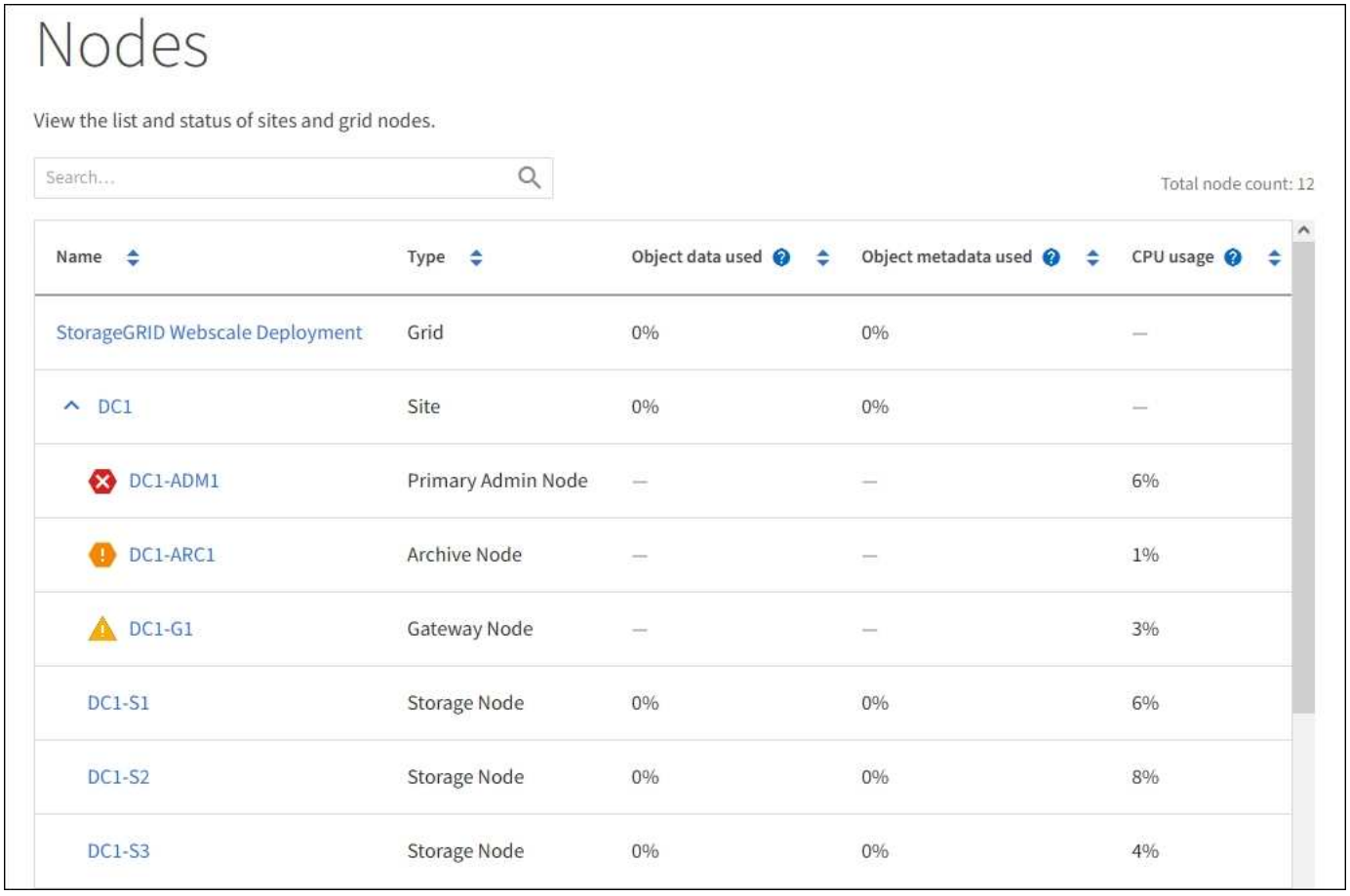
Cuando necesite información más detallada sobre el sistema de StorageGRID que la que

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 icono junto al nombre del nodo. Si el nodo está conectado y no tiene alertas activas, no se muestra ningún icono.

> 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.

> 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**.



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
	No conectado - Desconocido 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. La alerta **no se puede comunicar con el nodo** también puede activarse. Otras alertas también pueden estar activas.	Requiere atención inmediata. "Seleccione cada alerta" y siga las acciones recomendadas. Por ejemplo, es posible que deba reiniciar un servicio que haya detenido o reiniciar el host del nodo. **Nota**: Un nodo puede aparecer como Desconocido durante las operaciones de cierre administradas. Puede ignorar el estado Desconocido en estos casos.
	No conectado - administrativamente abajo Por un motivo esperado, el nodo no está conectado a la cuadrícula. 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. En función del problema subyacente, estos nodos suelen volver a estar en línea sin ninguna intervención.	Determine si alguna alerta afecta a este nodo. Si una o más alertas están activas, "Seleccione cada alerta" y siga las acciones recomendadas.

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.

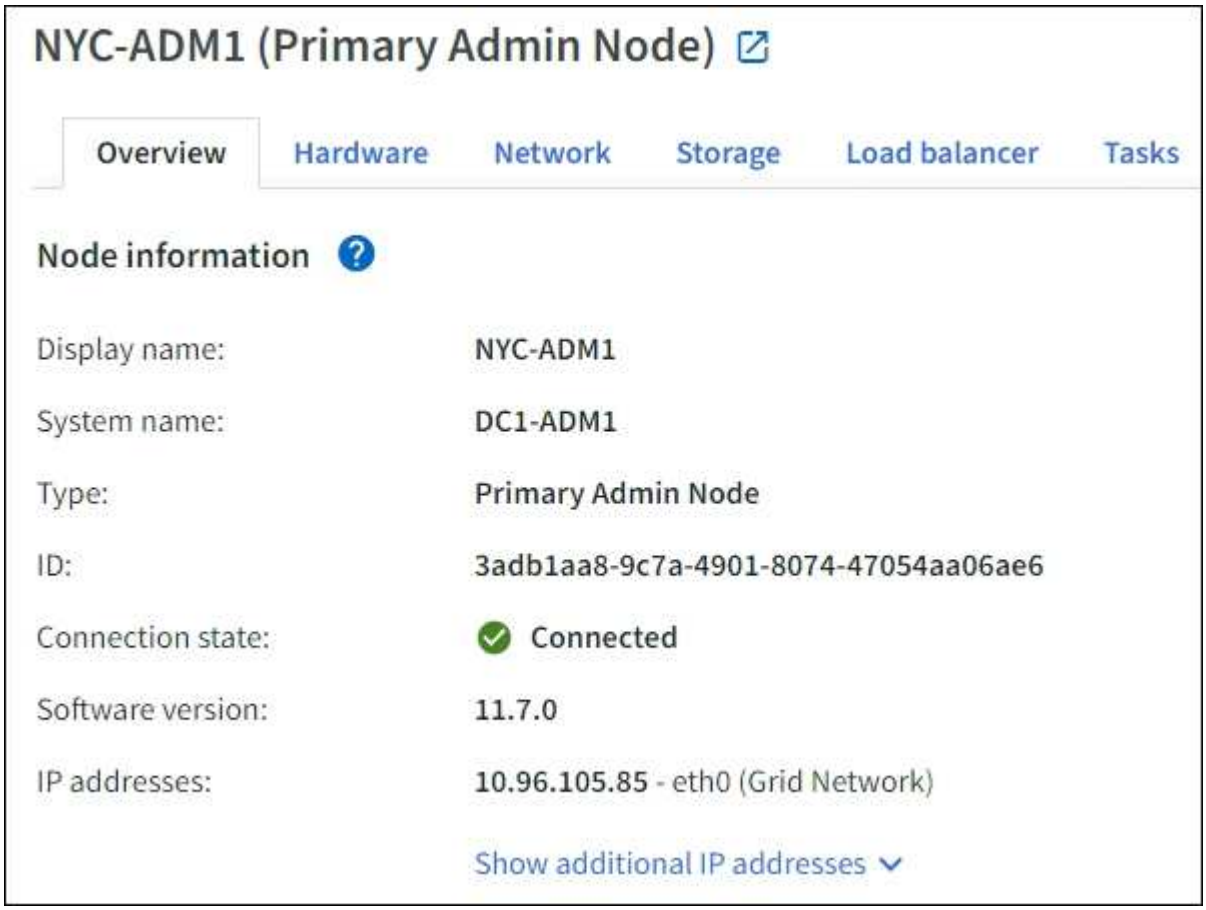
Vea la ficha Descripción general

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.



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 la "Cambie 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**: Tipo de nodo — nodo de administración, nodo de administración principal, nodo de almacenamiento, nodo de puerta de enlace o nodo de archivado.

> La compatibilidad con los nodos de archivo está obsoleta y se eliminará en una versión futura. El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades.

- **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 cuadrícula, o uno o más servicios están inesperadamente inactivos. 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 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. Una o más alertas también pueden estar activas.
  - **Conectado**: El nodo está conectado a la cuadrícula.
- **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 cualquiera "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.

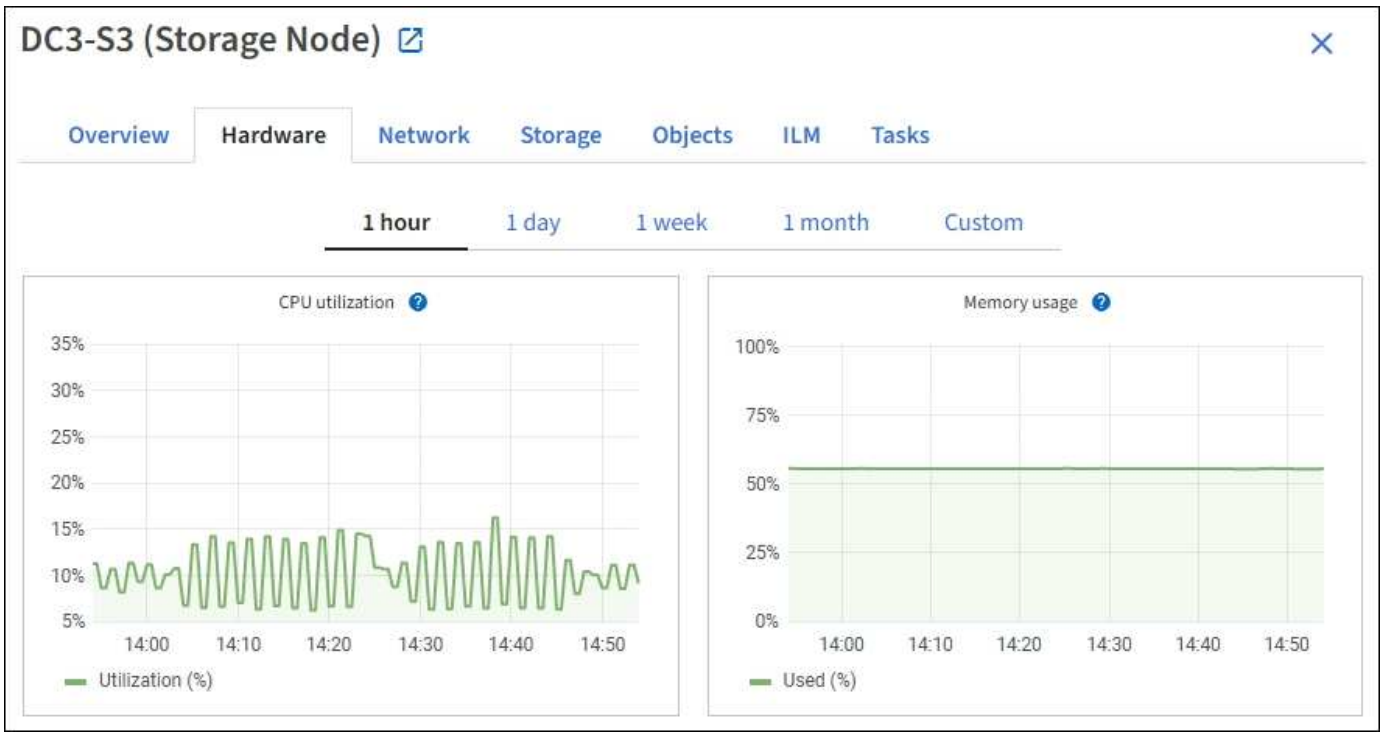
También se incluyen alertas para "estados de conexión de nodo".

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.

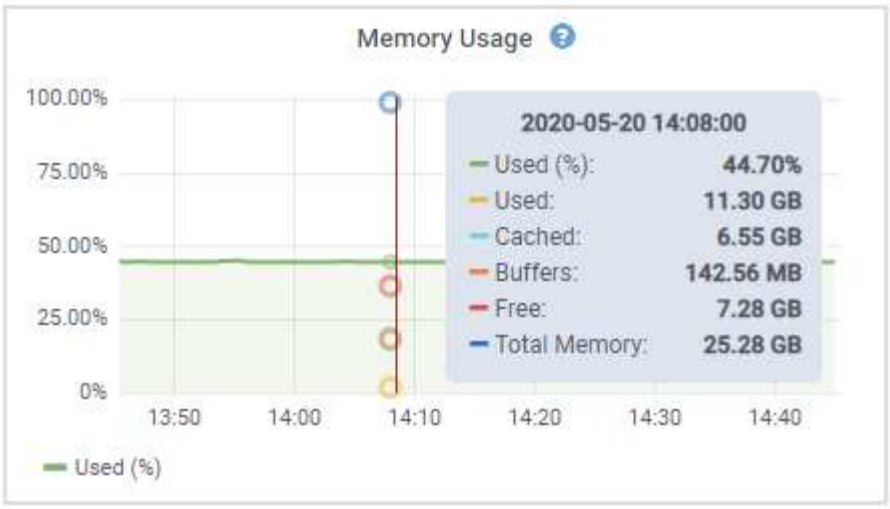
> Grid Manager se actualiza con cada versión, por lo que es posible que no coincida con las capturas de pantalla de los ejemplos de esta página.

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

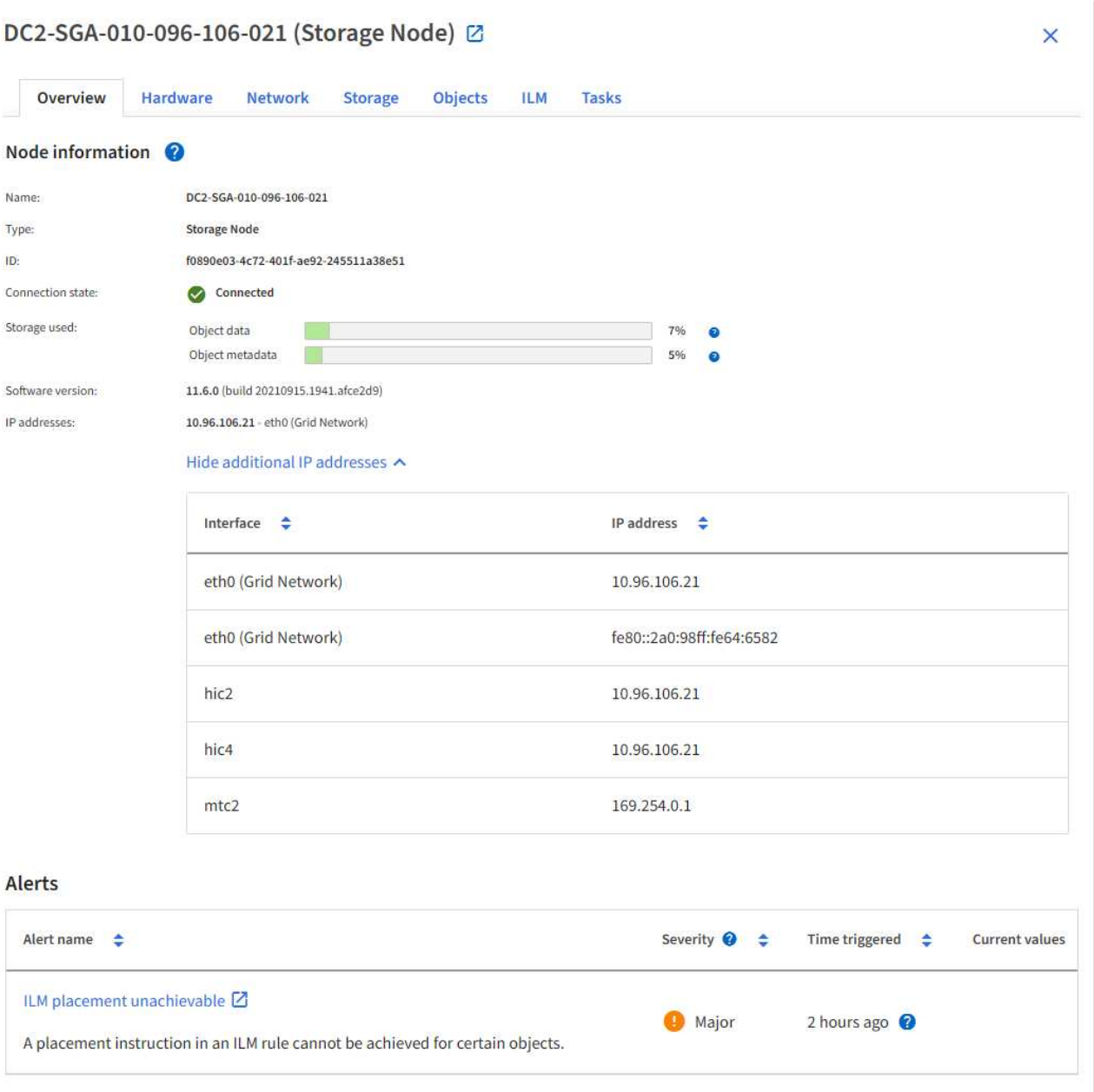
En la página Nodes, se incluye información sobre el estado del servicio y todos los recursos computacionales, de dispositivo de disco y de red para cada nodo de almacenamiento del dispositivo. También puede ver memoria, hardware de almacenamiento, versión del firmware de la controladora, recursos de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

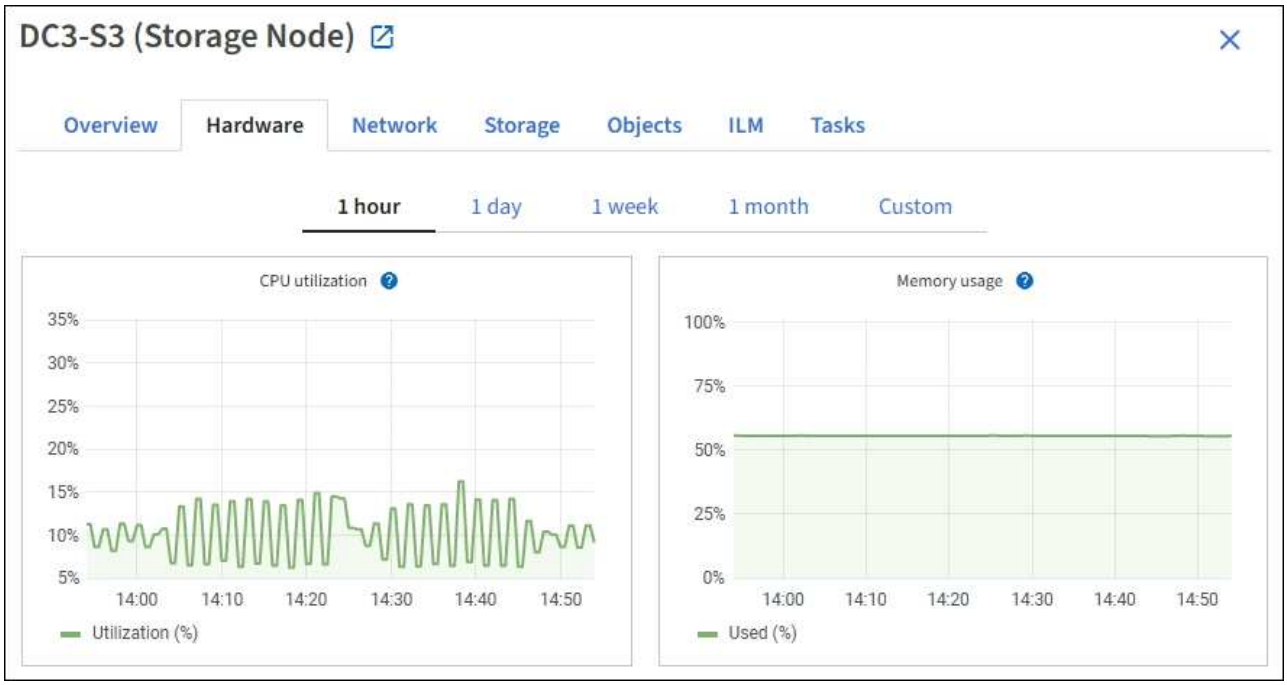
   - **Eth**: Red Grid, red de administración o red de cliente.
   - **Clic**: Uno de los puertos 10, 25 o 100 GbE físicos del aparato. Estos puertos se pueden unir y conectar a la red de cuadrícula de StorageGRID (eth0) y a la red de cliente (eth2).
   - * mtc*: Uno de los puertos físicos de 1 GbE del 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.



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.

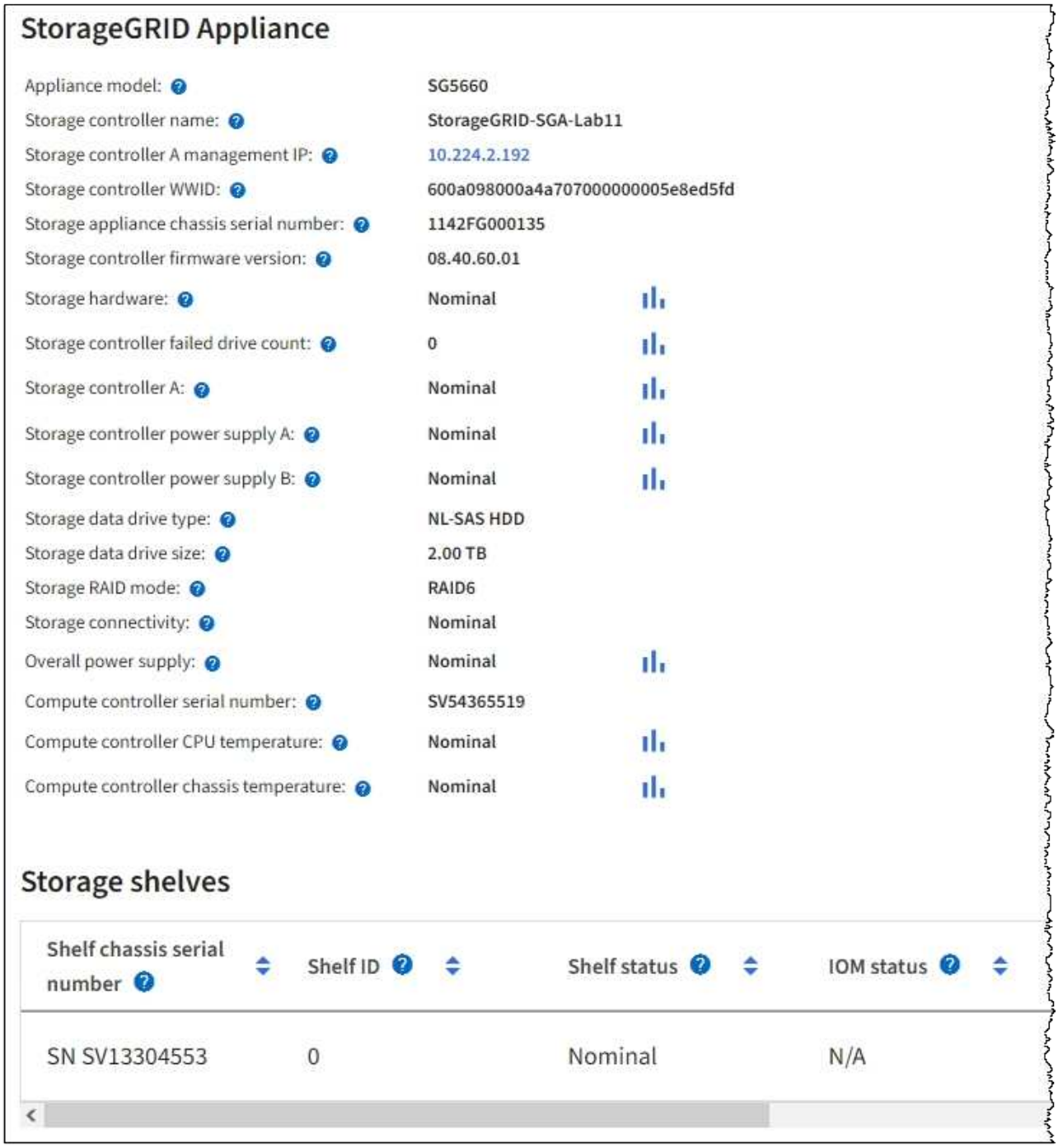
   a. Consulte los gráficos de utilización de CPU y memoria para determinar los porcentajes de uso de CPU y memoria a lo largo del tiempo. Para mostrar un intervalo de tiempo diferente, seleccione uno de los controles situados encima del gráfico o gráfico. Puede visualizar la información disponible para 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.



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	Dirección IP para el puerto de gestión 1 en la controladora de almacenamiento A. Esta IP se utiliza para acceder a SANtricity OS para solucionar problemas de almacenamiento.

En la tabla dispositivo	Descripción
IP de gestión de la controladora de almacenamiento B.	Dirección IP para el puerto de gestión 1 en la controladora de almacenamiento B. Esta IP se utiliza para acceder a SANtricity OS para solucionar problemas de almacenamiento. Algunos modelos de dispositivos no tienen una controladora de almacenamiento B.
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.
Hardware de almacenamiento	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. Si el estado es «Necesita atención», compruebe primero la controladora de almacenamiento con SANtricity OS. A continuación, asegúrese de que no existan otras alarmas que se apliquen al controlador de computación.
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.
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).

En la tabla dispositivo	Descripción
Tamaño de las unidades de datos de almacenamiento	El tamaño efectivo de una unidad de datos. **Nota**: Para los nodos con estantes de expansión, utilice 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.
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	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. Este campo no se muestra para los modelos de dispositivos que no contienen una BMC.
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	El identificador numérico de la bandeja de almacenamiento. • 99: Bandeja de controladoras de almacenamiento • 0: Primer estante de expansión • 1: Segunda bandeja de expansión **Nota:** las estanterías de expansión se aplican sólo al SG6060.
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.

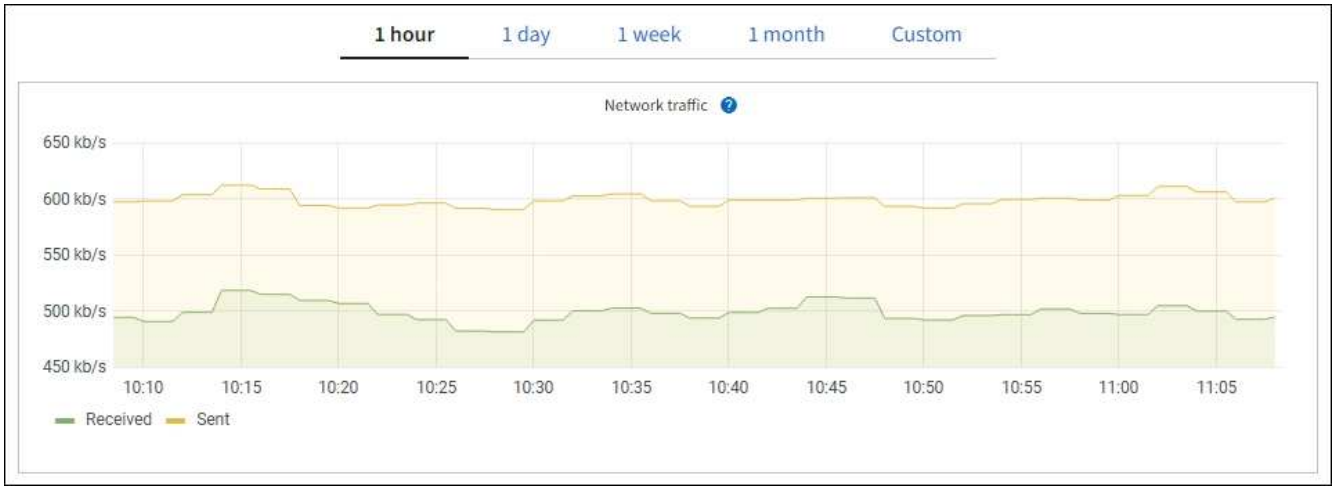
a. Confirmar que todos los estados son nominales.

   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

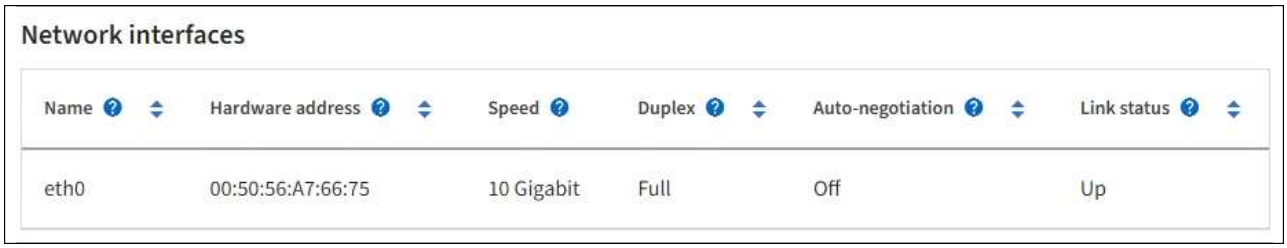
instrucciones de instalación y mantenimiento del aparato.

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.



   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.

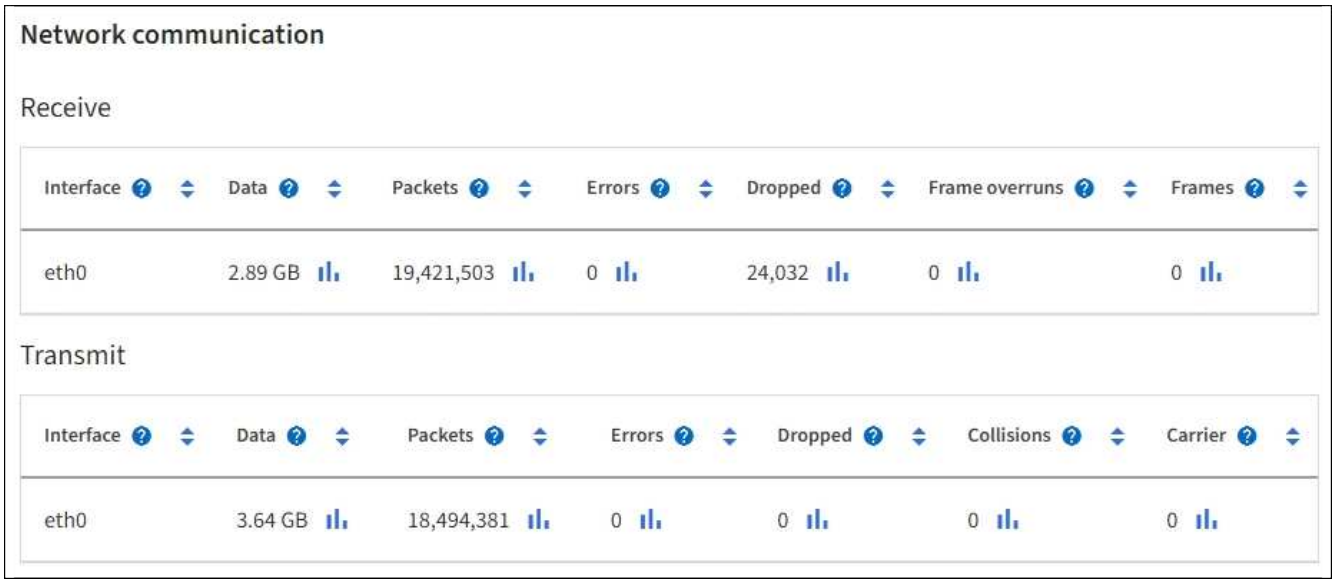
   Los valores mostrados en la tabla asumen que se utilizan los cuatro enlaces.

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
Fija	Activa/Backup	10	10

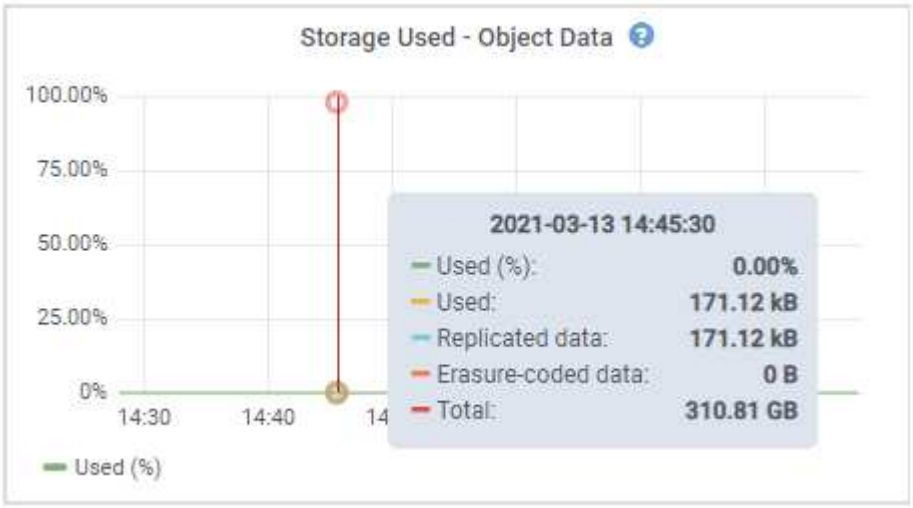
Consulte "Configure los enlaces de red" Para obtener más información sobre la configuración de los puertos 10/25 GbE.

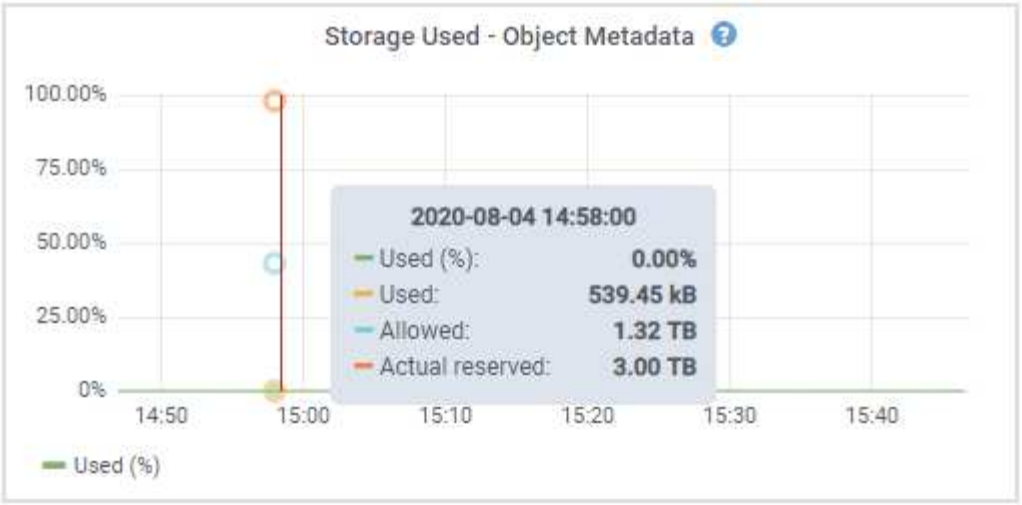
b. Revise la sección Comunicación de red.

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.



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.

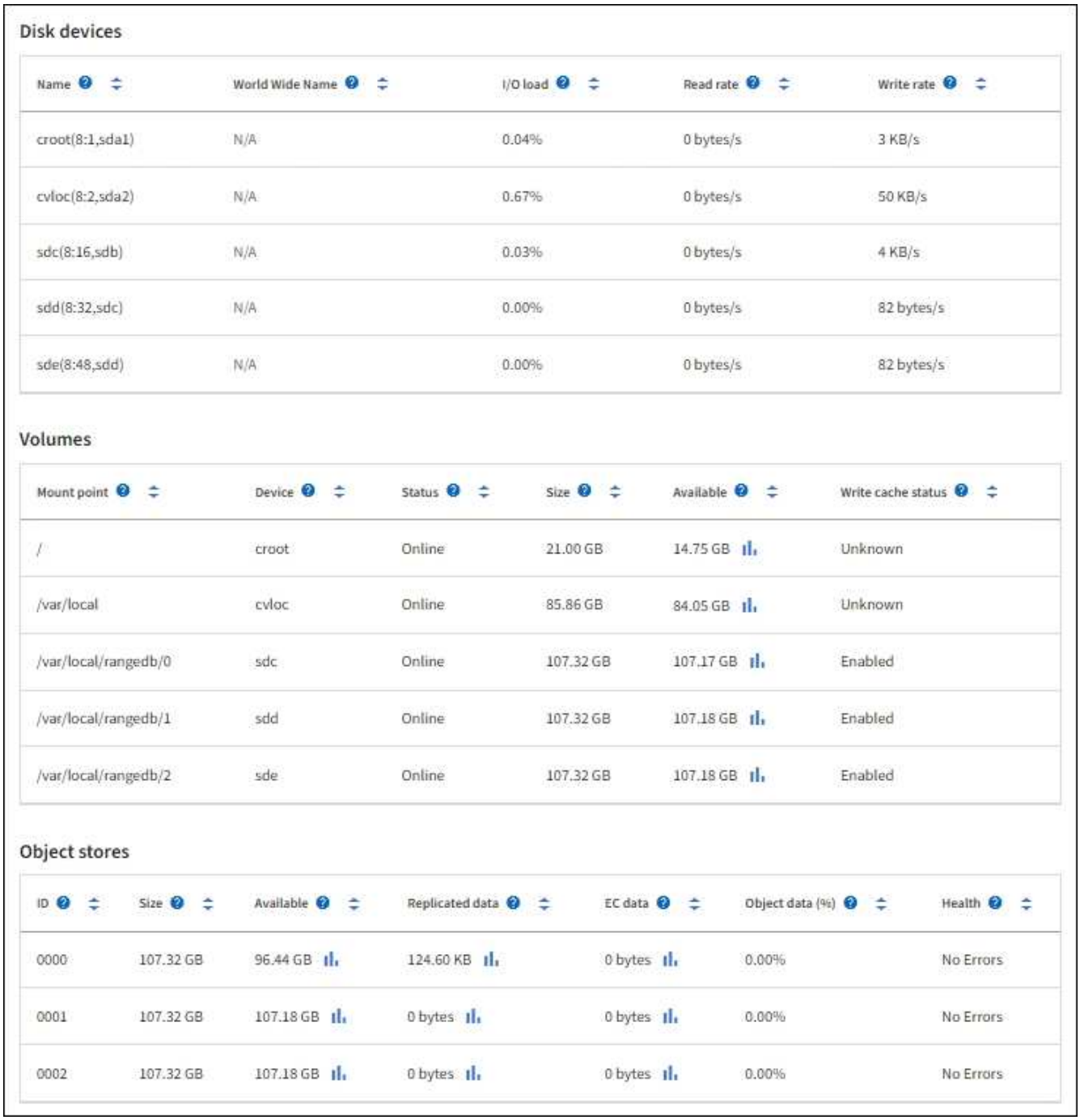




a. Desplácese hacia abajo para ver la cantidad de almacenamiento disponible para cada volumen y almacén de objetos.

   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.

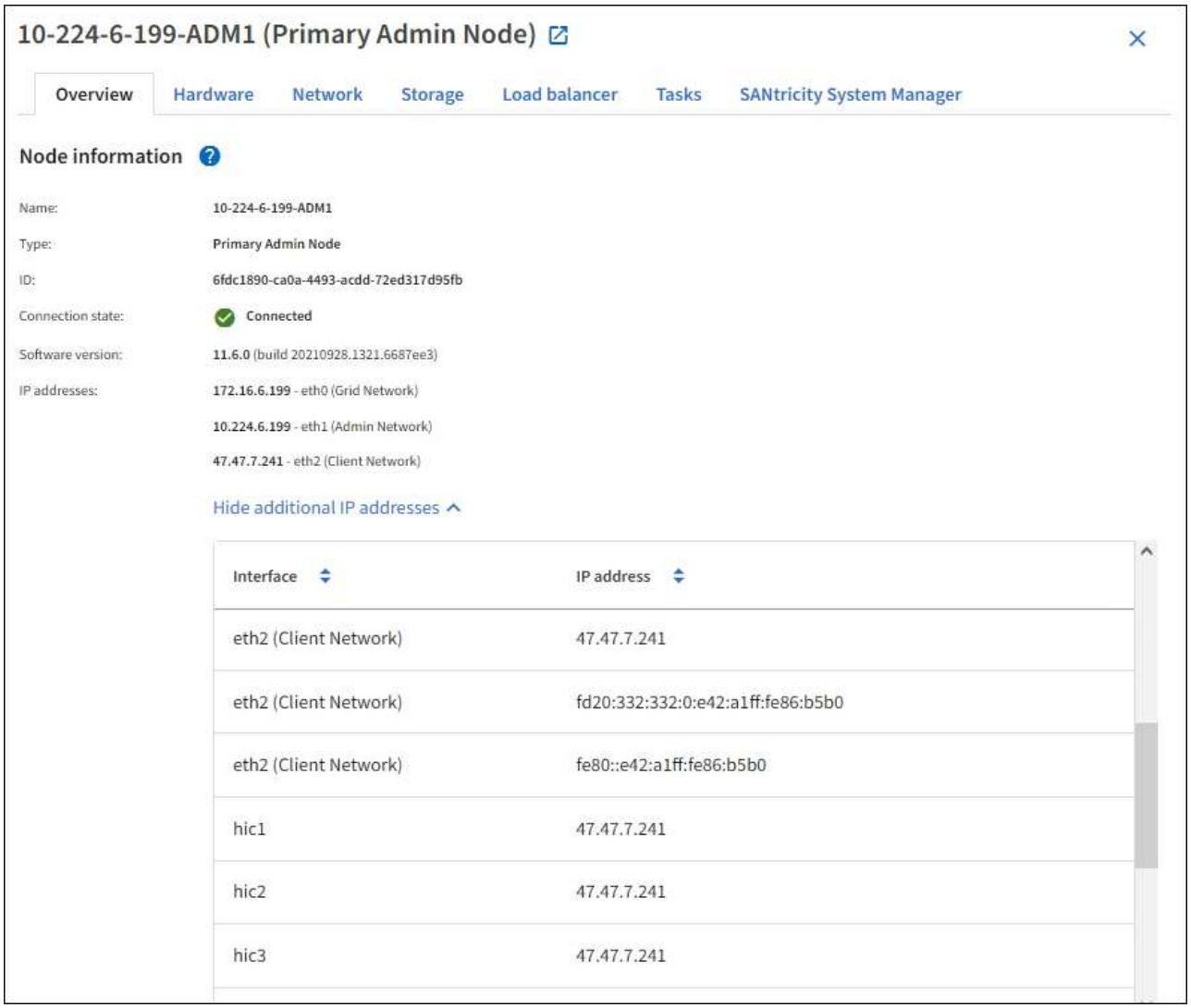
Pasos

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

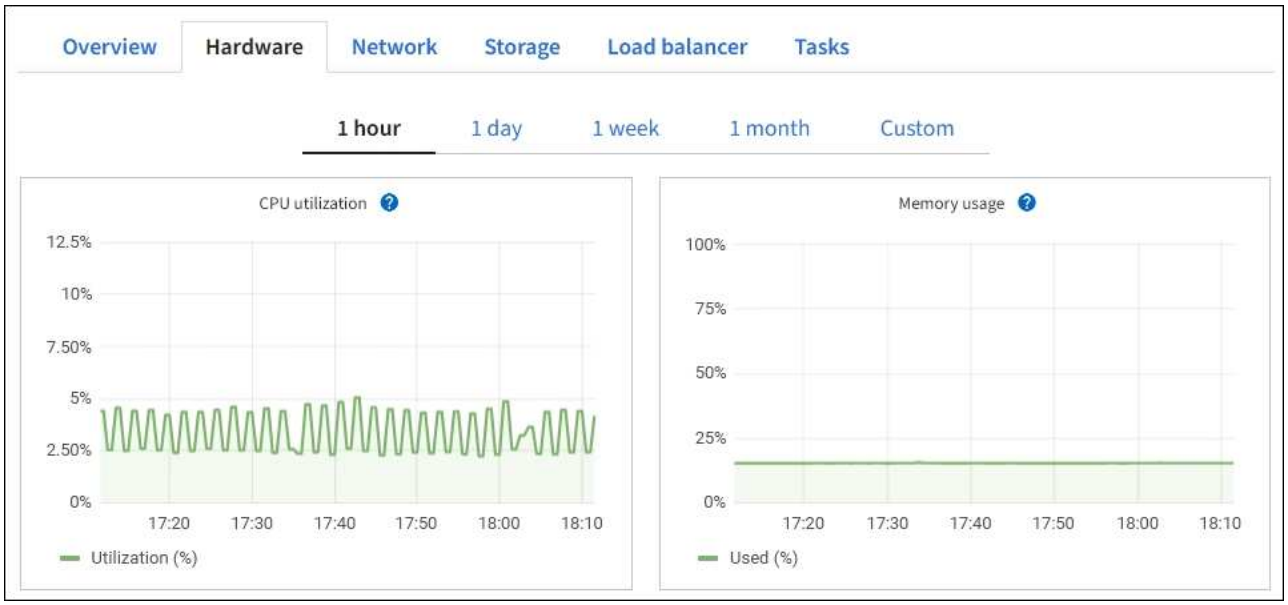
de la interfaz de cada dirección de la siguiente manera:

- **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.

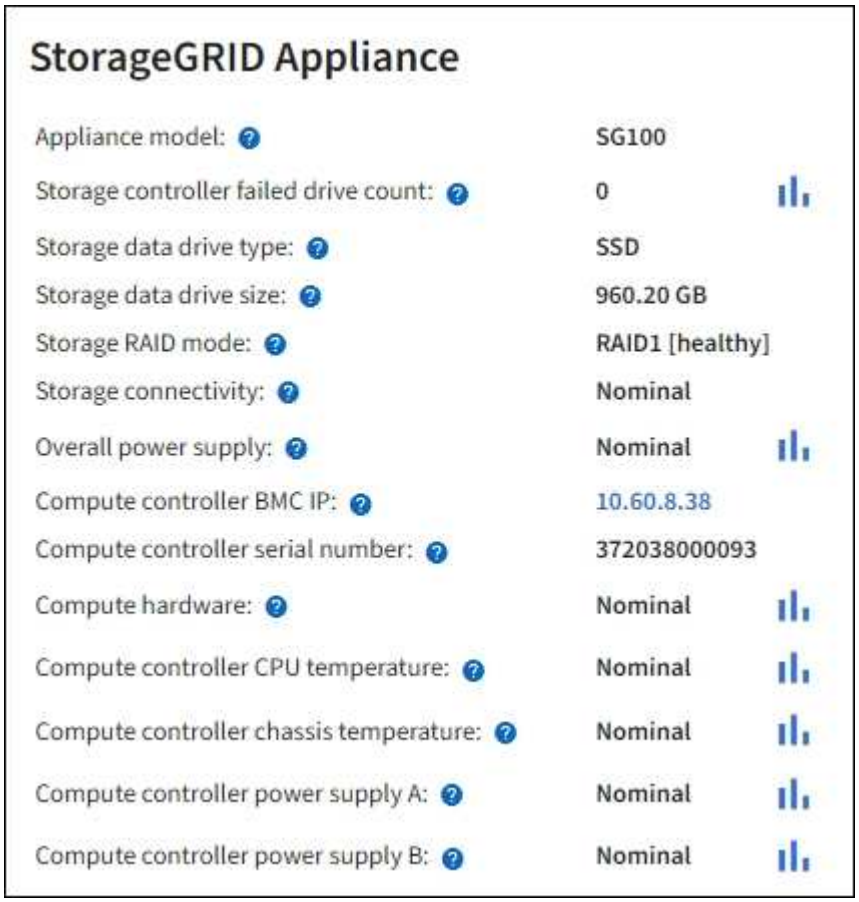


En la sección Alerts de la pestaña Overview se muestran las alertas activas para el nodo.

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



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

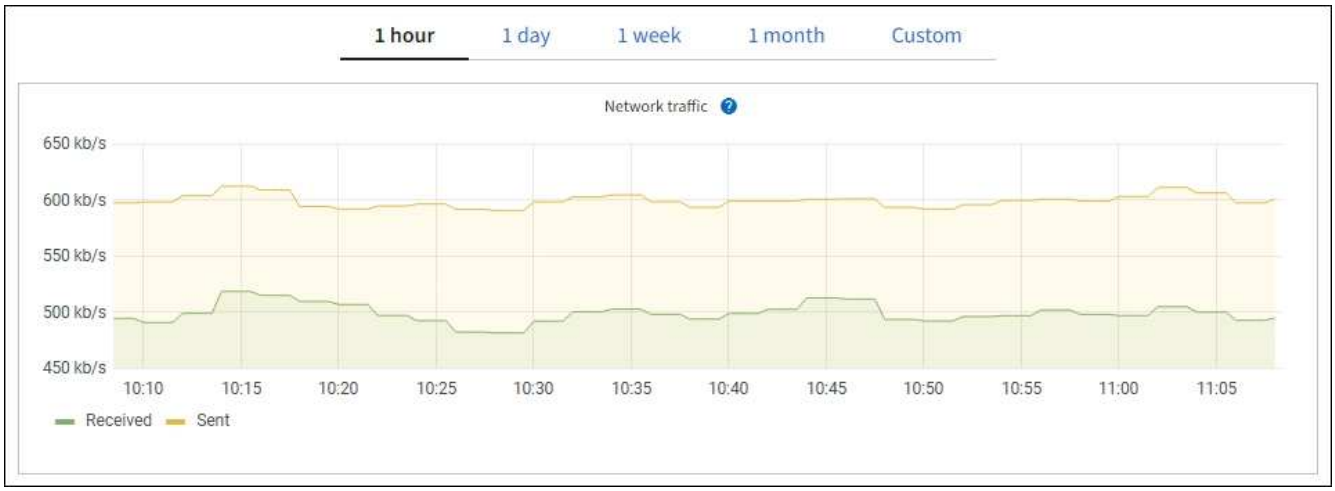
En la tabla dispositivo	Descripción
El número de unidades que la controladora de almacenamiento no pudo completar	La cantidad de unidades que no se encuentran en estado óptimo.
Tipo de unidad de datos de almacenamiento	El tipo de unidades en el dispositivo, como HDD (unidad de disco duro) o SSD (unidad 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	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. Este campo no se muestra para los modelos de dispositivos que no contienen una BMC.
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

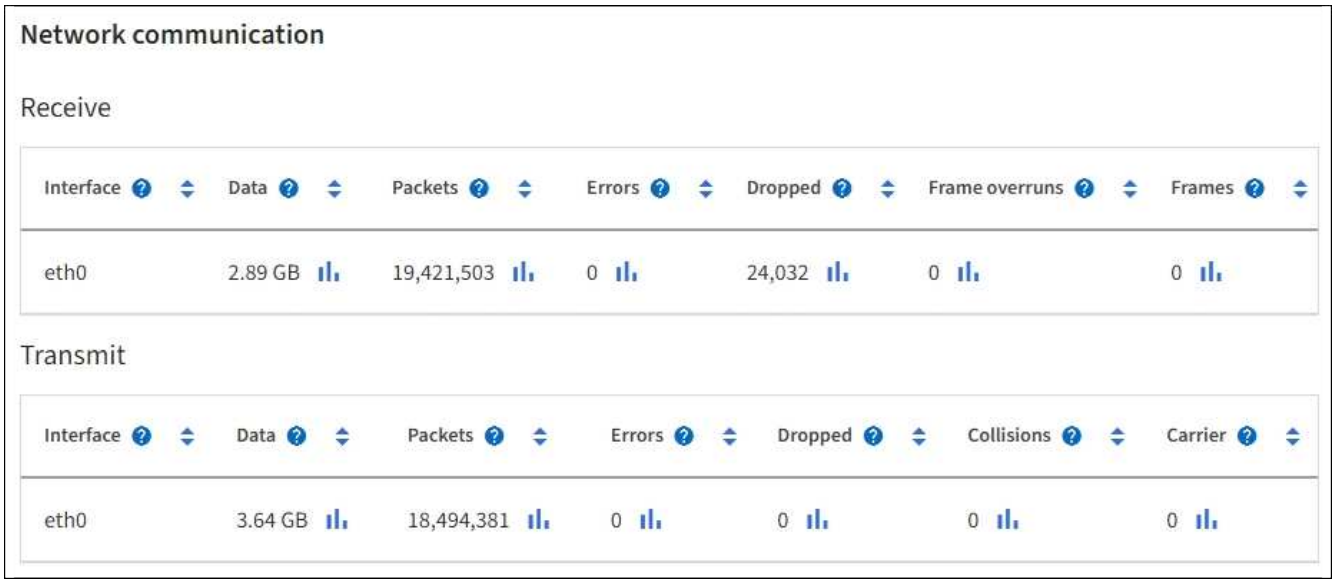
Utilice la siguiente tabla con los valores de la columna **velocidad** de la tabla interfaces de red para determinar si los cuatro puertos de red 40/100-GbE del dispositivo estaban configurados para utilizar el modo activo/backup o el modo LACP.

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

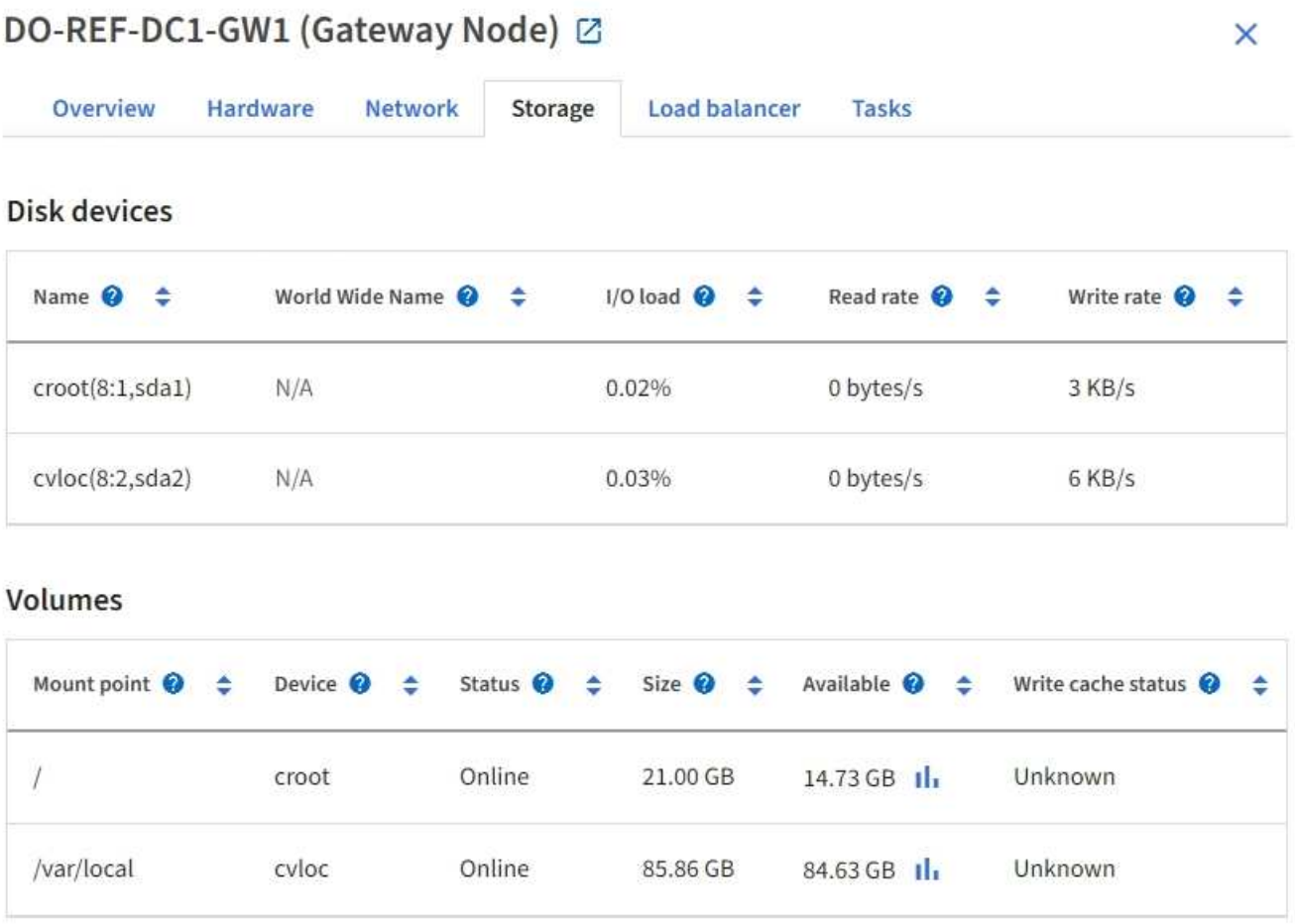
Modo de enlace	Modo de agregación	Velocidad de enlace de HIC individual (hipo 1, hipo 2, hipo 4)	Velocidad esperada de la red Grid/cliente (eth0, eth2)
Agregado	LACP	100	400
Fija	LACP	100	200
Fija	Activa/Backup	100	100
Agregado	LACP	40	160
Fija	LACP	40	80
Fija	Activa/Backup	40	40

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.



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



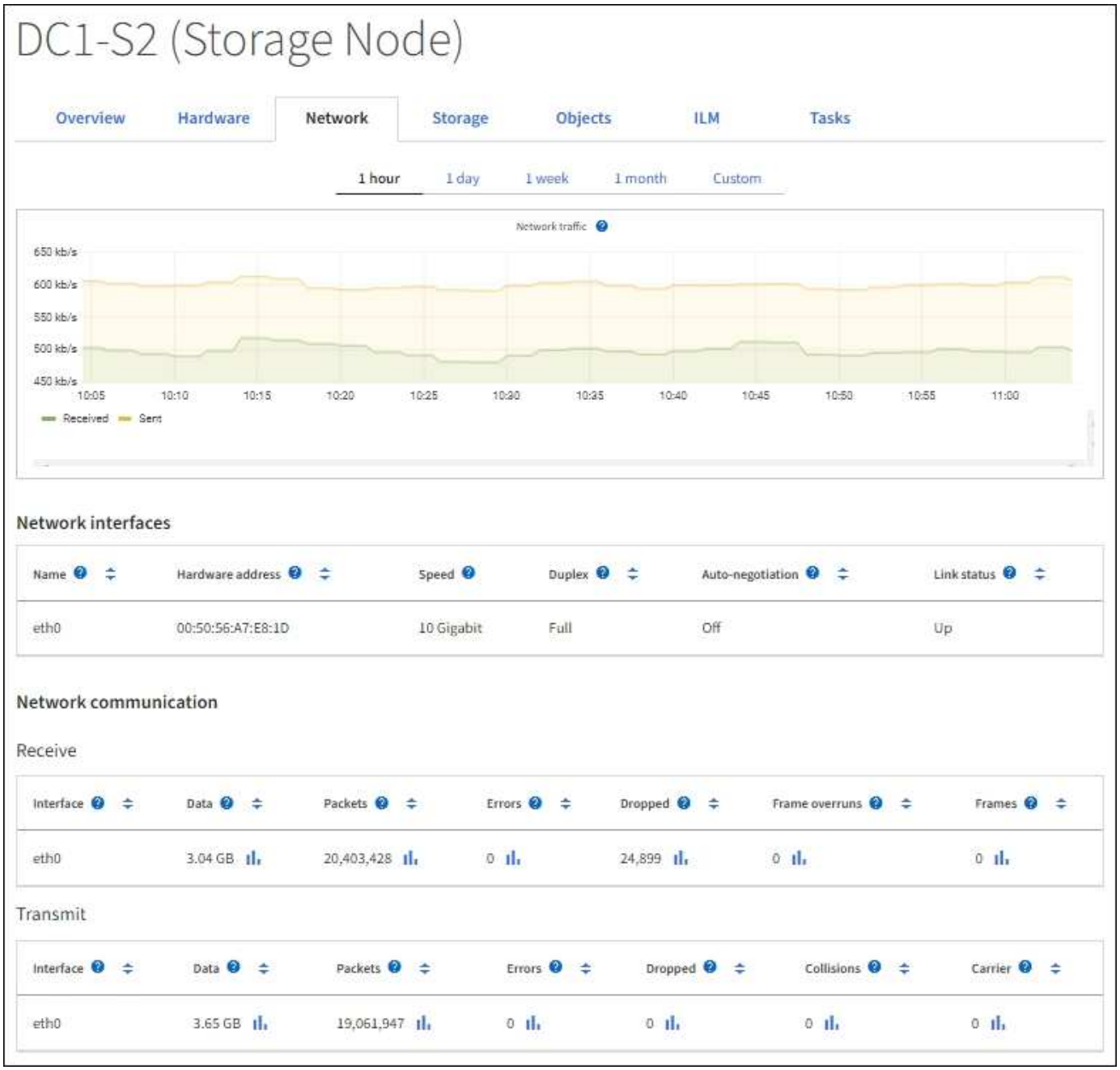
Abra la pestaña Network

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.



Información relacionada

"Supervisar las conexiones de red y el rendimiento"

Consulte la pestaña almacenamiento

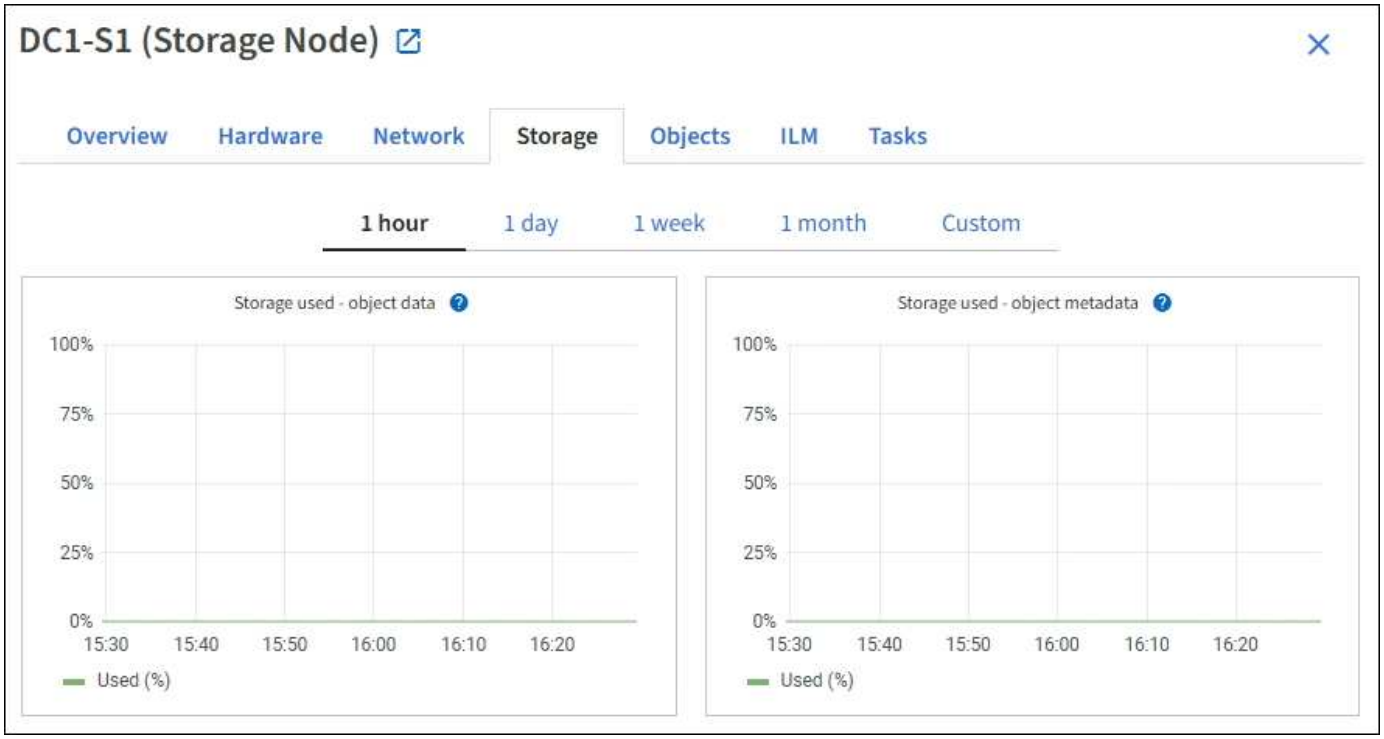
La pestaña almacenamiento resume la disponibilidad del almacenamiento y otras medidas relacionadas con él.

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

Gráficos de uso del almacenamiento

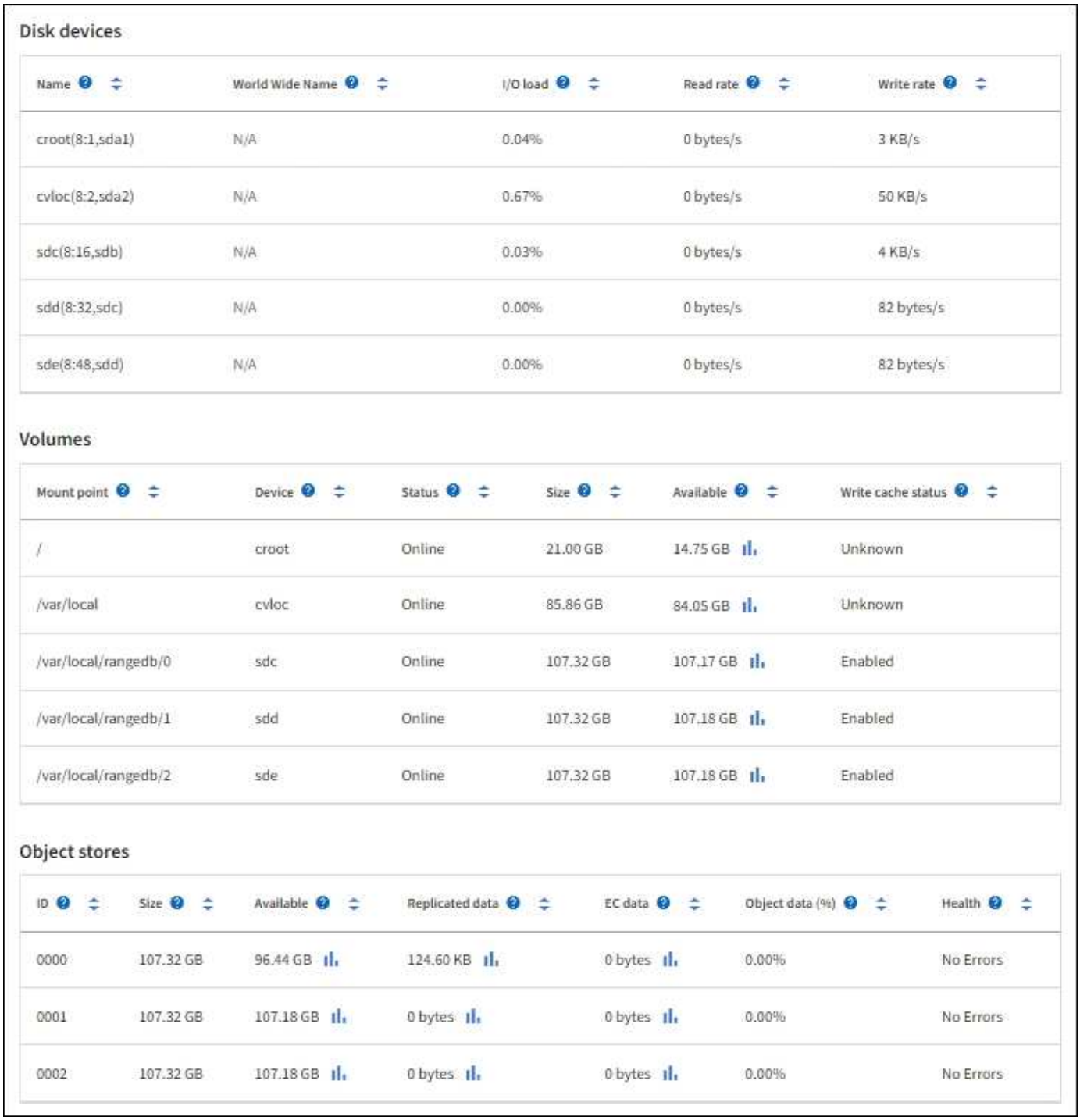
En los nodos de almacenamiento, cada sitio y toda la cuadrícula, la pestaña almacenamiento incluye gráficos que muestran cuánto almacenamiento han utilizado los datos de objetos y los metadatos de objetos a lo largo del tiempo.

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

La ficha objetos proporciona información acerca de "S3" y.. "Swift" las tasas de procesamiento y recuperación.

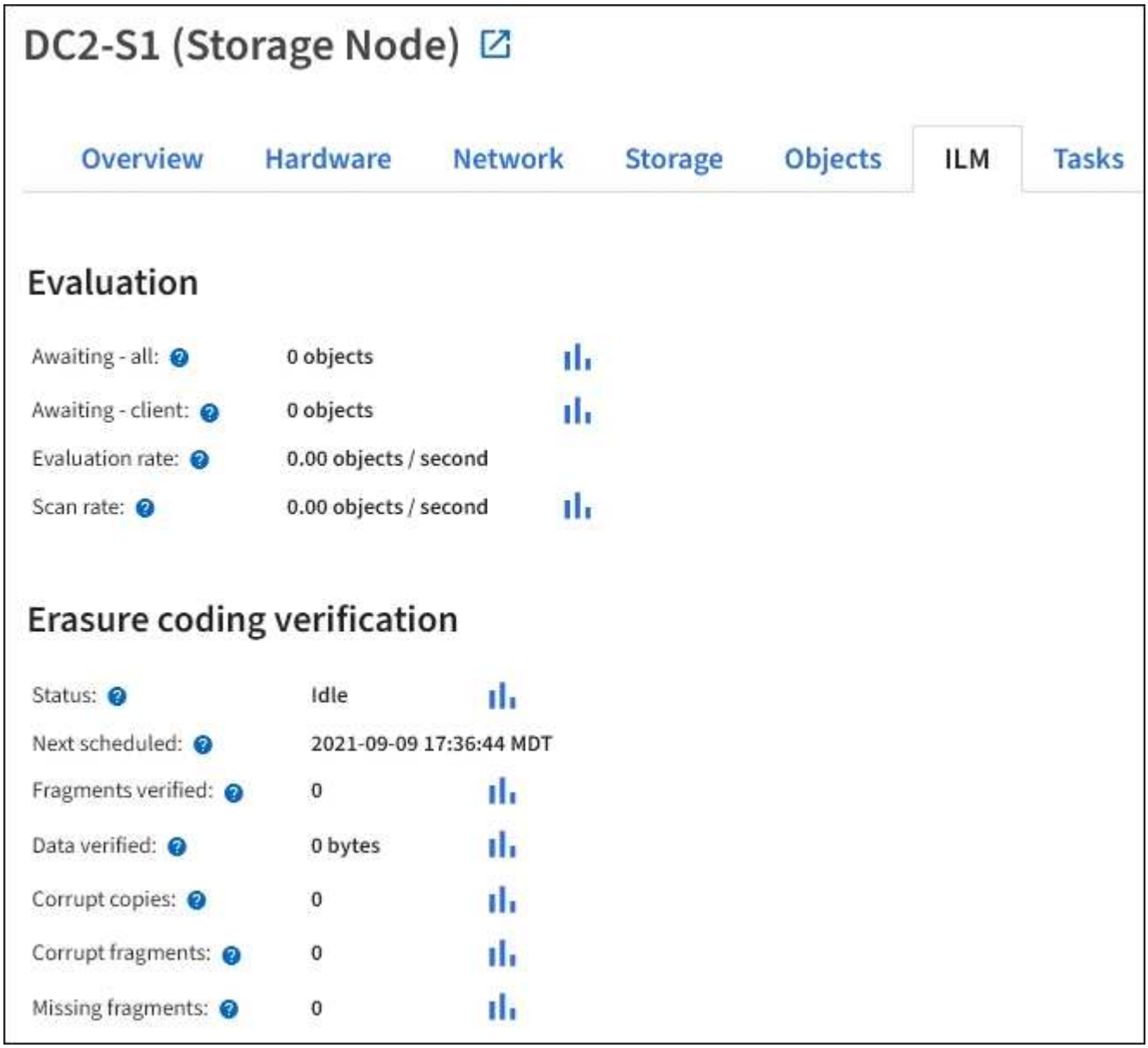
La pestaña Objects se muestra para cada nodo de almacenamiento, cada sitio y toda la cuadrícula. Para los nodos de almacenamiento, la pestaña Objects también proporciona información y recuentos de objetos acerca de consultas de metadatos y verificación en segundo plano.

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.



Información relacionada

"Supervise la gestión del ciclo de vida de la información"

"Administre StorageGRID"

Utilice la pestaña Tareas

La pestaña Tareas se muestra para todos los nodos. Puede usar esta pestaña para cambiar el nombre de un nodo o reiniciarlo, o para poner un nodo de dispositivo en modo de mantenimiento.

Para conocer los requisitos e instrucciones completos para cada opción de esta pestaña, consulte lo siguiente:

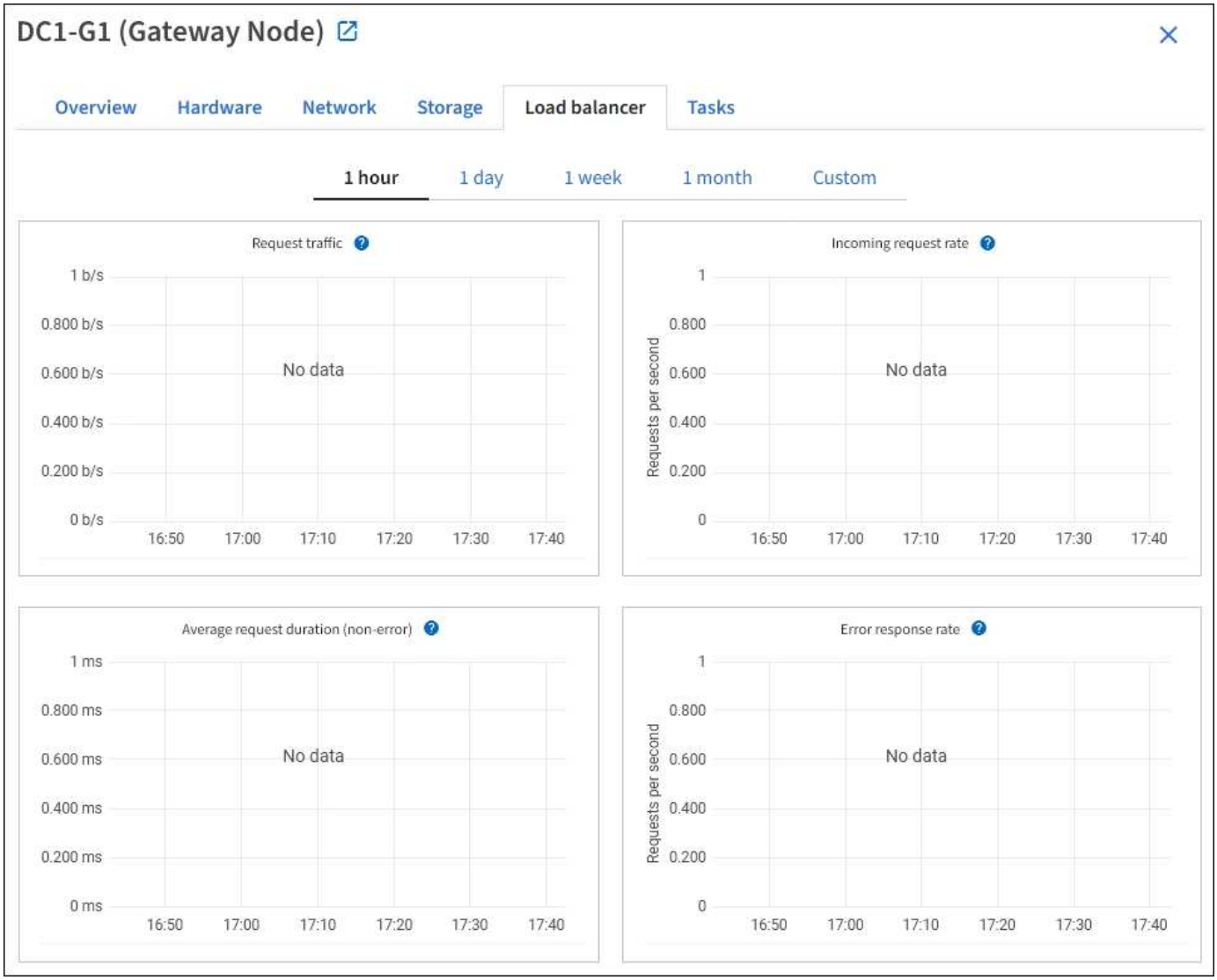
- "Cambie el nombre de cuadrícula, sitios y nodos"
- "Reinicie el nodo de cuadrícula"
- "Coloque el dispositivo en modo de mantenimiento"

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

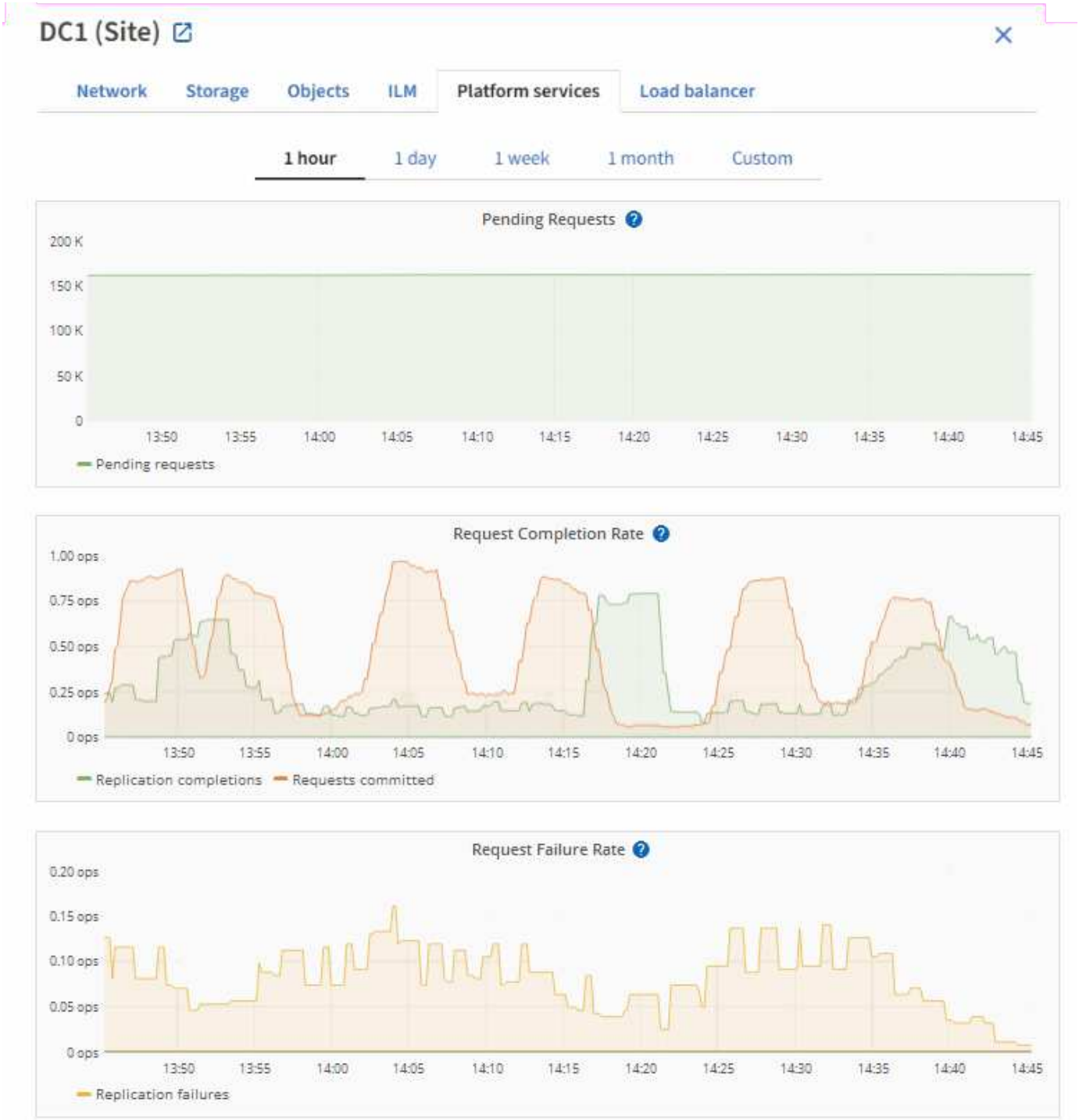
"Supervisar las operaciones de equilibrio de carga"

"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 detalles de la solución de problemas, consulte "Instrucciones para administrar StorageGRID".

Ver la pestaña Gestionar unidades (solo SGF6112)

La pestaña Manage drives permite acceder a los detalles y realizar tareas de solución de problemas y mantenimiento en las unidades del dispositivo SGF6112.

> La pestaña Gestionar unidades solo se muestra para los nodos del dispositivo de almacenamiento SGF6112.

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 tener el "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.

> 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.

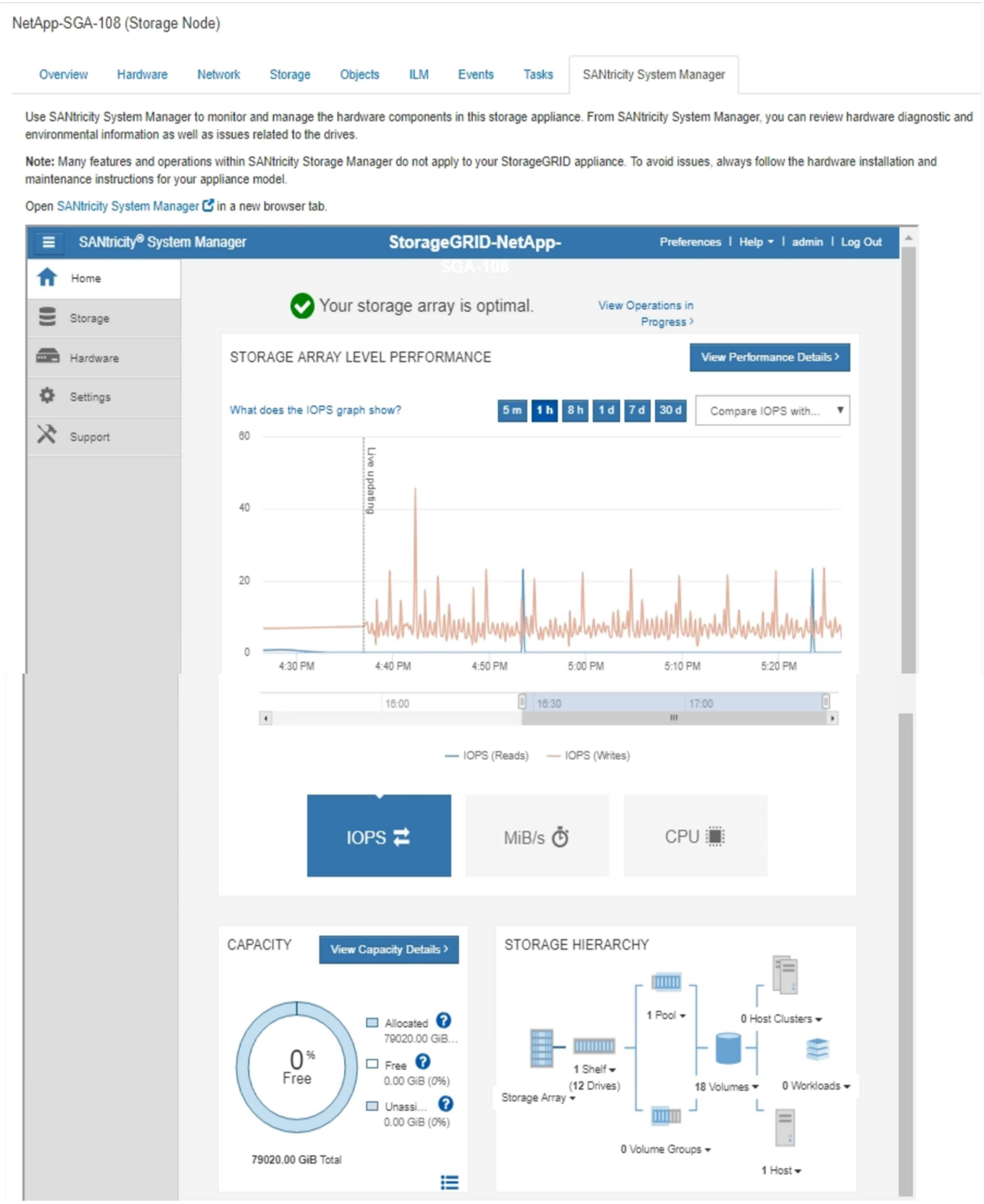
> Para utilizar System Manager de SANtricity a fin de configurar un proxy para E-Series AutoSupport, consulte "Envíe los paquetes AutoSupport de E-Series a través de StorageGRID".

Para acceder a SANtricity System Manager mediante Grid Manager, debe contar con el "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.

> 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.

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



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 cómo ver la información accesible en la pestaña System Manager 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 un "navegador web compatible".
- Ya 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"	Todos los días
Velocidad a la 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
"Operaciones del cliente S3 y Swift"	Semanal
"Operaciones de equilibrio de carga"	Tras la configuración inicial y tras cualquier cambio en la configuración
"Conexiones de federación de grid"	Semanal
"Capacidad del sistema de almacenamiento de archivos externo"	Semanal

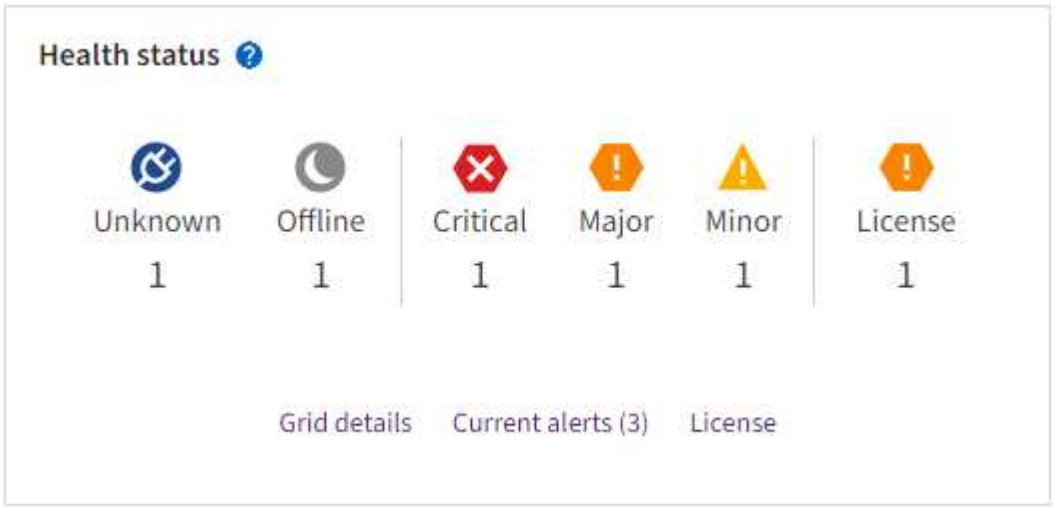
Supervise el estado del sistema

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 posibles problemas indicados por alertas o alarmas (sistema heredado) no son necesariamente problemas con las operaciones del sistema. Investigue los problemas resumidos en la tarjeta de estado del panel de Grid Manager.

Puede recibir notificaciones de alertas en cuanto se activen "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 hacerlo "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 cuadrícula, 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
	No conectado - Desconocido 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. La alerta **no se puede comunicar con el nodo** también puede activarse. Otras alertas también pueden estar activas.	Requiere atención inmediata. Seleccione cada alerta y siga las acciones recomendadas. Por ejemplo, es posible que deba reiniciar un servicio que haya detenido o reiniciar el host del nodo. **Nota**: Un nodo puede aparecer como Desconocido durante las operaciones de cierre administradas. Puede ignorar el estado Desconocido en estos casos.
	No conectado - administrativamente abajo Por un motivo esperado, el nodo no está conectado a la cuadrícula. 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. En función del problema subyacente, estos nodos suelen volver a estar en línea sin ninguna intervención.	Determine si alguna alerta afecta a este nodo. Si una o más alertas están activas, seleccione cada alerta y siga las acciones recomendadas.
	Conectado El nodo está conectado a la cuadrícula.	No se requiere ninguna acción.

Ver las alertas actuales y resueltas

Alertas actuales: Cuando se activa una alerta, se muestra un icono de alerta en el panel de control. También se muestra un icono de alerta para el nodo en la página Nodes. Si "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, ha visto el vídeo: "Vídeo: Información general de alertas de StorageGRID 11,8"

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	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. **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.
Tiempo activado	**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 (*Newest*) y la instancia más antigua de la alerta (*oldest*). **Alertas resueltas**: Hace cuánto tiempo se activó la alerta.
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 *valores de datos*	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. **Nota:** Si se agrupan varias alertas actuales, los valores actuales no se muestran en la fila de título.
Valores disparados (solo alertas resueltas)	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.

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 ampliar los grupos de alertas, seleccione el signo de intercalación hacia abajo . Para reducir las alertas individuales de un grupo, seleccione el signo de intercalación hacia arriba , 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 la "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 la "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.

Puede hacerlo "ver información sobre la capacidad de almacenamiento" Para todo el grid, para cada sitio y para cada nodo de almacenamiento de su 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.

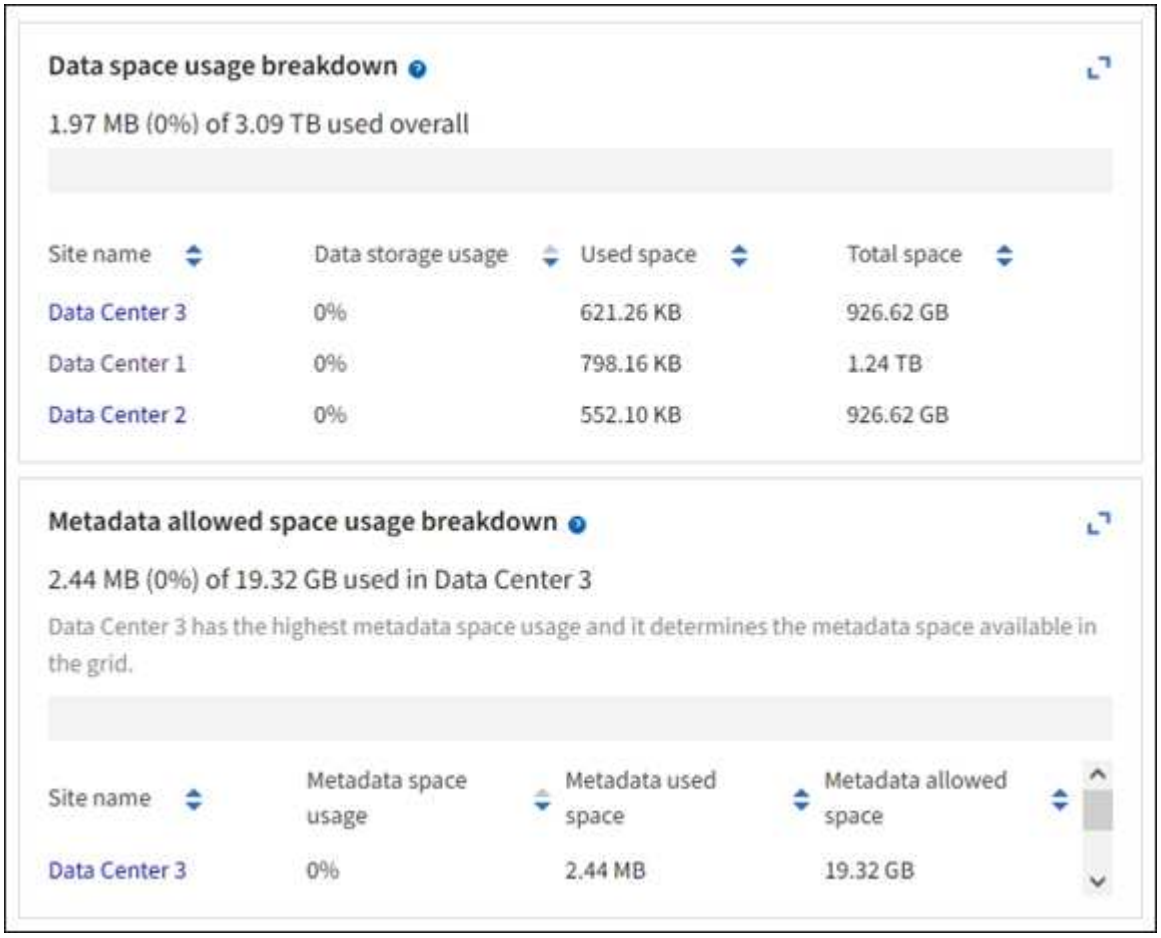
Pasos

1. Evaluar cuánto almacenamiento hay disponible para todo el grid y para cada centro de datos.

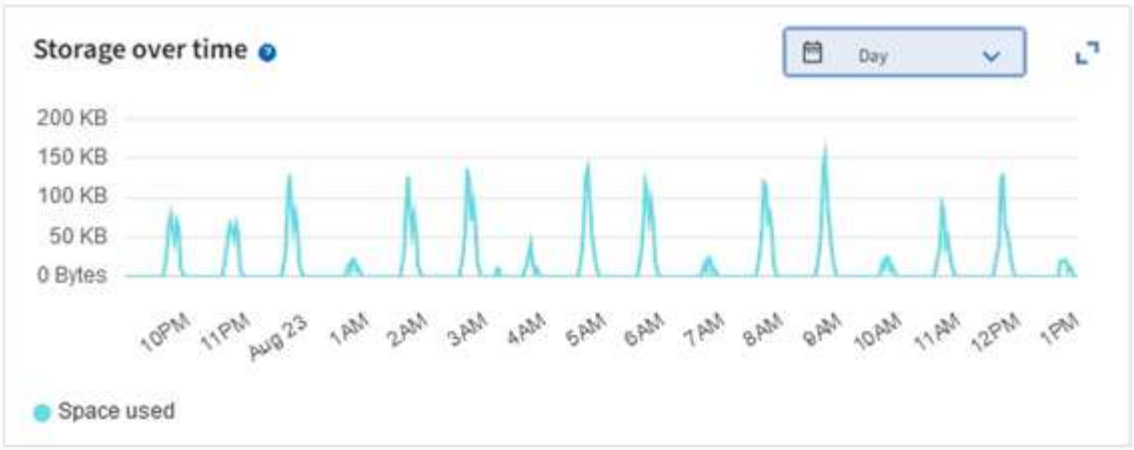
   a. Selecciona **Panel > Descripción general**.

   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.



   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. Selecciona **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.

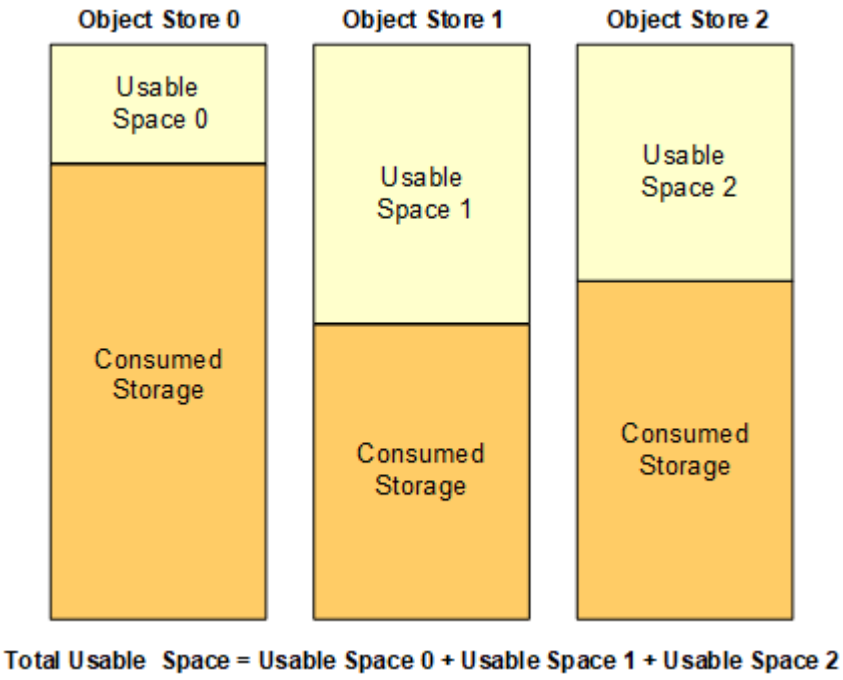
Para obtener más información sobre la planificación de una ampliación de almacenamiento, consulte "Instrucciones para ampliar StorageGRID".

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.



Pasos

1. Seleccione **NODES** > ***Storage Node*** > **Storage**.

   Aparecen los gráficos y las tablas del nodo.

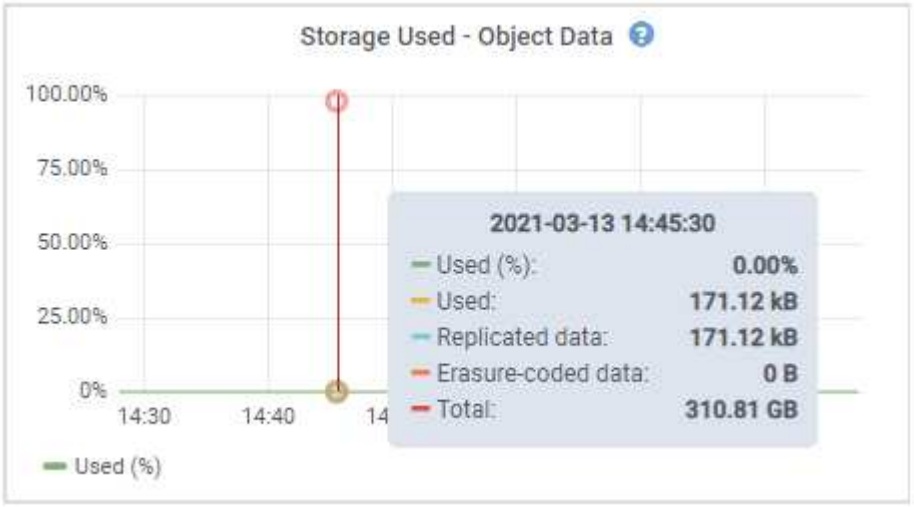
2. Coloque el cursor sobre el gráfico de datos de objetos Storage Used.

   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

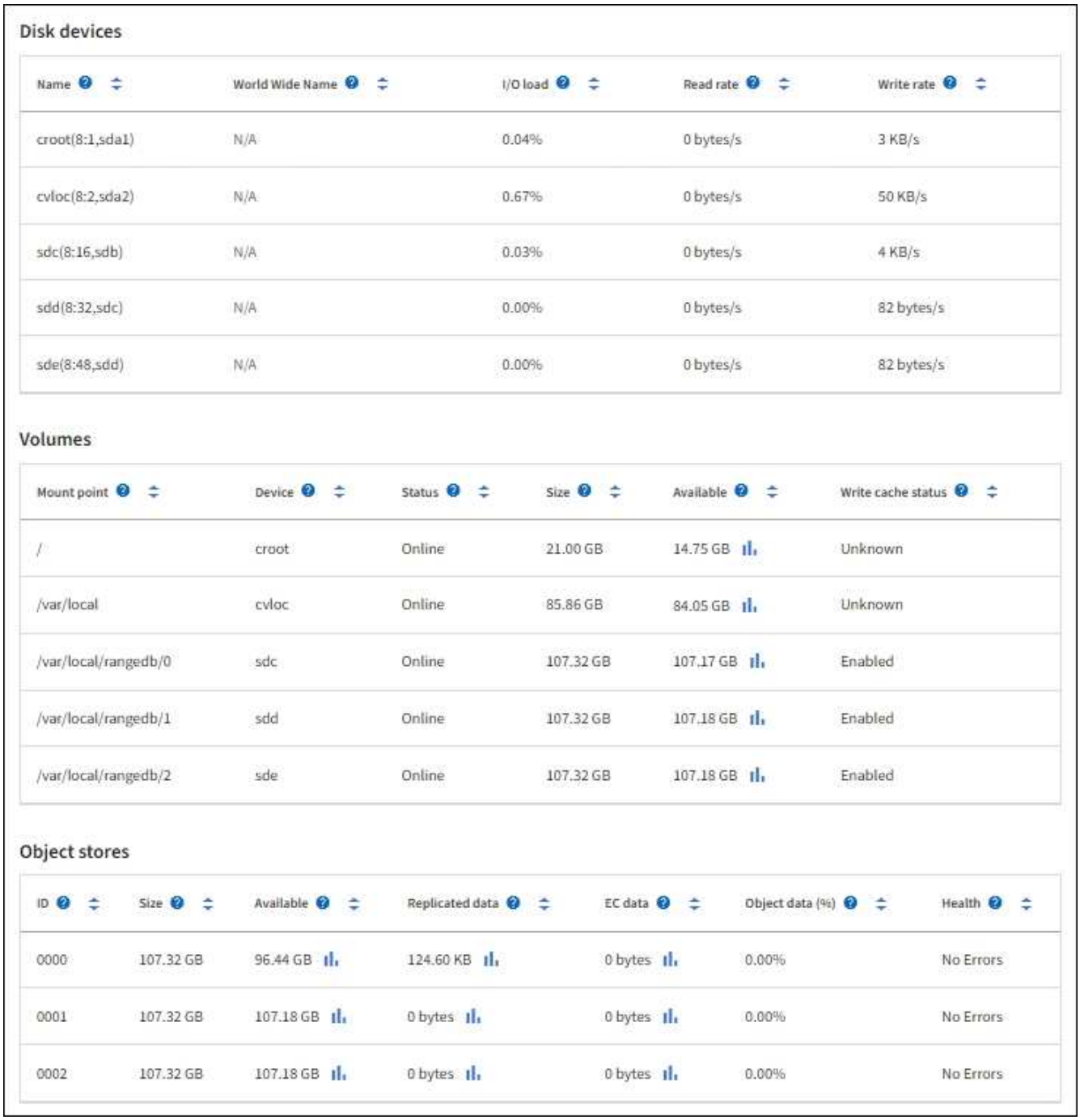
borrado en este nodo, sitio o cuadrícula.

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



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

4. Supervise los valores a lo largo del tiempo para estimar la tasa a la que se está consumiendo el espacio de almacenamiento útil.
5. 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 ampliación de almacenamiento, consulte

"Instrucciones para ampliar StorageGRID".

La "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

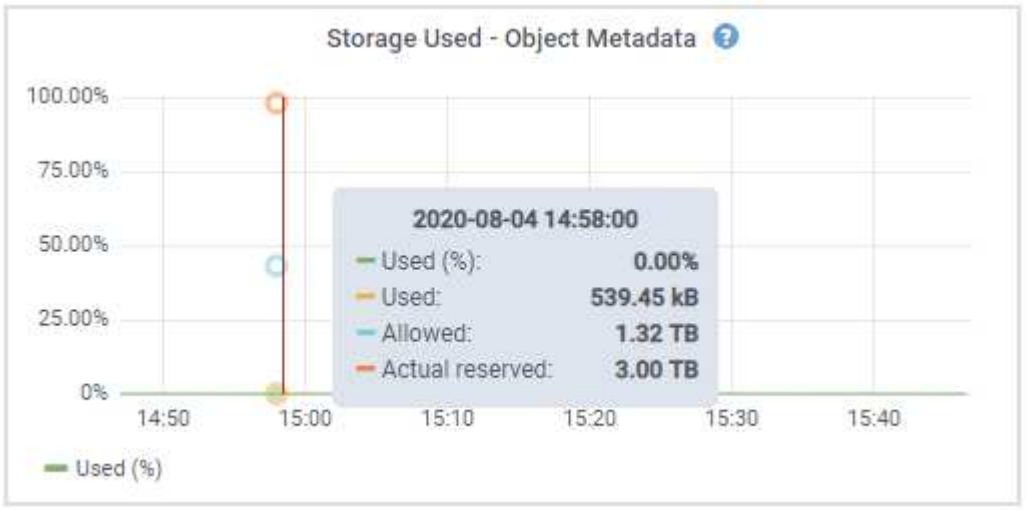
StorageGRID mantiene tres copias de metadatos de objetos en cada sitio para proporcionar redundancia y proteger los metadatos de objetos de la pérdida. Las tres copias se distribuyen uniformemente por todos los nodos de almacenamiento de cada sitio, utilizando el espacio reservado para los metadatos 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 **NODES** > ***Storage Node*** > **Storage**.
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 saber cómo determina este valor para cada nodo de almacenamiento, consulte "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 saber cómo se calcula este valor para cada nodo de almacenamiento, consulte "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.

3. 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 "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 lo necesitará "expanda una cuadrícula".

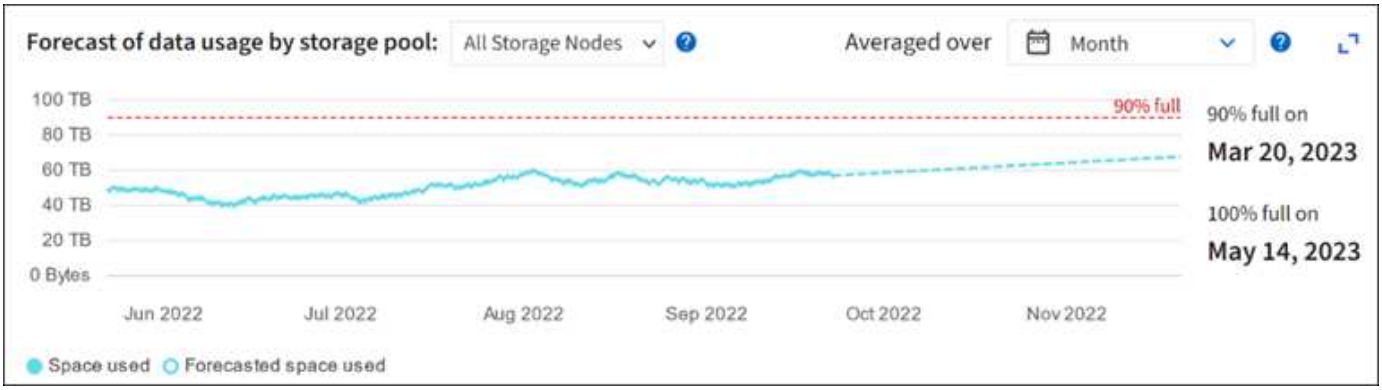
Si observa que la tasa de consumo cambia con el tiempo, seleccione un intervalo más corto del menú desplegable **Promediado sobre** para reflejar solo los patrones de ingesta más recientes. Si observa patrones estacionales, seleccione un rango más largo.

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

1. En el panel de control, seleccione **Almacenamiento**.
2. Vea las tarjetas de consolas, Previsión de uso de datos por pool de almacenamiento y Previsión de uso de metadatos por sitio.
3. 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 ingesta 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 pueden 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.

Use la página NODES

Pasos

Además, investigue las colas de ILM usando la página **NODES**:

> Los gráficos de la página **NODES** se reemplazarán con las tarjetas correspondientes del tablero de mando en una futura versión de StorageGRID.

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

   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.

   - **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 de objeto puede volver a incrementarse si la replicación ha fallado después de la reparación.

   Estos atributos pueden ser útiles cuando se supervisa el progreso de la recuperación de volumen del nodo de almacenamiento. Si el número de reparaciones que se intentaron ha dejado de aumentar y se ha completado una exploración completa, es probable que la reparación haya finalizado.

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.

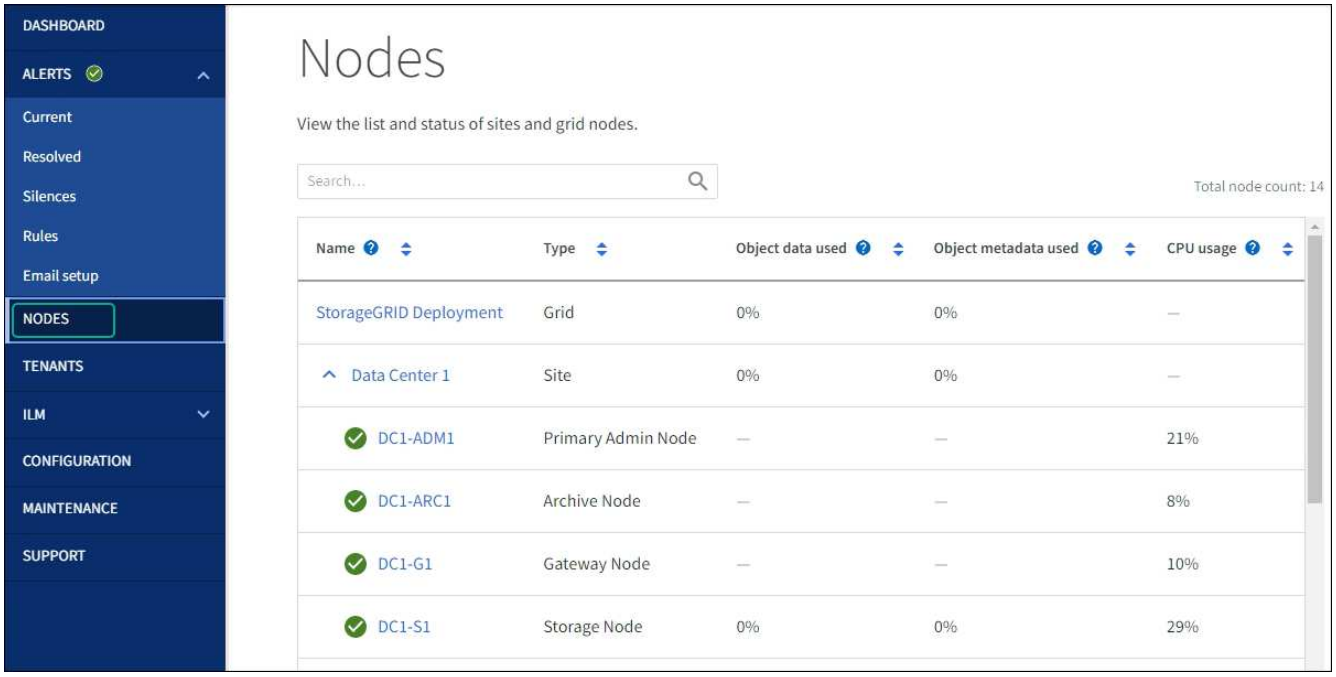
Utilice Grid Manager para supervisar la conectividad y el rendimiento de la red, de modo que pueda resolver cualquier problema con prontitud.

Además, considere "creación de políticas de clasificación del tráfico de red" de modo que pueda 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

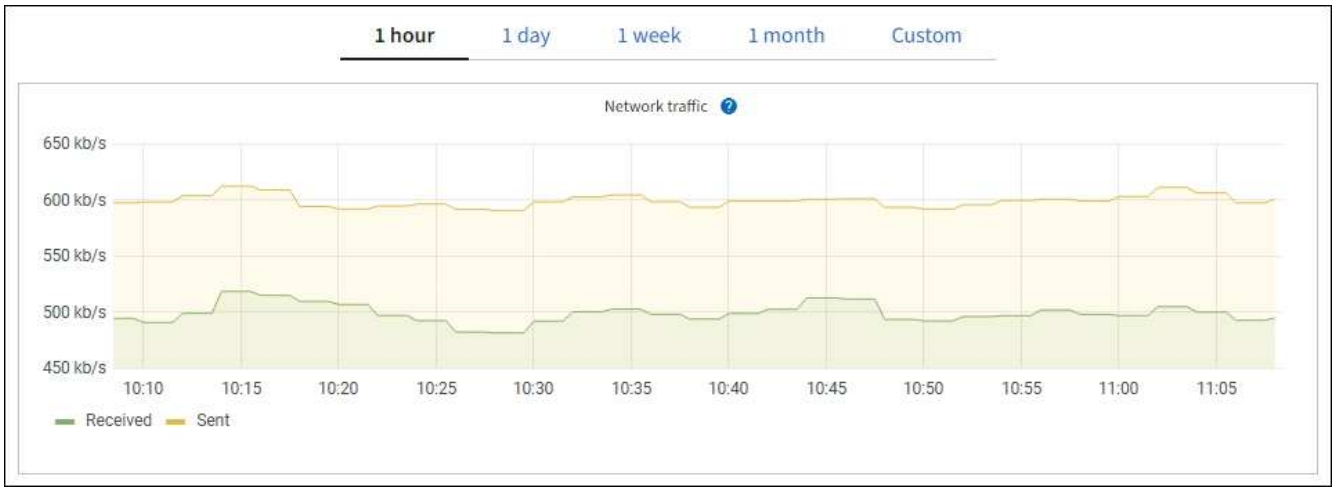
1. Selecciona **NODOS**.

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



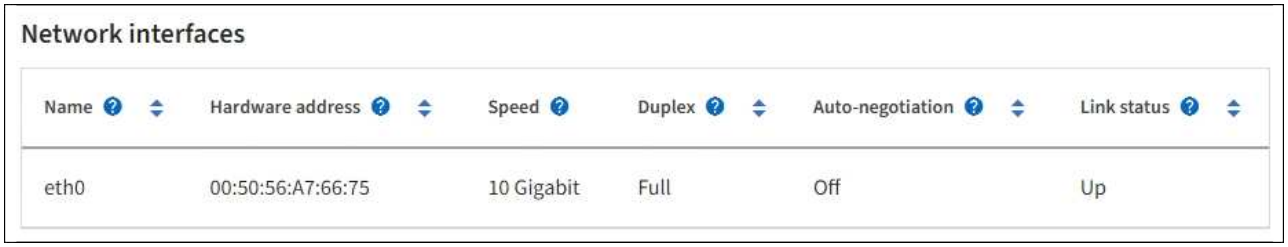
2. Seleccione el nombre de la cuadrícula, un sitio específico del centro de datos o un nodo de la cuadrícula y, a continuación, seleccione la ficha **Red**.

   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.



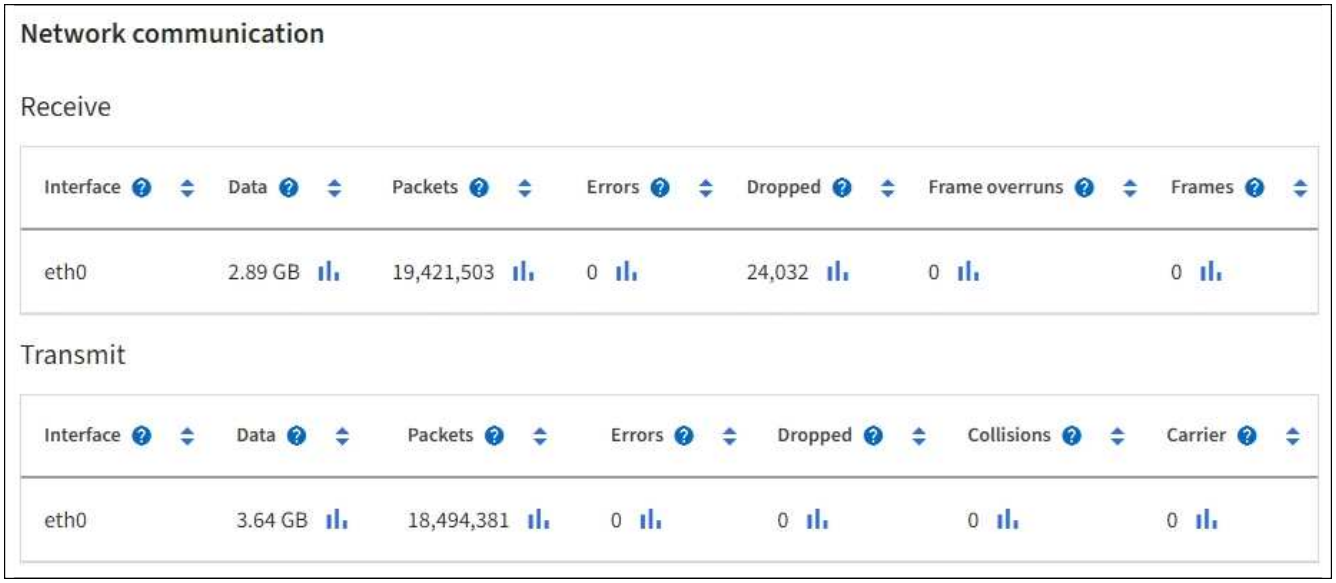
   a. Si ha seleccionado un nodo de cuadrícula, desplácese hacia abajo para revisar la sección **interfaces**

de red de la página.



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

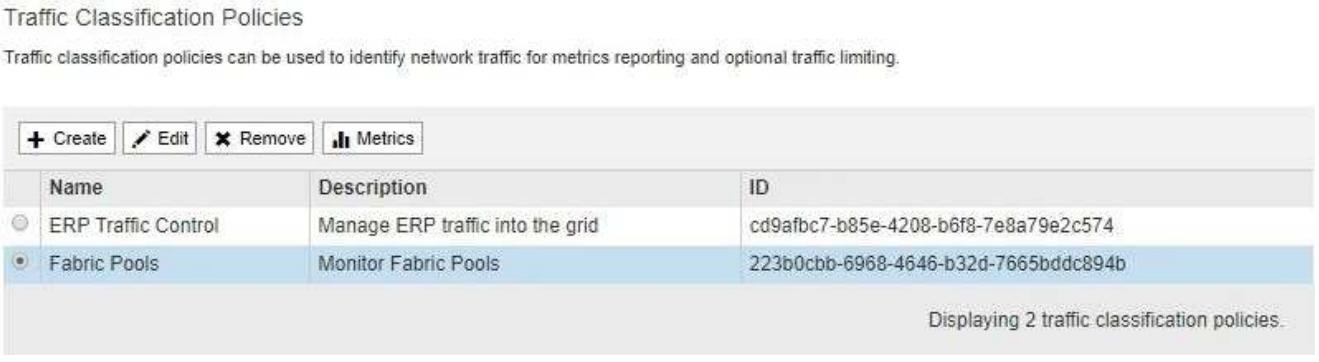
   Las tablas de recepción y transmisión muestran cuántos bytes y paquetes se han recibido y enviado a través de cada red, así como otras métricas de recepción y transmisión.



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.



   a. 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**.

   b. 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"

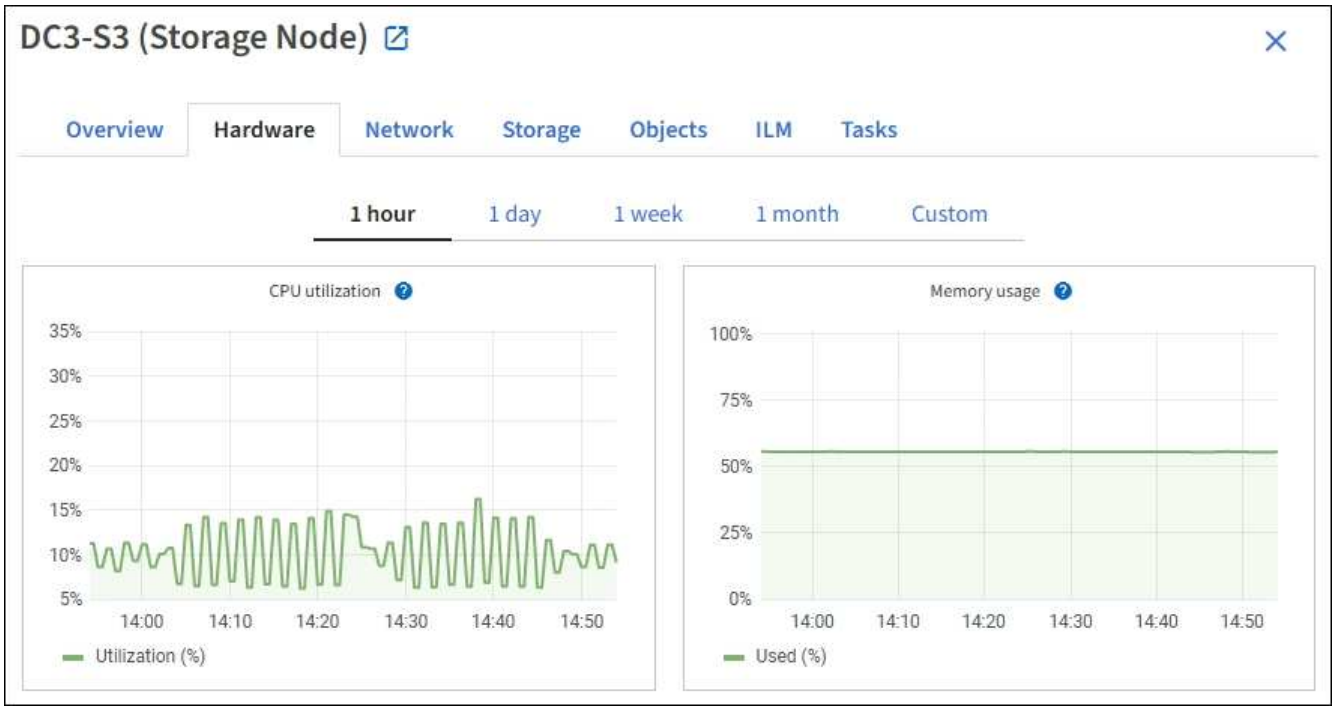
"Supervise los estados de conexión de los nodos"

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

1. En la página **NODES**, seleccione el nodo.
2. 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 S3 y Swift está asociada 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 un "navegador web compatible".
- Usted tiene la "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 **ARRENDATARIOS**.
2. Revise la información que se muestra en las páginas de arrendatario.

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

   > Los valores de espacio utilizado son estimados. Estas estimaciones se ven afectadas por el tiempo de los ingests, la conectividad de red y el estado del nodo.

3. Opcionalmente, inicie sesión en una cuenta de inquilino seleccionando el enlace de inicio de sesión En la columna **Iniciar sesión/Copiar URL**.
4. Si lo desea, copie la URL de la página de inicio de sesión de un inquilino seleccionando el enlace de copia URL En la columna **Iniciar sesión/Copiar URL**.

5. Opcionalmente, seleccione **Exportar a CSV** para ver y exportar A. `.csv` archivo que contiene los valores de uso para todos los inquilinos.

   Se le solicitará que abra o guarde el `.csv` archivo.

   El contenido del `.csv` el 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	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

   Puede abrir el `.csv` archiva en una aplicación de hoja de cálculo o utilízala en la automatización.

6. 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.

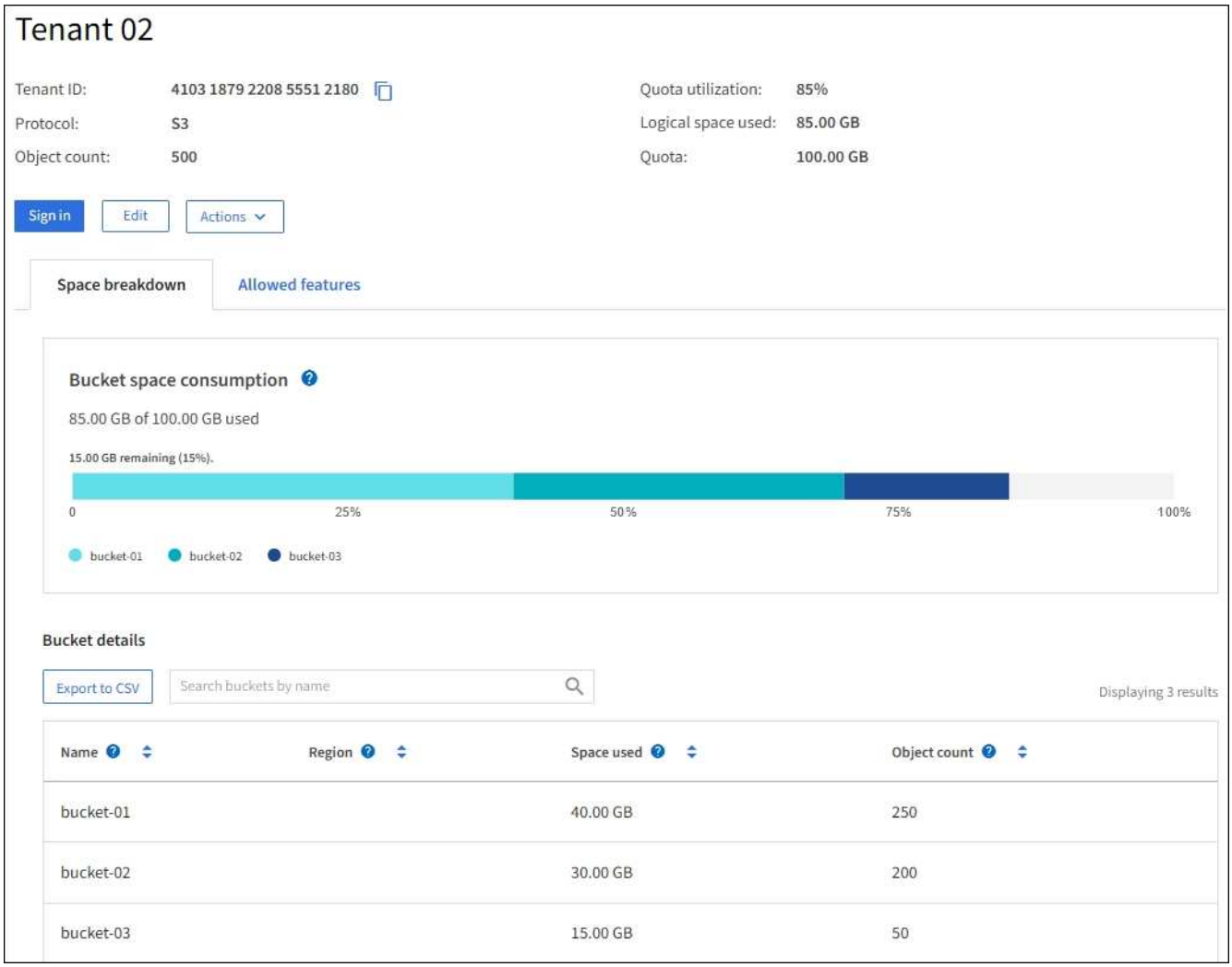
Ver un arrendatario específico

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.



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

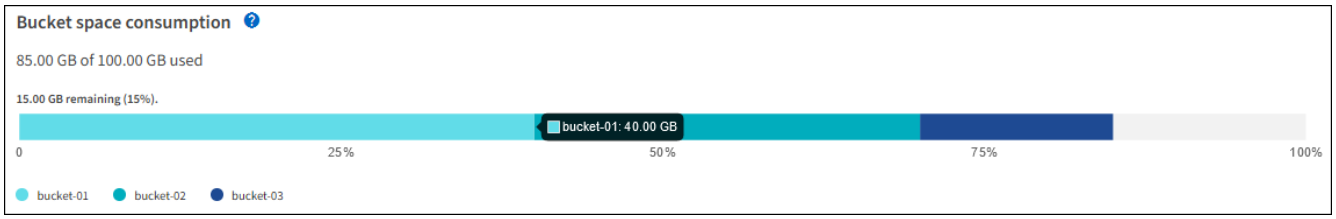
   En esta sección de la página de detalles se proporciona información de resumen para el inquilino, incluido el recuento de objetos del inquilino, el uso de la cuota, el espacio lógico utilizado y la configuración de cuota.

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 TB (o contenedores Swift) 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 incluye sólo 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.



> La utilización de cuotas 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, es posible que se impida temporalmente que un arrendatario cargue nuevos objetos hasta que se vuelva a calcular la utilización de cuota. El cálculo de la utilización de cuotas puede tardar 10 minutos o más.

> La utilización de cuota de un inquilino indica la cantidad total de datos de objeto que el inquilino ha cargado a StorageGRID (tamaño lógico). El uso de cuotas 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 ver 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 (o contenedores Swift) para el inquilino. 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 inquilino S3 individual `.csv` el archivo 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 el `.csv` archiva en una aplicación de hoja de cálculo o utilízala 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. Consulte "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" si quiere 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" si quiere más información.

Utilizar métricas de Prometheus

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

- En Grid Manager, seleccione **SUPPORT** > **Tools** > **Metrics**. Puede usar consolas 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 icono 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" si quiere más información.

Supervise las operaciones del cliente S3 y Swift

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 un "navegador web compatible".

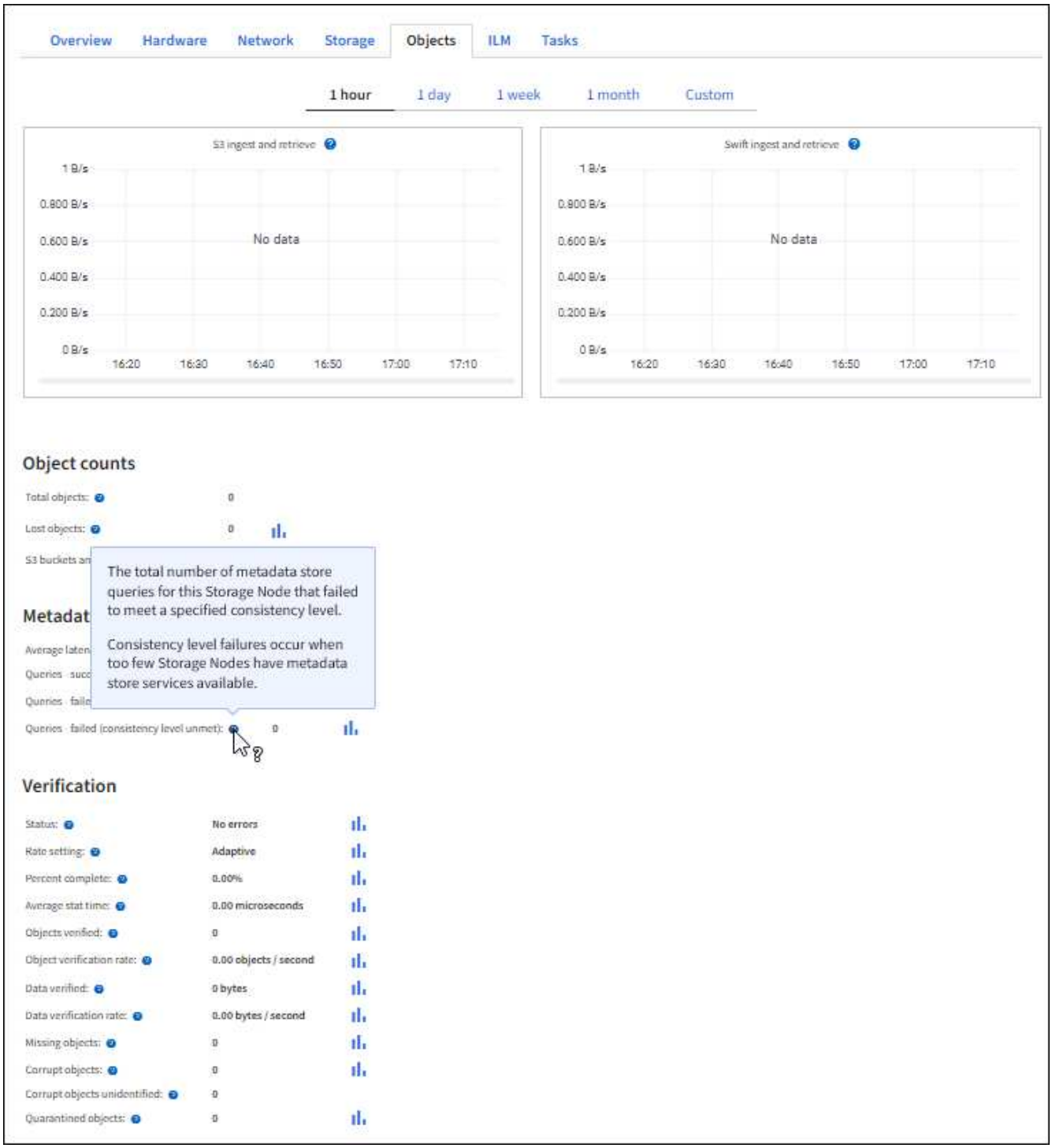
Pasos

1. En el panel de control, seleccione la pestaña **Rendimiento**.
2. Consulte los gráficos S3 y Swift, que resumen la cantidad de operaciones de cliente que realizan los nodos de almacenamiento y la cantidad de solicitudes de API que reciben los nodos de almacenamiento durante el lapso seleccionado.
3. Selecciona **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 y Swift para todo su sistema de 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 ingesta 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 clientes S3 y Swift".

Pasos

1. Si los clientes S3 o Swift se conectan mediante el servicio Load Balancer, compruebe que los nodos de administración o de puerta de enlace distribuyan de forma activa el tráfico según lo previsto:
   a. Selecciona **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 el "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 métricas de Prometheus sobre operaciones de replicación de red cruzada. Puede supervisar una conexión desde cualquier cuadrícula.

Antes de empezar

- Ha iniciado sesión en Grid Manager en cualquiera de las tablas mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz" 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

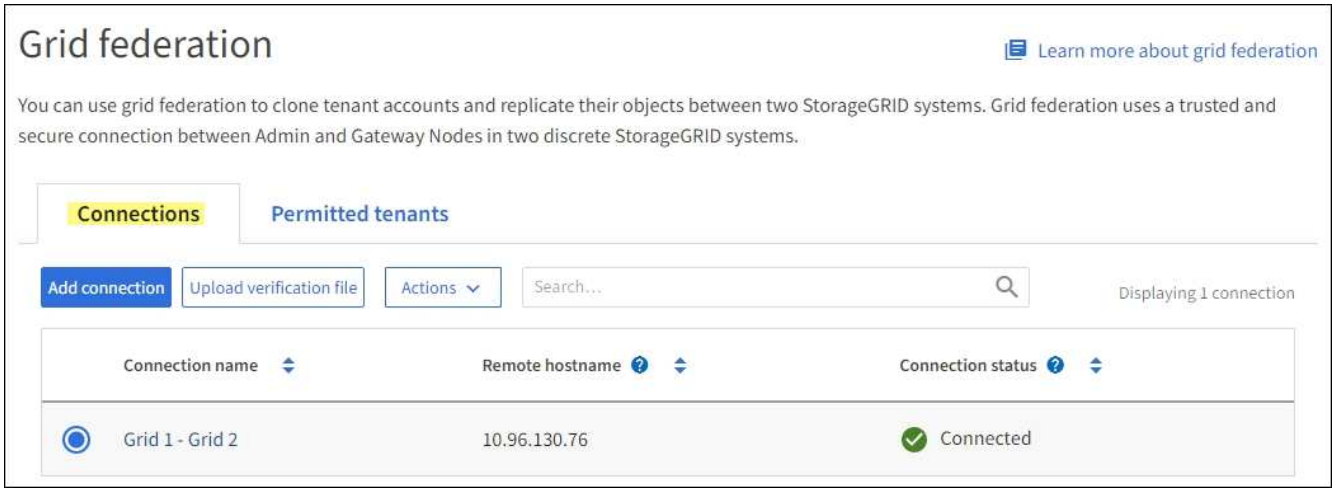
1. Selecciona **CONFIGURACIÓN** > **Sistema** > **federación de cuadrícula**.

   Aparecerá la página Grid federation.

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

   Desde esta pestaña, puede:

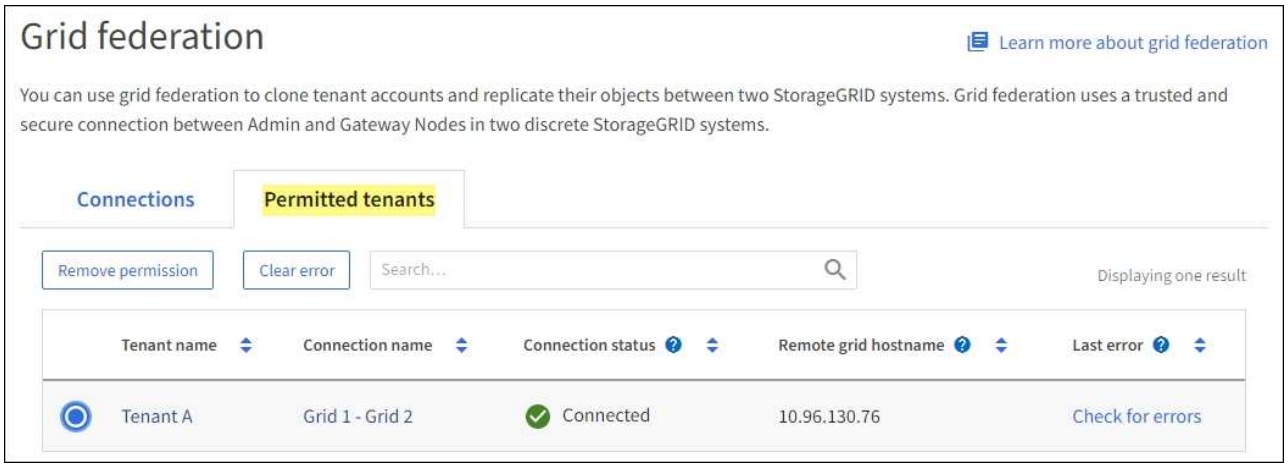
   - "Cree una nueva conexión".
   - Seleccione una conexión existente a. "editar o probar".



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".



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.

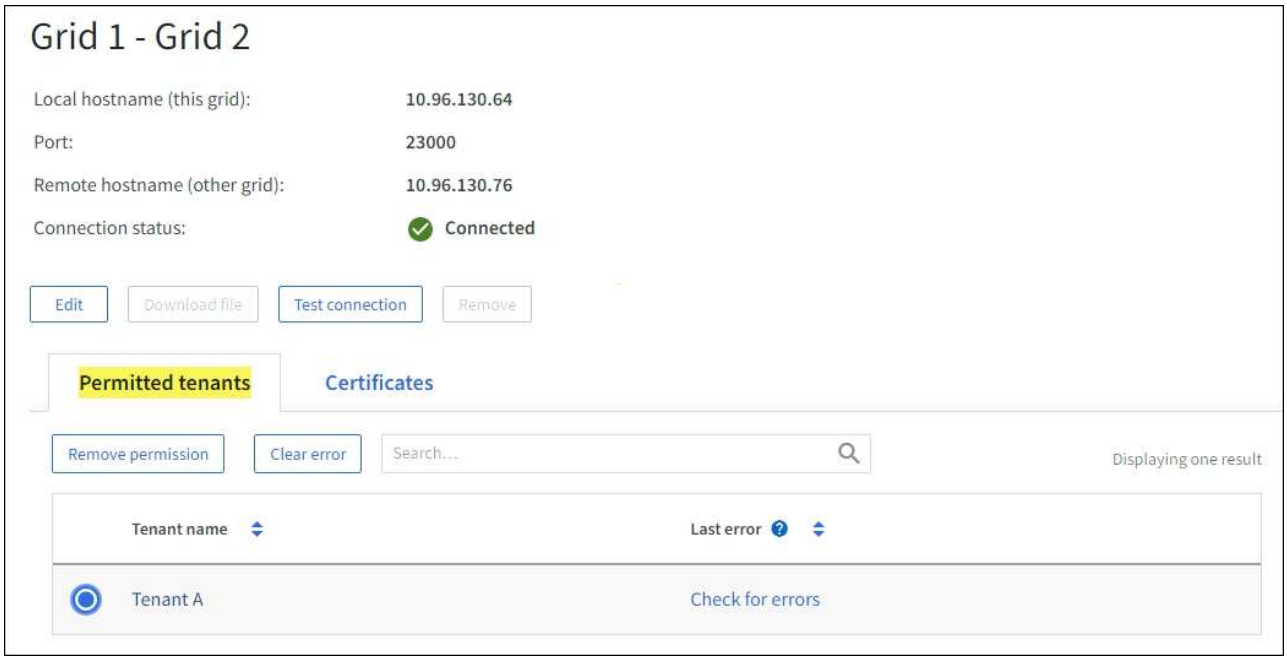
   En la página de detalles de la conexión, puede:

   - 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:

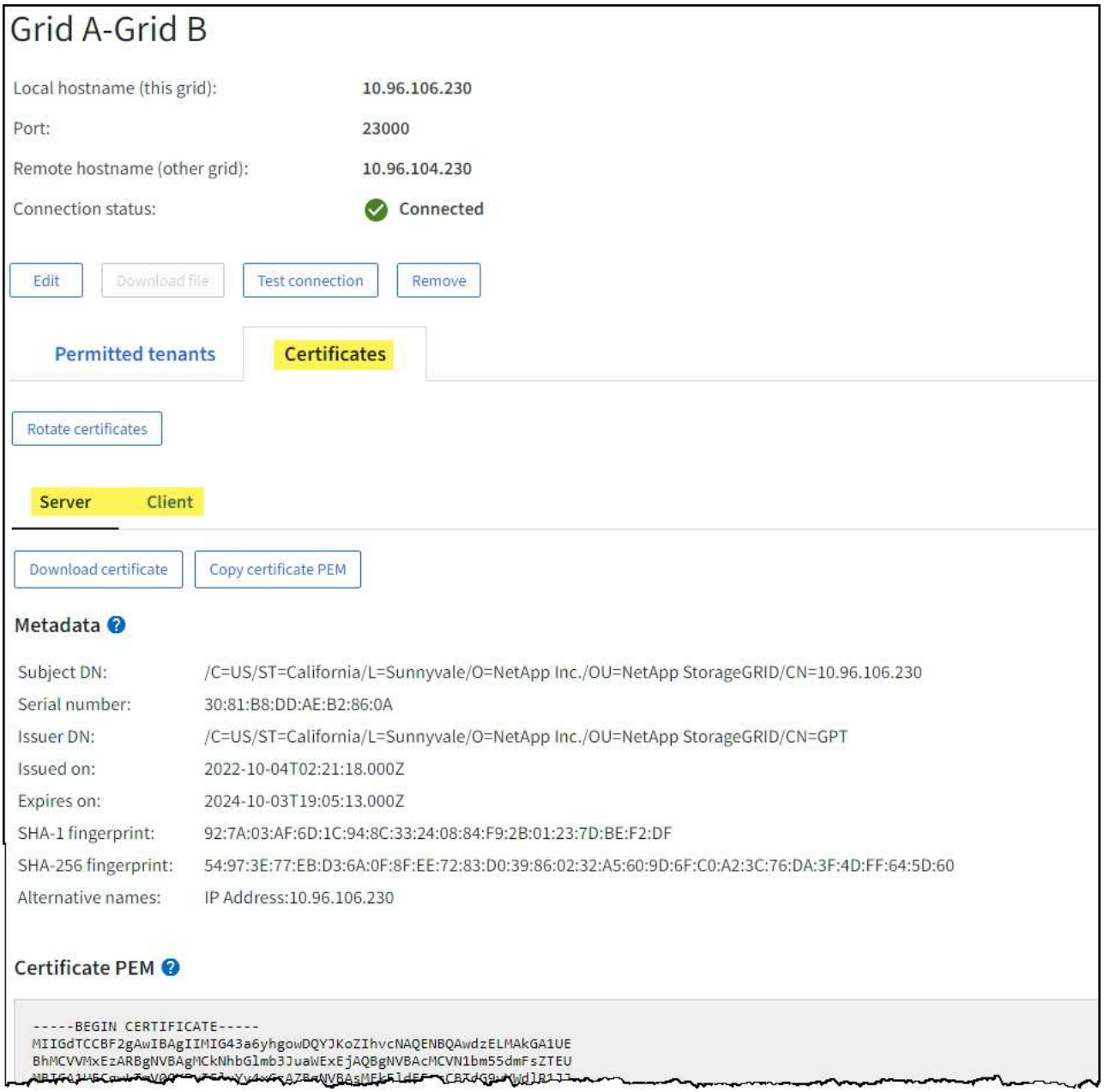
   - "Consulte la página de detalles de cada inquilino permitido".
   - "Eliminar el permiso de un inquilino" para utilizar la conexión.
   - Compruebe si hay errores de replicación entre cuadrículas y borre el último error. Consulte "Solucionar errores de federación de grid".



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.



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. En Grid Manager, selecciona **SUPPORT** > **Tools** > **Metrics**.

   > 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".

Supervise la capacidad de archivado

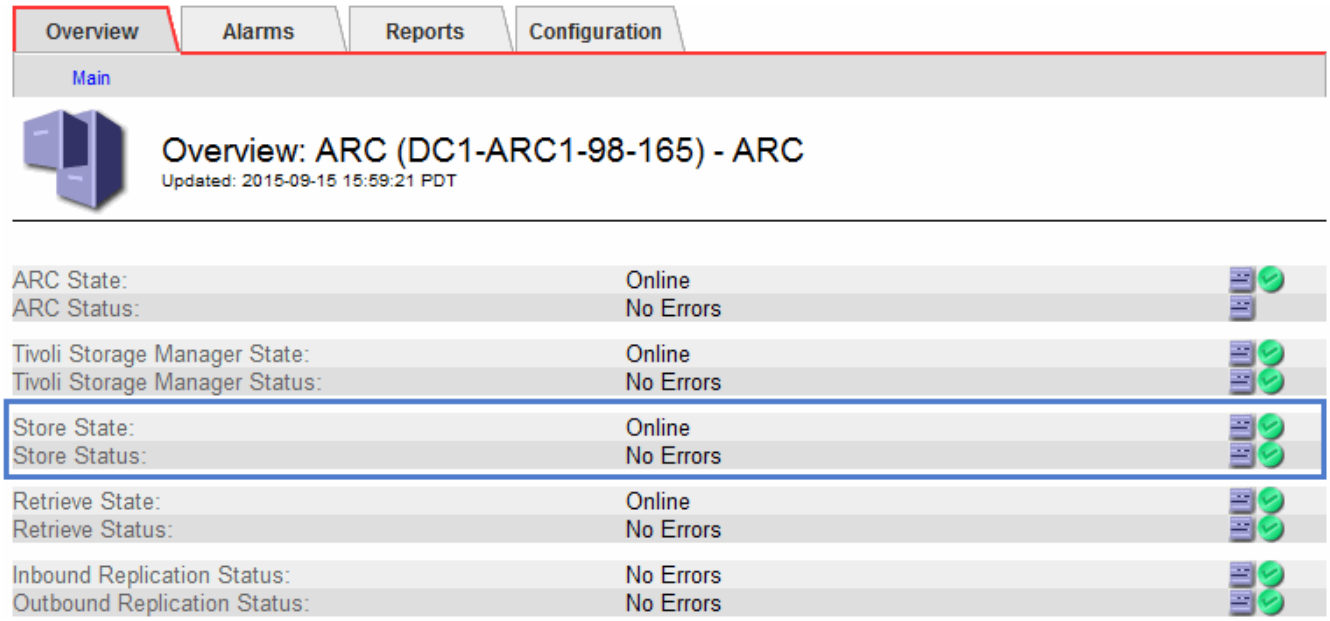
No puede supervisar directamente la capacidad de un sistema de almacenamiento de archivado externo mediante el sistema StorageGRID. Sin embargo, puede supervisar si el nodo de archivado aún puede enviar datos de objeto al destino de archivado, lo que podría indicar que se necesita una ampliación del medio de archivado.

Acerca de esta tarea

Puede supervisar el componente Store para comprobar si el nodo de archivado puede seguir enviando datos de objeto al sistema de almacenamiento de archivado de destino. La alarma de fallos de almacenamiento (ARVF) también puede indicar que el sistema de almacenamiento de archivado objetivo ha alcanzado la capacidad y que ya no puede aceptar datos de objetos.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Archive Node*** > **ARC> Descripción general> Principal**.
3. Compruebe los atributos Estado del almacén y Estado del almacén para confirmar que el componente Tienda está en línea sin errores.



Un componente de almacén sin conexión o uno con errores puede indicar que el sistema de almacenamiento de archivado dirigido ya no puede aceptar datos de objetos porque ha alcanzado su capacidad.

Alertas y alarmas

Gestionar alertas y alarmas: Descripción general

El sistema de alertas StorageGRID se ha diseñado para informarle de los problemas operativos que requieren su atención. El sistema de alarma heredado está obsoleto.

Sistema de alertas

El sistema de alertas está diseñado para ser su herramienta principal para supervisar cualquier problema que pueda producirse en el sistema StorageGRID. El sistema de alertas proporciona una interfaz fácil de usar para detectar, evaluar y resolver problemas.

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 icono 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 **NODES** y en la ficha **NODES** > ***node*** > **Overview**.
- 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.

Sistema de alarma heredado

Al igual que las alertas, las alarmas se activan en niveles de gravedad específicos cuando los atributos alcanzan valores de umbral definidos. Sin embargo, a diferencia de las alertas, se activan muchas alarmas para los eventos que se pueden ignorar de forma segura, lo que podría dar lugar a un número excesivo de mensajes de correo electrónico o notificaciones SNMP.

> El sistema de alarma está obsoleto y se quitará en un lanzamiento futuro. Si todavía utiliza alarmas heredadas, debe realizar una transición completa al Lo antes posible. del sistema de alertas.

Cuando se activa una alarma, se realizan las siguientes acciones:

- La alarma aparece en la página **SUPPORT** > **Alarms (Legacy)** > **Current Alarms**.
- Se envía una notificación por correo electrónico, suponiendo que ha configurado un servidor SMTP y una o más listas de correo.
- Es posible que se envíe una notificación de SNMP, suponiendo que haya configurado el agente SNMP de StorageGRID. (Las notificaciones SNMP no se envían para todas las alarmas o gravedades de alarma).

Comparar alertas y alarmas

Hay varias similitudes entre el sistema de alerta y el sistema de alarma heredado, pero el sistema de alerta ofrece ventajas significativas y es más fácil de usar.

Consulte la siguiente tabla para obtener información sobre cómo realizar operaciones similares.

	Alertas	Alarmas (sistema heredado)
¿Cómo puedo ver qué alertas o alarmas están activas?	• Seleccione el enlace **Alertas actuales** en el panel de control. • Seleccione la alerta en la página **NODES** > **Overview**. • Seleccione **ALERTS** > **Current**. "Ver las alertas actuales"	Seleccione **SUPPORT** > **Alarms (Legacy)** > **Current Alarms**. "Gestionar alarmas (sistema heredado)"
¿Qué hace que se active una alerta o una alarma?	Las alertas se activan cuando una expresión Prometheus de una regla de alerta se evalúa como TRUE para la condición y duración de desencadenador específicas. "Ver reglas de alerta"	Las alarmas se activan cuando un atributo StorageGRID alcanza un valor de umbral. "Gestionar alarmas (sistema heredado)"
Si se activa una alerta o alarma, ¿cómo puedo resolver el problema subyacente?	Las acciones recomendadas para una alerta se incluyen en las notificaciones por correo electrónico y están disponibles en las páginas Alertas de Grid Manager. Según sea necesario, se proporciona información adicional en la documentación de StorageGRID. "Referencia de alertas"	Puede obtener más información sobre una alarma seleccionando el nombre del atributo o puede buscar un código de alarma en la documentación de StorageGRID. "Referencia de alarmas (sistema heredado)"
¿Dónde puedo ver una lista de alertas o alarmas que se han resuelto?	Seleccione **ALERTS** > **Resolved**. "Ver las alertas actuales y resueltas"	Seleccione **SUPPORT** > **Alarms (Legacy)** > **Historical Alarms**. "Gestionar alarmas (sistema heredado)"
¿Dónde puedo gestionar la configuración?	Seleccione **ALERTS** > **Reglas**. "Gestionar alertas"	Seleccione **SOPORTE**. A continuación, utilice las opciones de la sección **Alarmas (heredadas)** del menú. "Gestionar alarmas (sistema heredado)"

	Alertas	Alarmas (sistema heredado)
¿Qué permisos de grupo de usuarios necesito?	• Cualquier persona que pueda iniciar sesión en Grid Manager puede ver las alertas actuales y resueltas. • Debe tener el permiso Gestionar alertas para gestionar silencios, notificaciones de alertas y reglas de alertas. "Administre StorageGRID"	• Cualquier persona que pueda iniciar sesión en Grid Manager puede ver las alarmas heredadas. • Debe tener el permiso de acuse de recibo de alarmas para acusar recibo de alarmas. • Debe tener tanto la configuración de la página de topología de cuadrícula como otros permisos de configuración de cuadrícula para gestionar las alarmas globales y las notificaciones por correo electrónico. "Administre StorageGRID"
¿Cómo puedo gestionar las notificaciones por correo electrónico?	Seleccione **ALERTS** > **Configuración de correo electrónico**. **Nota:** debido a que las alarmas y alertas son sistemas independientes, la configuración de correo electrónico utilizada para las notificaciones de alarma y AutoSupport no se utiliza para las notificaciones de alerta. Sin embargo, puede utilizar el mismo servidor de correo para todas las notificaciones. "Configure notificaciones por correo electrónico para las alertas"	Seleccione **SUPPORT** > **Alarms (Legacy)** > **Configuración de correo electrónico heredado**. "Gestionar alarmas (sistema heredado)"
¿Cómo se gestionan las notificaciones SNMP?	Seleccione **CONFIGURACIÓN** > **Supervisión** > **Agente SNMP**. "Usar supervisión de SNMP"	*No soportado*

	Alertas	Alarmas (sistema heredado)
¿Cómo puedo controlar quién recibe notificaciones?	1. Seleccione **ALERTS** > **Configuración de correo electrónico**. 2. En la sección **destinatarios**, introduzca una dirección de correo electrónico para cada lista de correo electrónico o persona que deba recibir un correo electrónico cuando se produzca una alerta. "Configure notificaciones por correo electrónico para las alertas"	1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Configuración de correo electrónico heredado**. 2. Crear una lista de correo. 3. Seleccione **Notificaciones**. 4. Seleccione la lista de correo. "Gestionar alarmas (sistema heredado)"
¿Qué nodos administrador envían notificaciones?	Un nodo de administración único (el remitente preferido). "¿Qué es un nodo de administración?"	Un nodo de administración único (el remitente preferido). "¿Qué es un nodo de administración?"
¿Cómo puedo suprimir algunas notificaciones?	1. Seleccione **ALERTS** > **silencios**. 2. Seleccione la regla de alerta que desea silenciar. 3. Especifique una duración para el silencio. 4. Seleccione la gravedad de la alerta que desea silenciar. 5. Seleccione esta opción para aplicar el silencio a toda la cuadrícula, un solo sitio o un único nodo. **Nota**: Si ha habilitado el agente SNMP, las silencios también suprimen las capturas SNMP e informan. "Silenciar notificaciones de alerta"	1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Configuración de correo electrónico heredado**. 2. Seleccione **Notificaciones**. 3. Seleccione una lista de correo y seleccione **Suprimir**. "Gestionar alarmas (sistema heredado)"

	Alertas	Alarmas (sistema heredado)
¿Cómo puedo suprimir todas las notificaciones?	Seleccione **ALERTS** > **silencios**.luego, seleccione **todas las reglas**. **Nota**: Si ha habilitado el agente SNMP, las silencios también suprimen las capturas SNMP e informan. "Silenciar notificaciones de alerta"	*No soportado*
¿Cómo puedo personalizar las condiciones y los desencadenantes?	1. Seleccione **ALERTS** > **Reglas**. 2. Seleccione una regla predeterminada para editar o seleccione **Crear regla personalizada**. "Editar reglas de alerta" "Crear reglas de alerta personalizadas"	1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Global Alarms**. 2. Cree una alarma Global Custom para anular una alarma predeterminada o para supervisar un atributo que no tenga una alarma predeterminada. "Gestionar alarmas (sistema heredado)"
¿Cómo puedo desactivar una alerta o alarma individual?	1. Seleccione **ALERTS** > **Reglas**. 2. Seleccione la regla y seleccione **Editar regla**. 3. Desactive la casilla de verificación **enabled**. "Deshabilitar reglas de alerta"	1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Global Alarms**. 2. Seleccione la regla y seleccione el icono Editar. 3. Desactive la casilla de verificación **enabled**. "Gestionar alarmas (sistema heredado)"

Gestionar alertas

Gestionar alertas: descripción general

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.

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

Si quiere más información:

- Vea el vídeo: "Vídeo: Información general de alertas de StorageGRID 11,8"

- Vea el vídeo: "Vídeo: Usar métricas para crear alertas personalizadas en StorageGRID 11,8"

- Consulte "Referencia de alertas".

Ver reglas de alerta

Las reglas de alerta definen las condiciones que desencadenan "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.

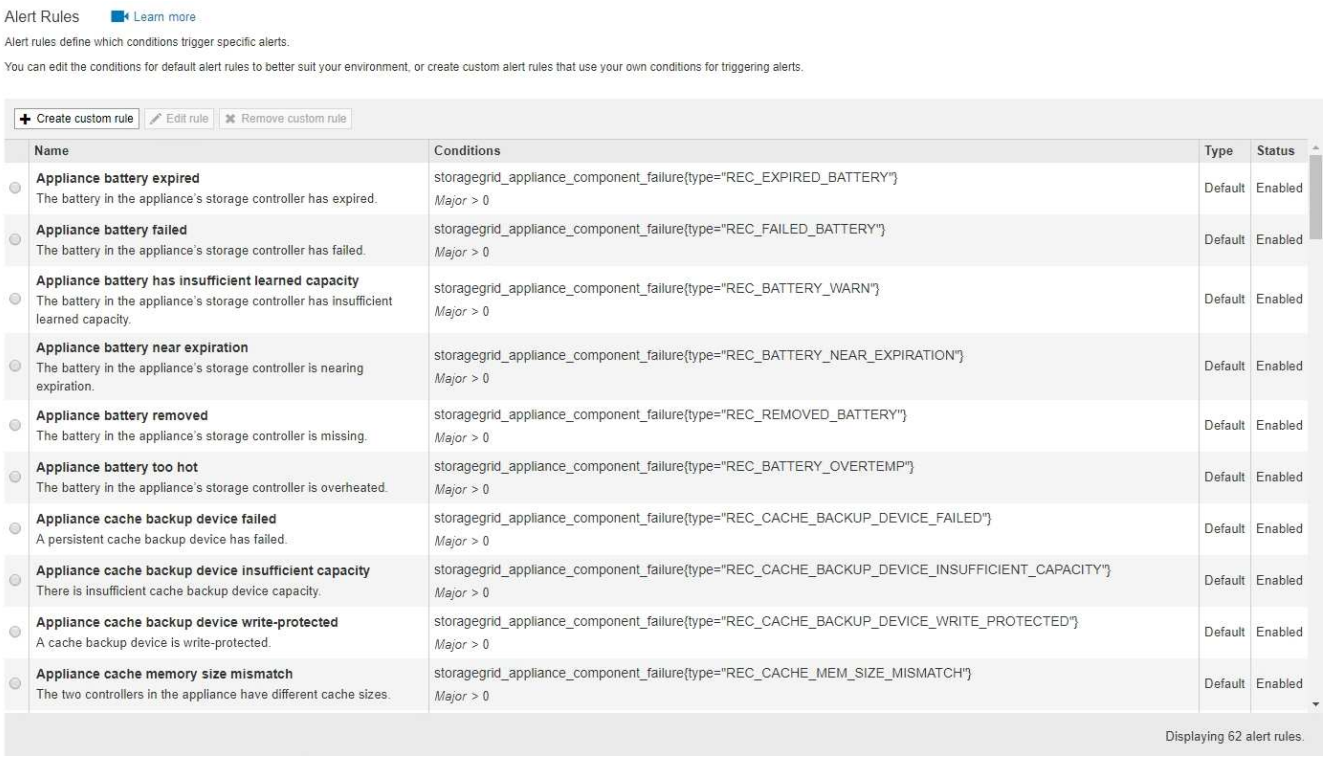
Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Gestionar alertas o permisos de acceso raíz".
- Opcionalmente, ha visto el vídeo: "Vídeo: Información general de alertas de StorageGRID 11,8"

Pasos

1. Seleccione **ALERTS** > **Reglas**.

   Aparecerá la página Reglas de alerta.



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.
Condiciones	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. • **Crítico**: Existe una condición anormal que ha detenido las operaciones normales de un nodo StorageGRID o servicio. 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 afecta a las operaciones actuales o se acerca 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 de funcionamiento del sistema 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	Tipo de regla de alerta: • **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	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.

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 un "navegador web compatible".
- Usted tiene la "Gestionar alertas o permisos de acceso raíz".
- Usted está familiarizado con el "Métricas de Prometheus que se usan habitualmente".
- Usted entiende la "Sintaxis de las consultas Prometheus".
- Opcionalmente, ha visto el vídeo: "Vídeo: Usar métricas para crear alertas personalizadas en StorageGRID 11,8".

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`, primera ejecución `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.

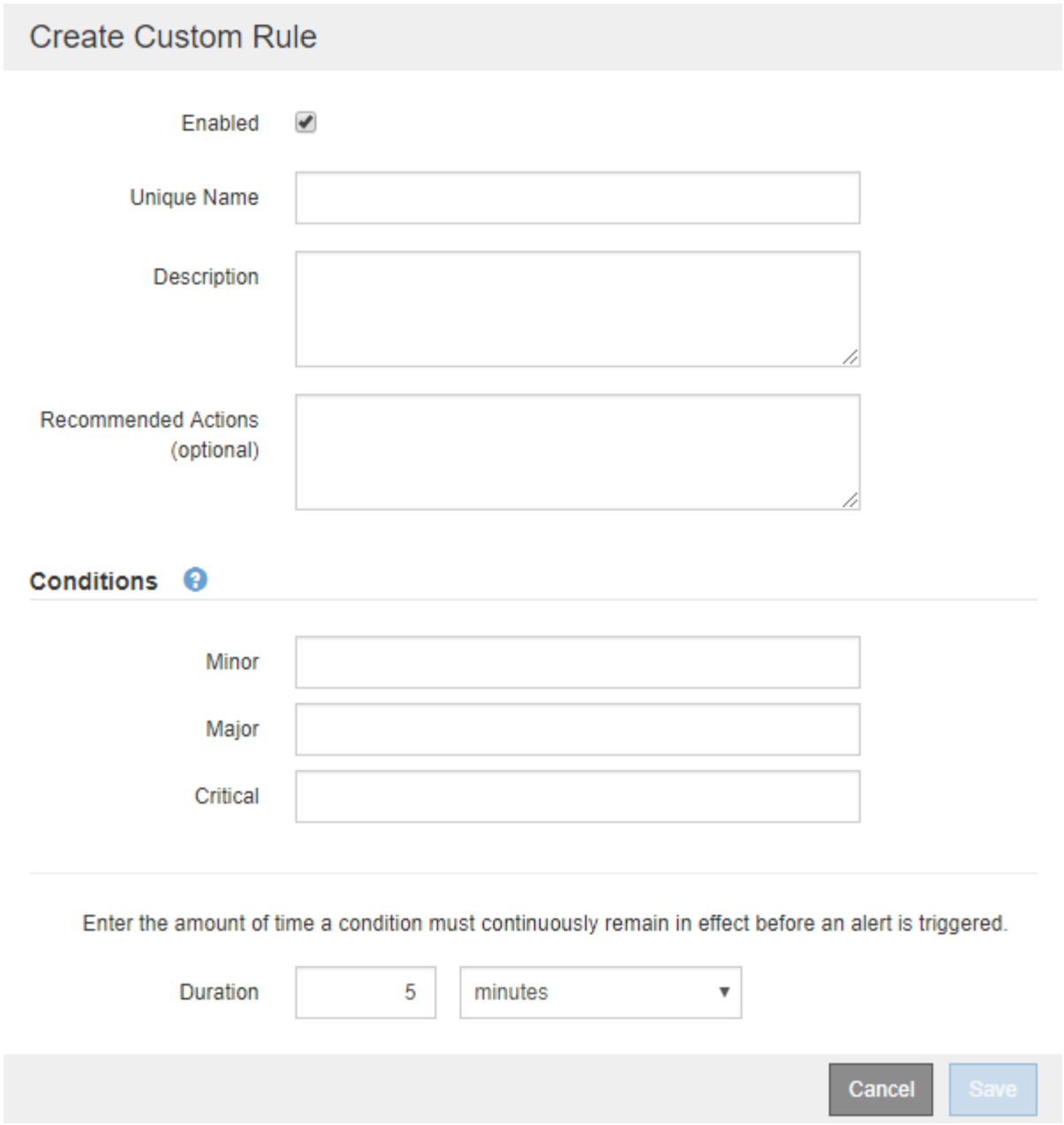
Pasos

1. Seleccione **ALERTS** > **Reglas**.

   Aparecerá la página Reglas de alerta.

2. Seleccione **Crear regla personalizada**.

   Aparece el cuadro de diálogo Crear regla personalizada.



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 expresiones Prometheus, seleccione el icono de ayuda Y siga el enlace a la sección Metrics de la API de Grid Management.

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 un "navegador web compatible".
- Usted tiene la "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.

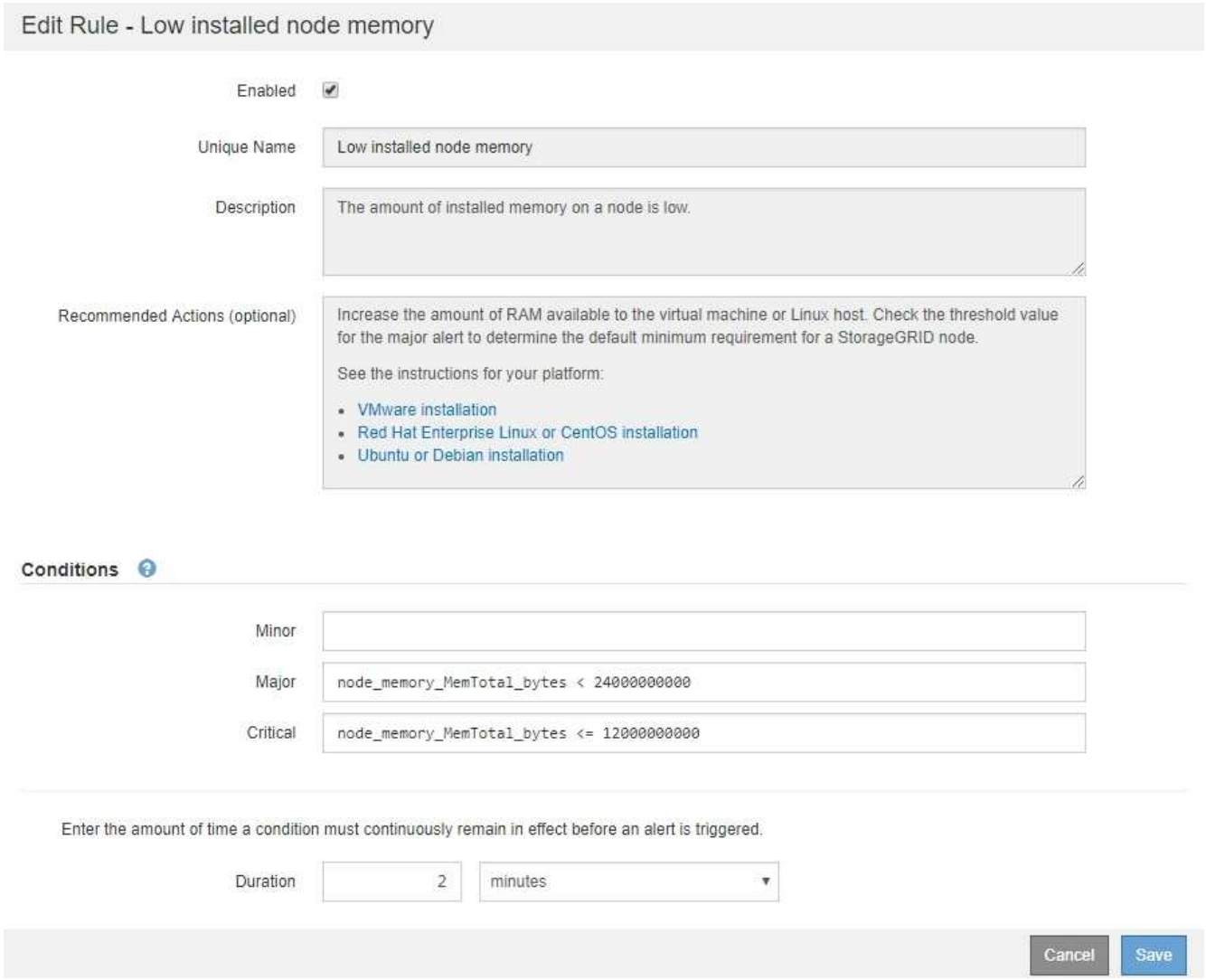
Pasos

1. Seleccione **ALERTS** > **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.



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.

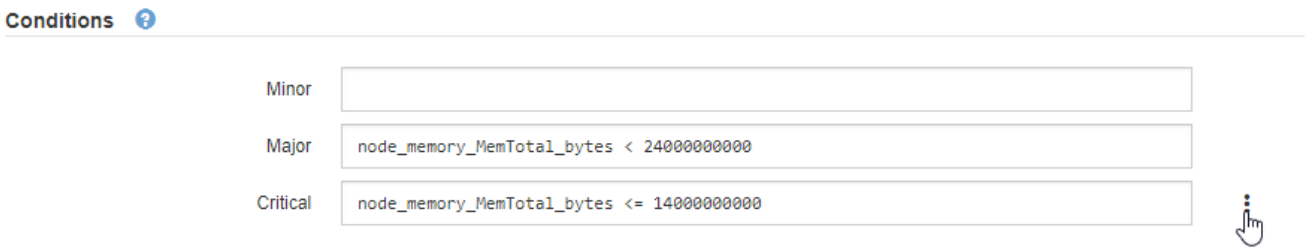
5. En el caso de reglas de alerta personalizadas, actualice la siguiente información según sea necesario.

   > 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.



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 un "navegador web compatible".
- Usted tiene la "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 **ALERTS** > **Reglas**.

Aparecerá la página Reglas de alerta.

2. Seleccione el botón de opción de la regla de alerta que desee 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 un "navegador web compatible".
- Usted tiene la "Gestionar alertas o permisos de acceso raíz".

Pasos

1. Seleccione **ALERTS** > **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** > **Supervisión** > **agente SNMP** en el Administrador de grid o los puntos finales SNMP de la API de administración de grid para activar y configurar el agente SNMP de StorageGRID. El agente SNMP admite las tres versiones del protocolo SNMP.

Para aprender a 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 informa son compatibles con SNMPv2c y SNMPv3.

Las notificaciones Trap e inform 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, las capturas e informes SNMP y las notificaciones de alarmas heredadas. 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 un "navegador web compatible".
- Usted tiene la "Gestionar alertas o permisos de acceso raíz".

Acerca de esta tarea

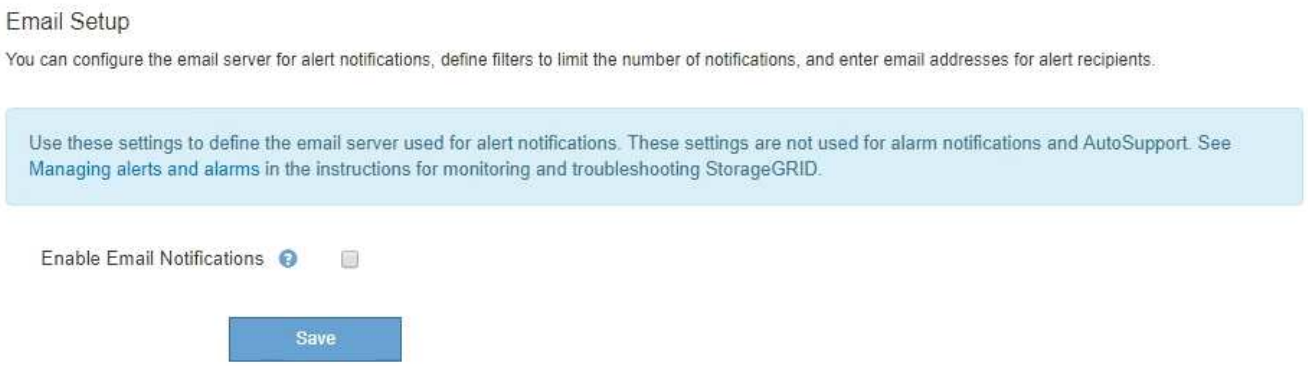
Debido a que las alarmas y las alertas son sistemas independientes, la configuración de correo electrónico utilizada para las notificaciones de alertas no se utiliza para las notificaciones de alarmas ni los paquetes AutoSupport. Sin embargo, puede utilizar el mismo servidor de correo electrónico para 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, las capturas e informes SNMP y las notificaciones de alarmas heredadas. 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 **ALERTS** > **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.
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.

   a. 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`

   b. 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).

   a. 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.

   b. 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.

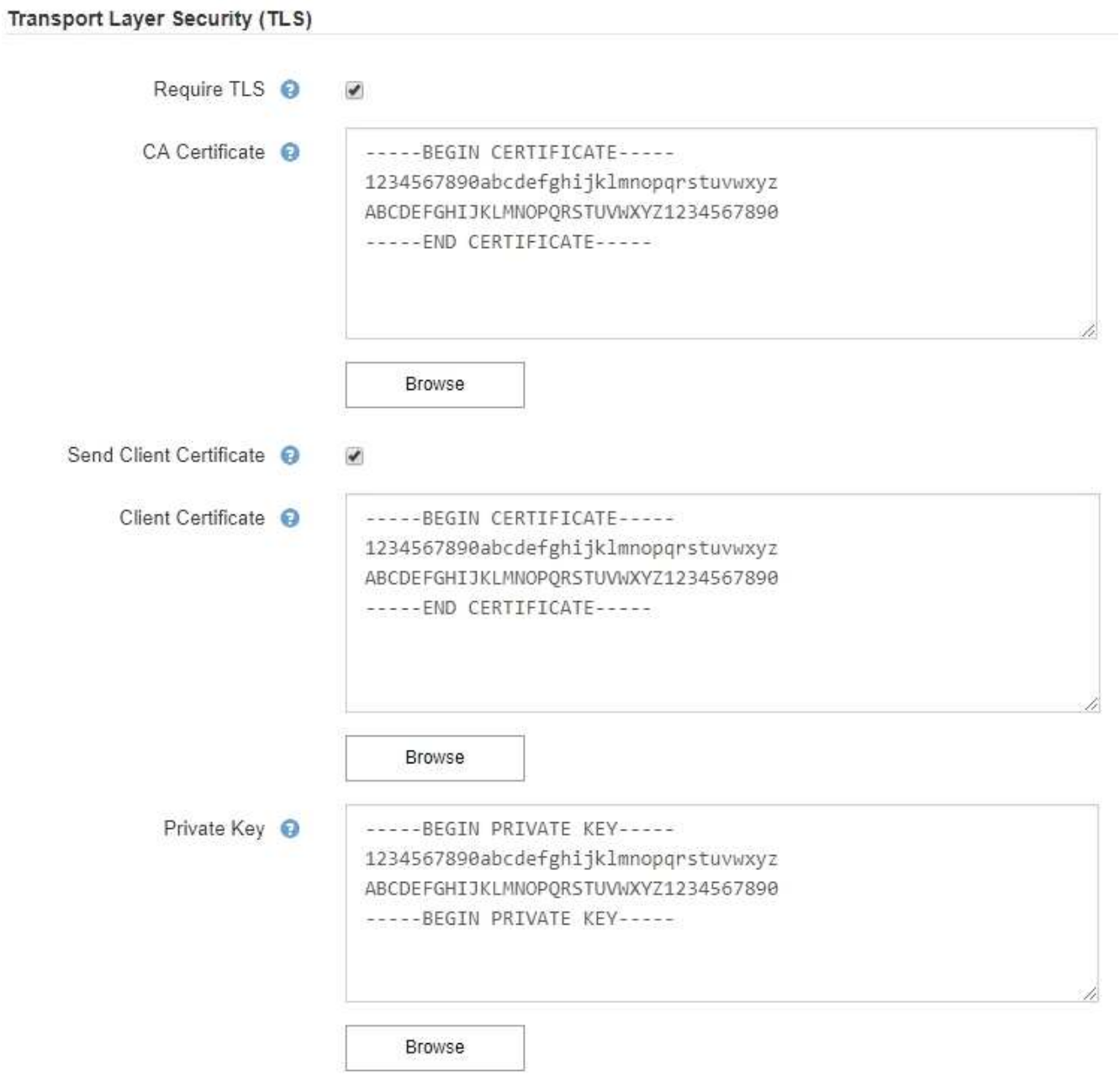
   c. En el campo **Certificado de cliente**, proporcione el certificado de cliente codificado con PEM para enviar al servidor SMTP.

      Puede copiar y pegar el contenido en este campo, o seleccione **examinar** y seleccione el archivo.

   d. En el campo **clave privada**, introduzca la clave privada del certificado de cliente en codificación PEM sin cifrar.

      Puede copiar y pegar el contenido en este campo, o seleccione **examinar** y seleccione el archivo.

      > Si necesita editar la configuración de correo electrónico, seleccione el icono del 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.

Gravedad	Descripción
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:
   a. Seleccione **Enviar correo electrónico de prueba**.

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

   b. 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.

   c. 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 y notificaciones de alarma heredadas, donde todos los nodos de administración envían el correo electrónico de prueba.

8. Seleccione **Guardar**.

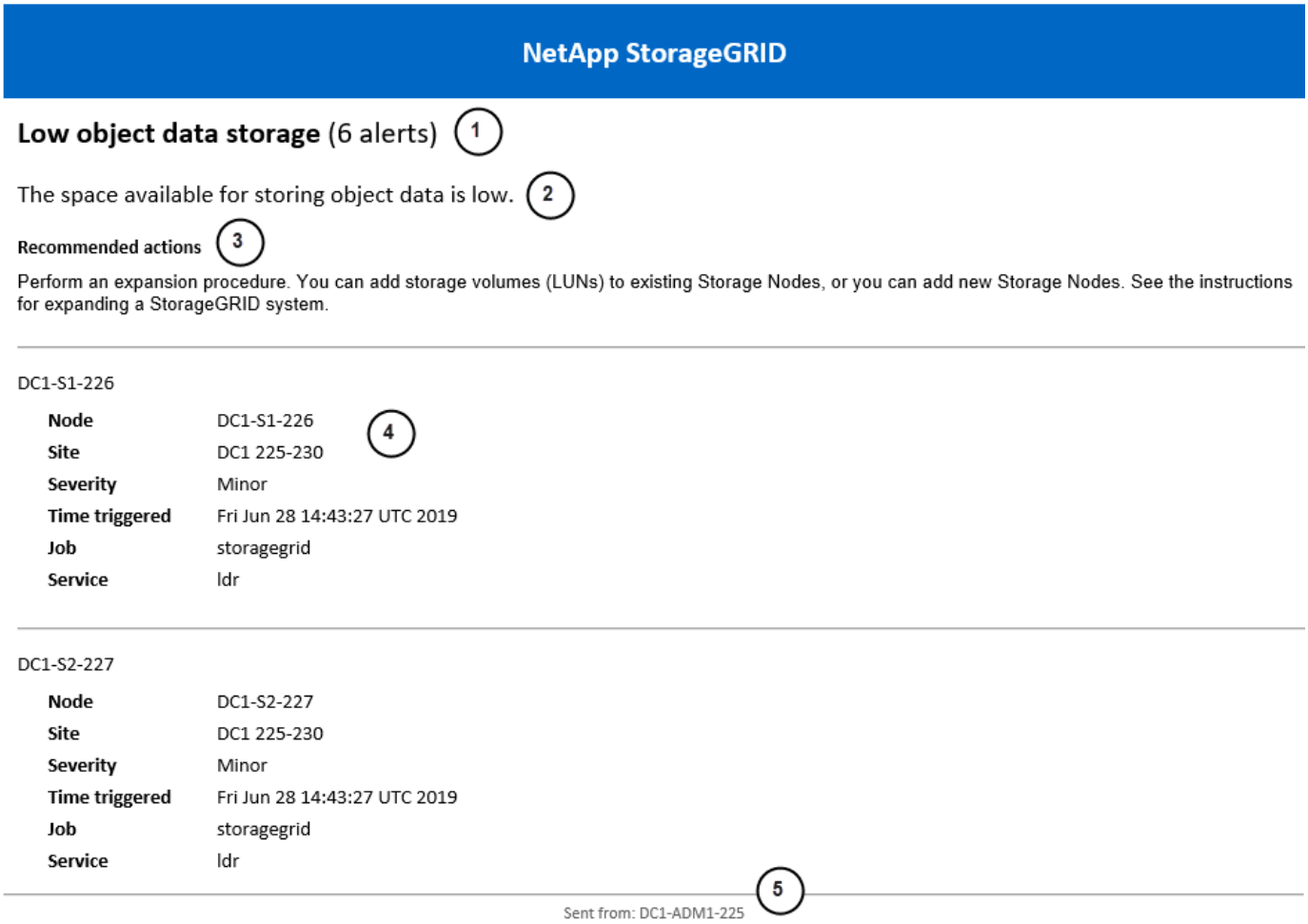
   El envío de un mensaje de correo electrónico de prueba no guarda la configuración. Debe seleccionar **Guardar**.

   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:



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.	• 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.	• 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.	1. La alerta A se activa en el nodo 1 a las 08:00. No se envía ninguna notificación. 2. La alerta A se activa en el nodo 2 a las 08:01. No se envía ninguna notificación. 3. 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.	1. La alerta A se activa en el nodo 1 a las 08:00. Se envía una notificación a las 08:02. 2. 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.	1. La alerta A se activa para el nodo 1. Se envía una notificación. 2. Se activa la alerta A para el nodo 2. Se envía una segunda notificación. 3. La alerta A se ha resuelto para el nodo 2, pero sigue estando activa para el nodo 1. 4. 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.	1. La alerta A se activa para el nodo 1 el 8 de marzo. Se envía una notificación. 2. 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.

Solucione 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 un "navegador web compatible".
- Usted tiene la "Gestionar alertas o permisos de acceso raíz".

Pasos

1. Compruebe la configuración.
   a. Seleccione **ALERTS** > **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 un "navegador web compatible".
- Usted tiene la "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 silencios también suprimen las capturas SNMP e informan.

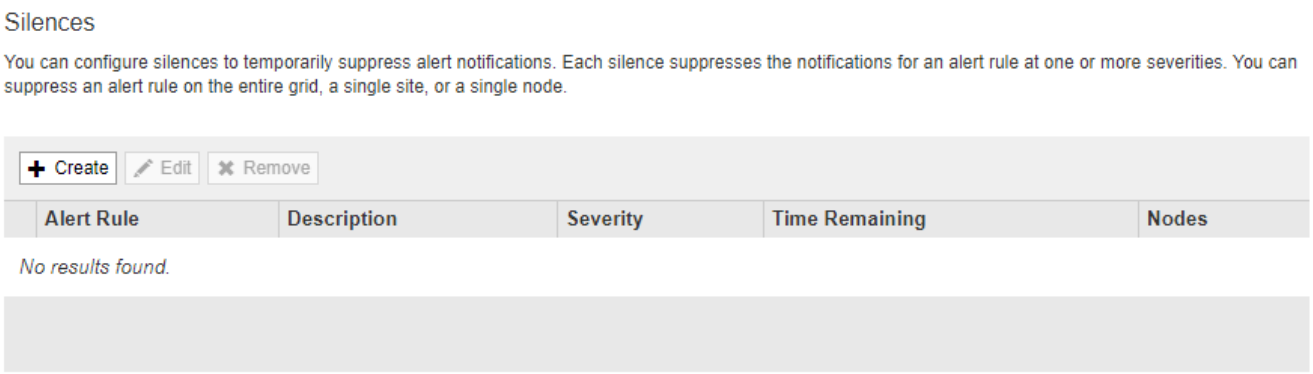
> Tenga cuidado al decidir silenciar una regla de alerta. Si silencia una alerta, es posible que no detecte un problema subyacente hasta que impida que se complete una operación crítica.

> Como las alarmas y las alertas son sistemas independientes, no puede utilizar esta funcionalidad para suprimir las notificaciones de alarma.

Pasos

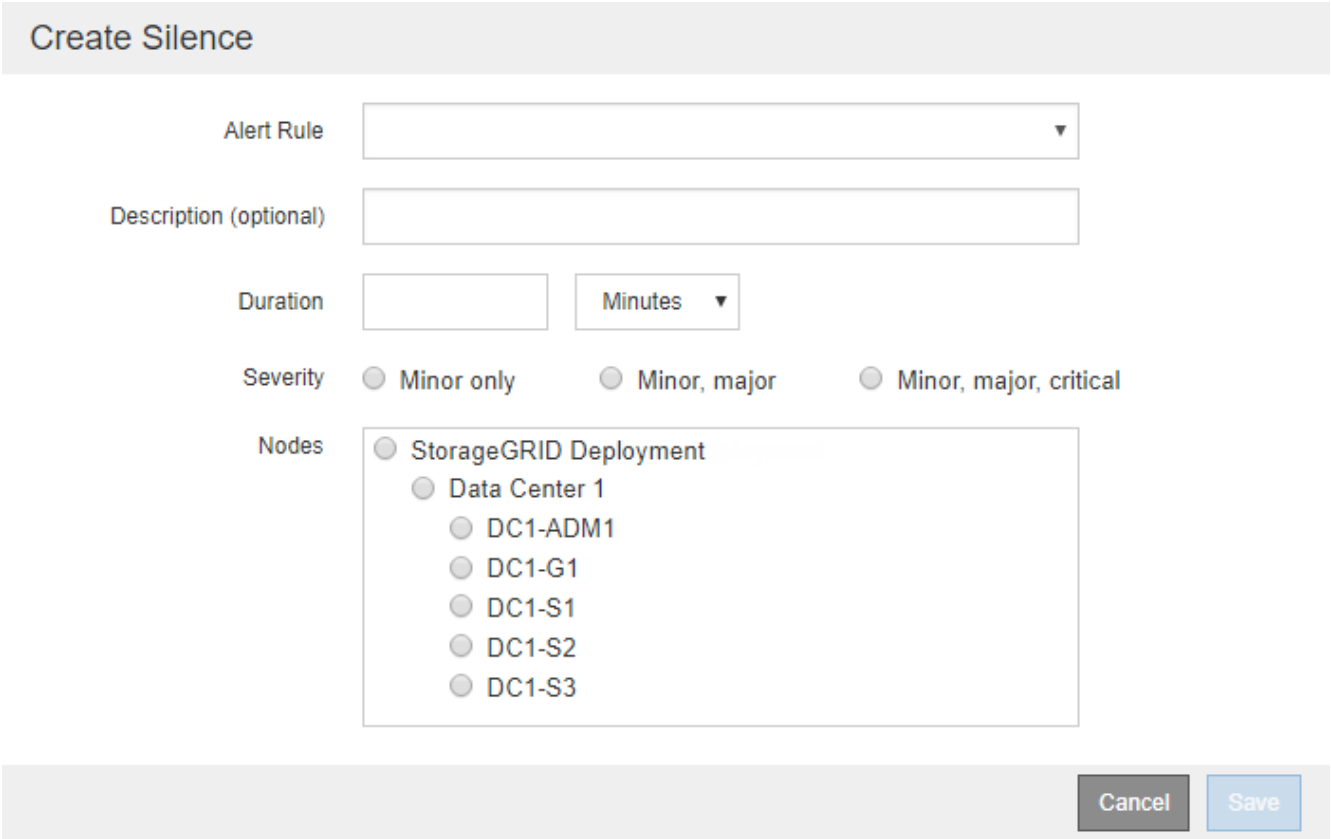
1. Seleccione **ALERTS** > **silencios**.

   Aparece la página silencios.



2. Seleccione **Crear**.

   Aparece el cuadro de diálogo Crear silencio.



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	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). **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**.
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	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. **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.

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

Opción	Descripción
Edite un silencio	a. Seleccione **ALERTS** > **silencios**. b. En la tabla, seleccione el botón de opción para el silencio que desea editar. c. Seleccione **Editar**. d. Cambie la descripción, la cantidad de tiempo restante, las gravedades seleccionadas o el nodo afectado. e. Seleccione **Guardar**.

Opción	Descripción
Elimine un silencio	a. Seleccione **ALERTS** > **silencios**. b. En la tabla, seleccione el botón de radio para el silencio que desea eliminar. c. Seleccione **Quitar**. d. Seleccione **Aceptar** para confirmar que desea eliminar este silencio. **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.

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 predeterminadas 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).
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.
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.
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.

Nombre de alerta	Descripción
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.
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.

Nombre de alerta	Descripción
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	La E/S de disco muy lenta puede afectar 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.
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 discos para los mensajes de auditoría está llena. Si no se resuelve esta condición, es posible que se produzcan errores en las operaciones S3 o Swift.
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.

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.
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.

Nombre de alerta	Descripción
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.

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 en la notificación por correo electrónico	No se pudo enviar la notificación por correo electrónico para una alerta.

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.

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 y Swift	El certificado de servidor global para S3 y Swift 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.
El periodo de análisis de ILM es demasiado largo	El tiempo necesario para analizar, evaluar y aplicar ILM a los objetos es demasiado largo.

Nombre de alerta	Descripción
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.
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.

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 resuelve esta condición, es posible que se produzcan errores en las operaciones S3 o Swift.
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 Marca de agua de solo lectura suave 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 resuelve esta condición, es posible que se produzcan errores en las operaciones S3 o Swift.
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
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 perdidos	Se han perdido uno o más objetos de la cuadrícula.
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 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 ha estado desconectado durante más de 5 minutos, posiblemente debido a que el nodo se reinició durante el paso de formato del volumen.
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.

Nombre de alerta	Descripción
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 directiva de seguridad no requiere el modo FIPS, pero el módulo de seguridad criptográfica de NetApp está habilitado.
Es necesario reiniciar para habilitar FIPS	La directiva de seguridad requiere el modo FIPS, pero el módulo de seguridad criptográfica de NetApp está deshabilitado.
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.

También puede hacerlo obtener una lista completa de todas las métricas.

Para obtener más información sobre la sintaxis de las consultas de Prometheus, consulte "Consultando a Prometeo".

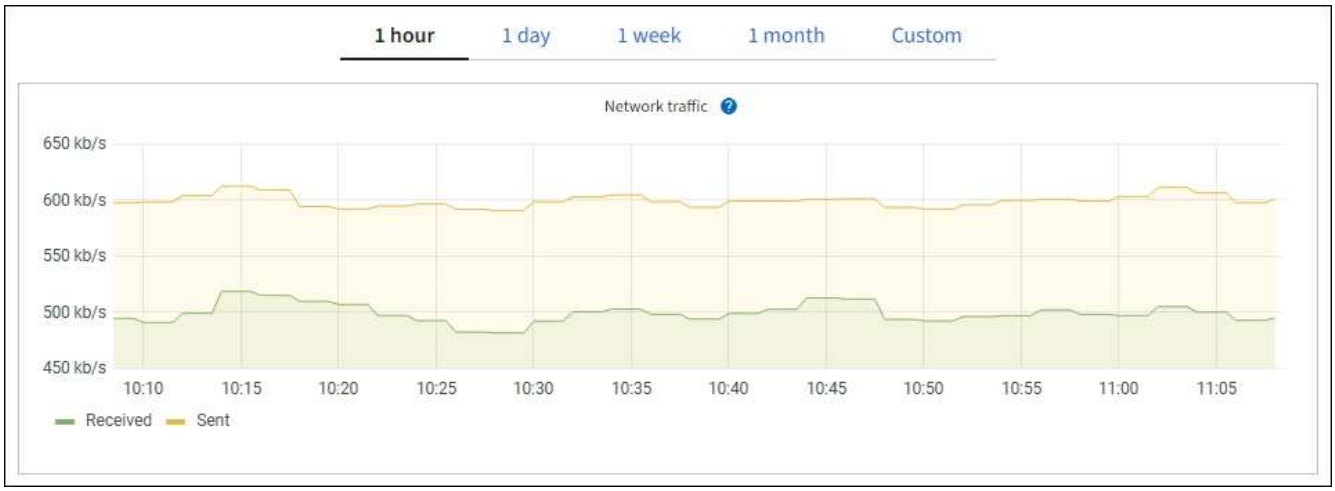
¿Qué son las métricas de Prometheus?

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 la `/var/local/mysql_ibdata/` el volumen alcanza la capacidad; las métricas más antiguas se eliminan primero.

¿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 icono de ayuda y selecciona **Documentación de API** > **Métricas**). Aunque hay más de mil métricas disponibles, solo se necesita un número relativamente pequeño para supervisar las operaciones de StorageGRID más críticas.

> 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 **SUPPORT** > **Tools** > **Diagnostics** y la página **SUPPORT** > **Tools** > **Metrics**: Estas páginas, que están destinadas principalmente al 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_retifations_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 del dispositivo de red `receive_errs`.

node_network_transmit_errs_total

Estadística del 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

El número total de bloques S3 y contenedores Swift que se conocen en este nodo de almacenamiento.

storagegrid_content_objects

La cantidad total de objetos de datos S3 y Swift que se conocen en 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 o Swift.

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 ingesta).

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_ingeridos

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_recuperados

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_operaciones_error

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_operaciones_correctamente

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

storagegrid_s3_operaciones_no autorizadas

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_swift_data_transfers_bytes_ingeridos

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

storagegrid_swift_data_transfers_bytes_recuperados

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

storagegrid_swift_operaciones_failed

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

storagegrid_swift_operaciones_correctamente

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

storagegrid_swift_operaciones_no autorizado

Número total de operaciones Swift fallidas que son el resultado de un error de autorización (códigos de estado HTTP 401, 403, 405).

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.

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 el `GET /grid/metric-names` funcionamiento.
4. Descargue los resultados.

Gestionar alarmas (sistema heredado)

Gestionar alarmas (sistema heredado)

El sistema de alarma StorageGRID es el sistema heredado utilizado para identificar puntos problemáticos que a veces ocurren durante el funcionamiento normal.

Aunque el sistema de alarma heredado sigue siendo compatible, el sistema de alerta ofrece importantes ventajas y es más fácil de usar.

Clases de alarma (sistema heredado)

Una alarma heredada puede pertenecer a una de las dos clases de alarma mutuamente excluyentes.

- Las alarmas predeterminadas se proporcionan con cada sistema StorageGRID y no se pueden modificar. Sin embargo, puede desactivar las alarmas predeterminadas o anularlas definiendo las alarmas personalizadas globales.
- Las alarmas personalizadas globales controlan el estado de todos los servicios de un tipo determinado en el sistema StorageGRID. Puede crear una alarma Global Custom para anular una alarma predeterminada. También puede crear una nueva alarma Global Custom. Esto puede ser útil para supervisar cualquier condición personalizada de su sistema StorageGRID.

Lógica de activación de alarmas (sistema heredado)

Una alarma heredada se activa cuando un atributo StorageGRID alcanza un valor de umbral que se evalúa como verdadero frente a una combinación de clase de alarma (predeterminada o personalizada global) y nivel de gravedad de alarma.

.	Color	Gravedad de alarma	Significado
	Amarillo	Aviso	El nodo está conectado a la cuadrícula, pero existe una condición poco habitual que no afecta a las operaciones normales.

.	Color	Gravedad de alarma	Significado
	Naranja claro	Menor	El nodo está conectado a la cuadrícula, pero existe una condición anormal que podría afectar al funcionamiento en el futuro. Debe investigar para evitar el escalado.
	Naranja oscuro	Importante	El nodo está conectado a la cuadrícula, pero existe una condición anormal que afecta actualmente al funcionamiento. Esto requiere atención inmediata para evitar un escalado.
	Rojo	Crítico	El nodo está conectado a la cuadrícula, pero existe una condición anormal que ha detenido las operaciones normales. Debe abordar el problema de inmediato.

La gravedad de la alarma y el valor del umbral correspondiente se pueden establecer para cada atributo numérico. El servicio NMS de cada nodo de administración supervisa continuamente los valores de atributos actuales en función de los umbrales configurados. Cuando se activa una alarma, se envía una notificación a todo el personal designado.

Tenga en cuenta que un nivel de gravedad normal no desencadena una alarma.

Los valores de los atributos se evalúan en relación con la lista de alarmas activadas definidas para ese atributo. La lista de alarmas se Marca en el siguiente orden para encontrar la primera clase de alarma con una alarma definida y activada para el atributo:

1. Alarmas personalizadas globales con niveles de alarma desde críticos hasta avisos.
2. Alarmas predeterminadas con límites de alarma desde crítica hasta Aviso.

Después de que se encuentre una alarma activada para un atributo en la clase de alarma superior, el servicio NMS sólo evalúa dentro de esa clase. El servicio NMS no se evaluará en comparación con las otras clases de menor prioridad. Es decir, si hay una alarma Global Custom activada para un atributo, el servicio NMS sólo evalúa el valor del atributo frente a las alarmas Global Custom. Las alarmas predeterminadas no se evalúan. Por lo tanto, una alarma predeterminada activada para un atributo puede cumplir los criterios necesarios para activar una alarma, pero no se activará porque se activa una alarma personalizada global (que no cumple los criterios especificados) para el mismo atributo. No se activa ninguna alarma y no se envía ninguna notificación.

Ejemplo de activación de alarma

Puede utilizar este ejemplo para entender cómo se activan las alarmas personalizadas globales y las alarmas predeterminadas.

En el ejemplo siguiente, un atributo tiene una alarma Global Custom y una alarma predeterminada definida y activada, como se muestra en la siguiente tabla.

	Umbral de alarma global personalizada (activado)	Umbral de alarma predeterminado (activado)
Aviso	>= 1500	>= 1000
Menor	>= 15.000	>= 1000
Importante	>=150,000	>= 250.000

Si el atributo se evalúa cuando su valor es 1000, no se activa ninguna alarma y no se envía ninguna notificación.

La alarma Global Custom tiene prioridad sobre la alarma predeterminada. Un valor de 1000 no alcanza el valor umbral de ningún nivel de gravedad para la alarma Global Custom. Como resultado, el nivel de alarma se evalúa para ser normal.

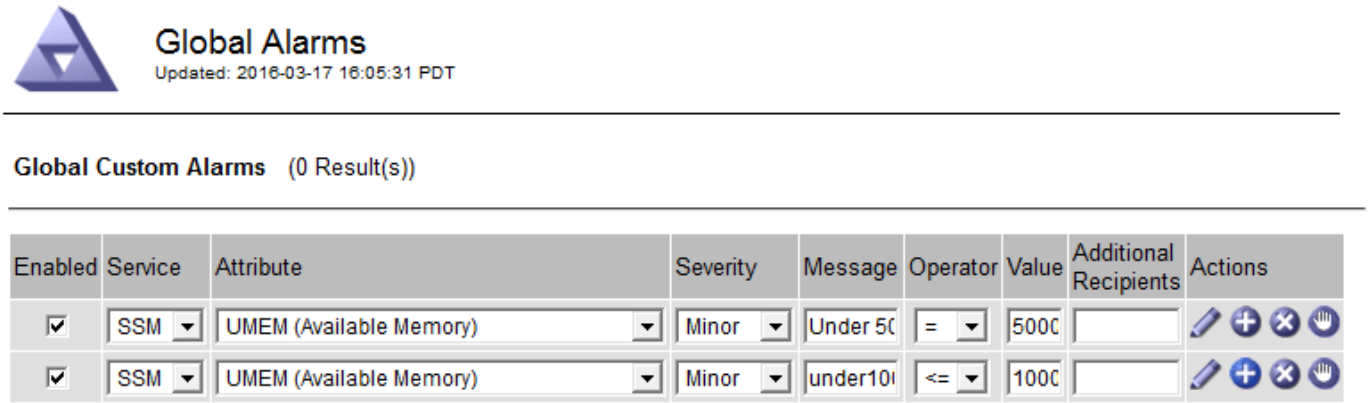
Después de la situación anterior, si la alarma Global Custom está desactivada, no cambia nada. El valor del atributo se debe volver a evaluar antes de que se active un nuevo nivel de alarma.

Con la alarma Global Custom desactivada, cuando se vuelve a evaluar el valor del atributo, el valor del atributo se evalúa frente a los valores de umbral de la alarma predeterminada. El nivel de alarma activa una alarma de nivel de aviso y se envía una notificación por correo electrónico al personal designado.

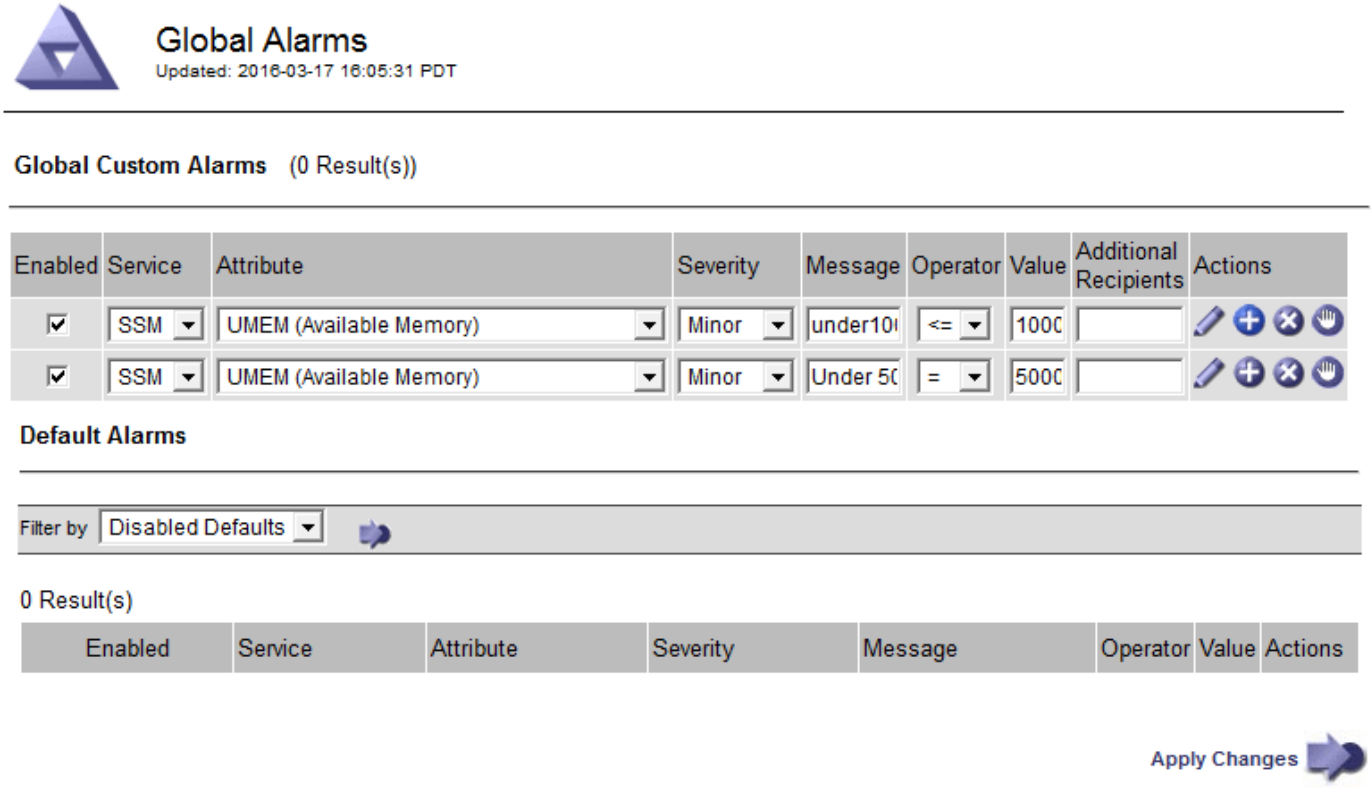
Alarmas de la misma gravedad

Si dos alarmas personalizadas globales para el mismo atributo tienen la misma gravedad, las alarmas se evalúan con una prioridad descendente.

Por ejemplo, si UMEM cae a 50 MB, se activa la primera alarma (= 50000000), pero no la que está debajo de ella (<=100000000).



Si el orden se invierte, cuando UMEM cae a 100MB, se activa la primera alarma (<=100000000), pero no la que está por debajo (= 50000000).



Notificaciones

Una notificación informa de la aparición de una alarma o del cambio de estado de un servicio. Las notificaciones de alarma se pueden enviar por correo electrónico o mediante SNMP.

Para evitar que se envíen varias alarmas y notificaciones cuando se alcance un valor de umbral de alarma, se comprueba la gravedad de la alarma con respecto a la gravedad actual del atributo. Si no hay cambio, no se toman medidas adicionales. Esto significa que, a medida que el servicio NMS siga supervisando el sistema, sólo generará una alarma y enviará notificaciones la primera vez que observe una condición de alarma para un atributo. Si se alcanza y se detecta un nuevo umbral de valor para el atributo, la gravedad de la alarma cambia y se envía una nueva notificación. Las alarmas se borran cuando las condiciones vuelven al nivel normal.

El valor del disparador que se muestra en la notificación de un estado de alarma se redondea a tres posiciones decimales. Por lo tanto, un valor de atributo de 1.9999 activa una alarma cuyo umbral es inferior a (<) 2.0, aunque la notificación de alarma muestra el valor de activación como 2.0.

Nuevos servicios

A medida que se agregan nuevos servicios mediante la adición de nuevos nodos de cuadrícula o sitios, heredan las alarmas predeterminadas y las alarmas personalizadas globales.

Alarmas y tablas

Los atributos de alarma que se muestran en las tablas se pueden desactivar a nivel del sistema. Las alarmas no se pueden desactivar para filas individuales de una tabla.

Por ejemplo, en la siguiente tabla se muestran dos alarmas de entradas críticas disponibles (VMFI). (Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***Storage Node*** > **SSM** > **Resources**.)

Puede desactivar la alarma VMFI para que no se active la alarma VMFI de nivel crítico (ambas alarmas críticas aparecerán en verde en la tabla); Sin embargo, no puede desactivar una sola alarma en una fila de tabla, de modo que una alarma VMFI se muestre como una alarma de nivel crítico mientras que la otra se mantenga verde.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	sda1	Online	10.6 GB	7.46 GB	655,360	559,263	Enabled
/var/local	sda3	Online	63.4 GB	59.4 GB	3,932,160	3,931,842	Unknown
/var/local/rangedb/0	sdb	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled
/var/local/rangedb/1	sdc	Online	53.4 GB	53.4 GB	52,428,800	52,427,848	Enabled
/var/local/rangedb/2	sdd	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled

Confirmar alarmas actuales (sistema heredado)

Las alarmas heredadas se activan cuando los atributos del sistema alcanzan valores de umbral de alarma. De forma opcional, si desea reducir o borrar la lista de alarmas heredadas, puede reconocer las alarmas.

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Debe tener el permiso de acuse de recibo de alarmas.

Acerca de esta tarea

Dado que el sistema de alarmas heredado sigue siendo compatible, la lista de alarmas heredadas de la página Alarmas actuales aumenta cada vez que se produce una nueva alarma. Por lo general, puede ignorar las alarmas (ya que las alertas proporcionan una mejor vista del sistema) o puede confirmar las alarmas.

De manera opcional, cuando haya pasado completamente al sistema de alertas, puede desactivar cada alarma heredada para evitar que se active y se agregue al recuento de alarmas heredadas.

Cuando reconoce una alarma, ésta ya no aparece en la página Alarmas actuales del Gestor de cuadrícula, a menos que la alarma se active en el siguiente nivel de gravedad o se resuelva y se vuelva a producir.

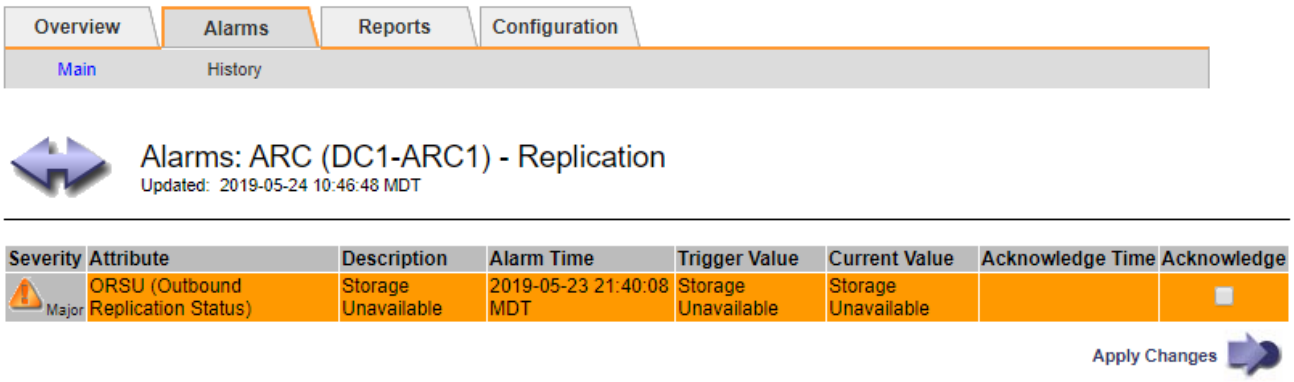
Aunque el sistema de alarma heredado sigue siendo compatible, el sistema de alerta ofrece importantes ventajas y es más fácil de usar.

Pasos

1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Current Alarms**.

2. Seleccione el nombre del servicio en la tabla.

   Aparece la ficha Alarmas para el servicio seleccionado (**SUPPORT** > **Tools** > **Topología de cuadrícula** > ***nodo de cuadrícula*** > ***Servicio*** > **Alarmas**).



3. Seleccione la casilla de verificación **Aceptar** para la alarma y haga clic en **Aplicar cambios**.

   La alarma ya no aparece en el panel de control ni en la página Alarmas actuales.

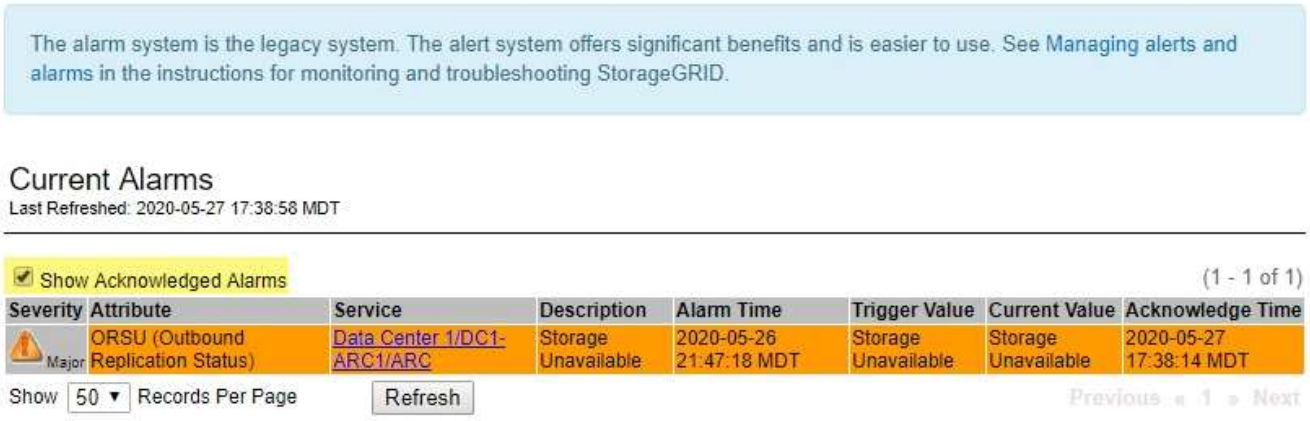
   > Cuando reconoce una alarma, la confirmación no se copia en otros nodos de administración. Por este motivo, si ve el panel de control desde otro nodo de administración, puede continuar viendo la alarma activa.

4. Según sea necesario, vea las alarmas confirmadas.

   a. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Current Alarms**.

   b. Seleccione **Mostrar alarmas aceptadas**.

      Se muestran todas las alarmas confirmadas.



Ver alarmas predeterminadas (sistema heredado)

Puede ver la lista de todas las alarmas heredadas predeterminadas.

Antes de empezar

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

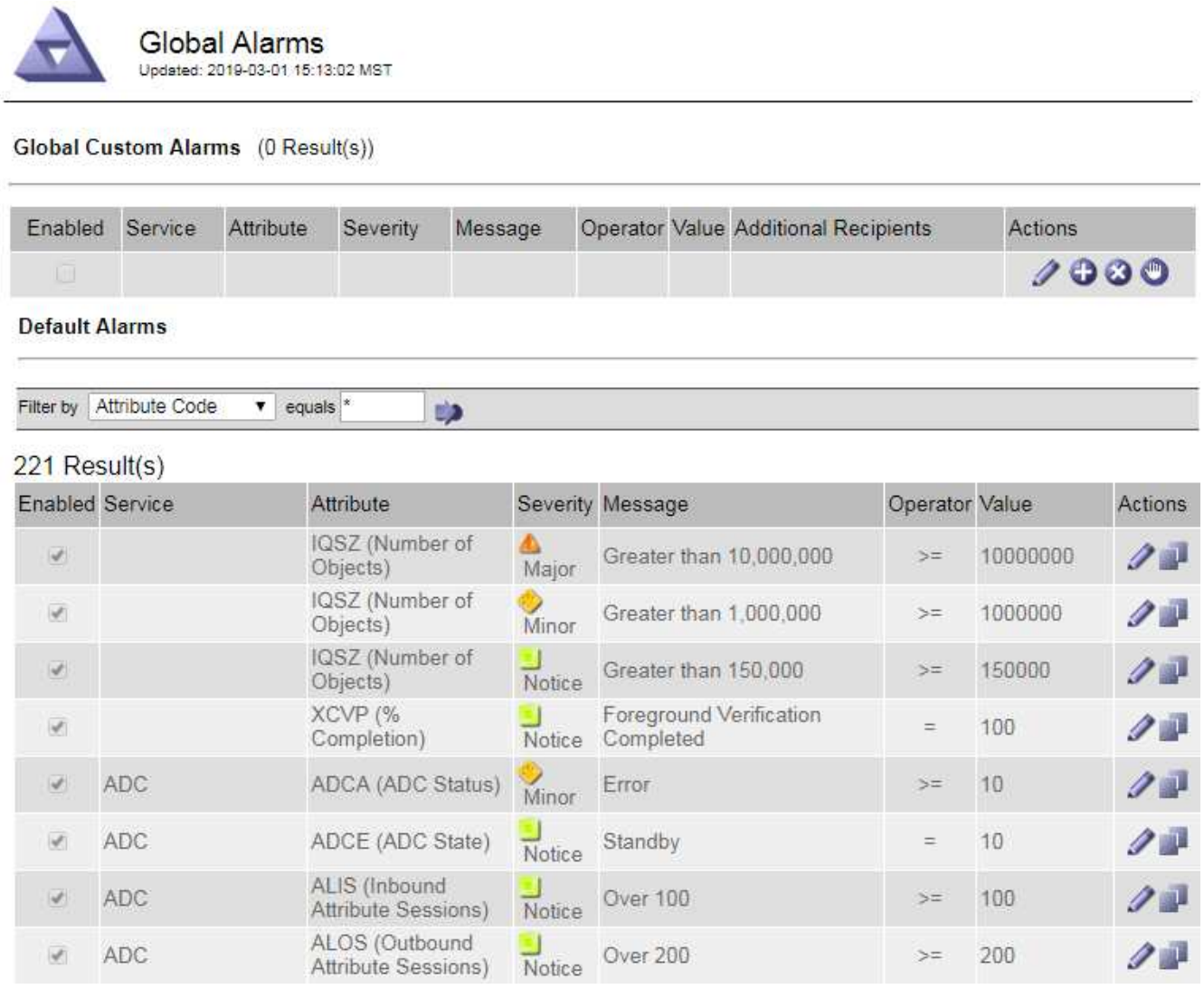
- Ya tienes "permisos de acceso específicos".

> Aunque el sistema de alarma heredado sigue siendo compatible, el sistema de alerta ofrece importantes ventajas y es más fácil de usar.

Pasos

1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Global Alarms**.
2. En filtro por, seleccione **Código de atributo** o **Nombre de atributo**.
3. En el caso de igual a, introduzca un asterisco: *
4. Haga clic en la flecha O pulse **Intro**.

   Se muestran todas las alarmas predeterminadas.



Revisar las alarmas históricas y la frecuencia de las alarmas (sistema heredado)

Al solucionar un problema, puede revisar la frecuencia con la que se ha activado una alarma heredada en el pasado.

Antes de empezar

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

> Aunque el sistema de alarma heredado sigue siendo compatible, el sistema de alerta ofrece importantes ventajas y es más fácil de usar.

Pasos

1. Siga estos pasos para obtener una lista de todas las alarmas activadas durante un período de tiempo.
   a. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Historical Alarms**.
   b. Debe realizar una de las siguientes acciones:
      - Haga clic en uno de los períodos de tiempo.
      - Introduzca un rango personalizado y haga clic en **Consulta personalizada**.
2. Siga estos pasos para averiguar con qué frecuencia se han activado las alarmas para un atributo determinado.
   a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
   b. Seleccione ***Grid node*** > ***service o component*** > **Alarms** > **History**.
   c. Seleccione el atributo de la lista.
   d. Debe realizar una de las siguientes acciones:
      - Haga clic en uno de los períodos de tiempo.
      - Introduzca un rango personalizado y haga clic en **Consulta personalizada**.

      Las alarmas se enumeran en orden cronológico inverso.
   e. Para volver al formulario de solicitud del historial de alarmas, haga clic en **Historial**.

Crear alarmas personalizadas globales (sistema heredado)

Es posible que haya utilizado alarmas personalizadas globales para el sistema heredado para atender requisitos de supervisión específicos. Las alarmas personalizadas globales pueden tener niveles de alarma que anulan las alarmas predeterminadas o pueden supervisar atributos que no tienen una alarma predeterminada.

Antes de empezar

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

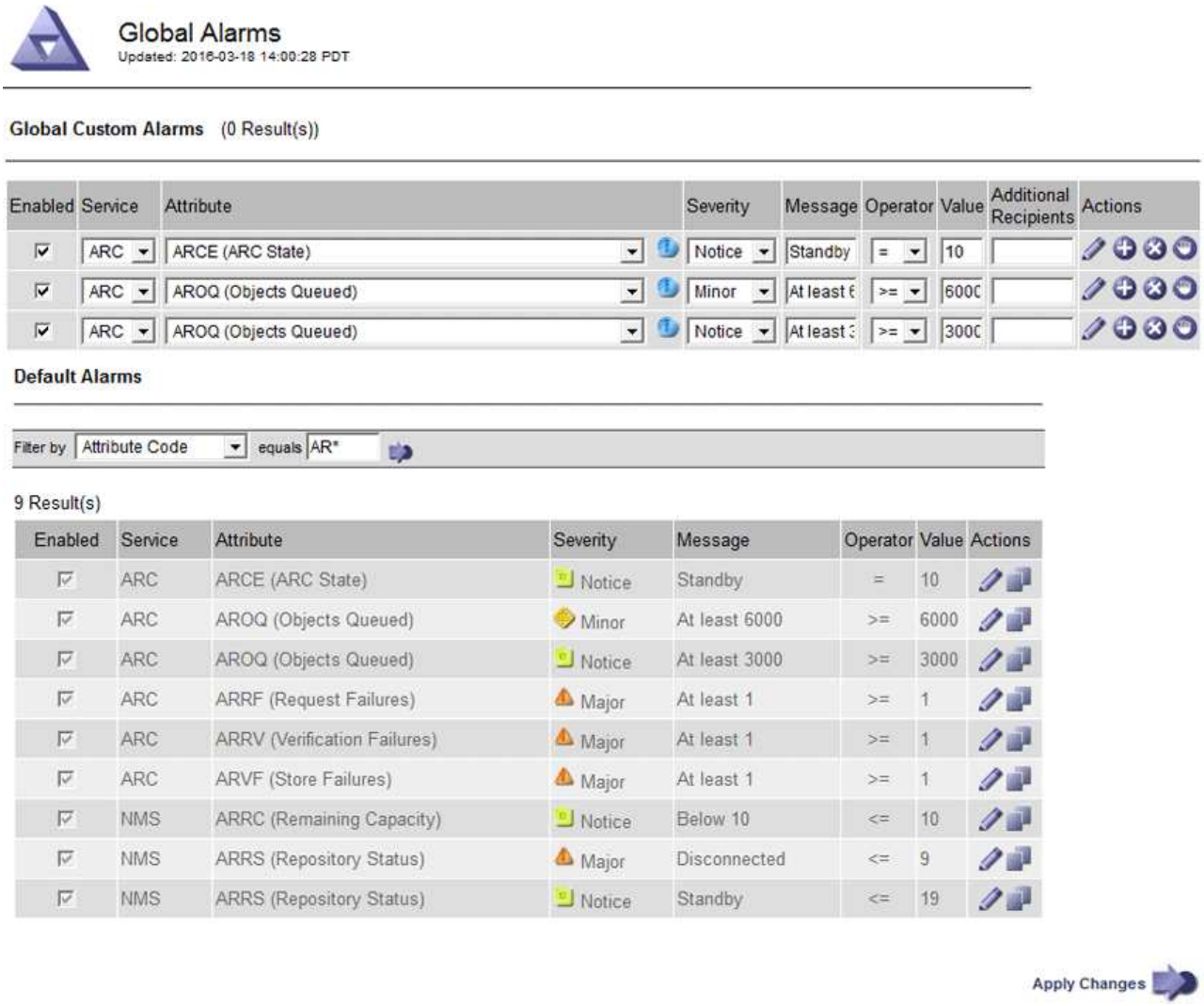
> Aunque el sistema de alarma heredado sigue siendo compatible, el sistema de alerta ofrece importantes ventajas y es más fácil de usar.

Las alarmas personalizadas globales anulan las alarmas predeterminadas. No debe cambiar los valores de alarma predeterminados a menos que sea absolutamente necesario. Al cambiar las alarmas predeterminadas, corre el riesgo de ocultar problemas que, de lo contrario, podrían desencadenar una alarma.

> Tenga cuidado si cambia los ajustes de alarma. Por ejemplo, si aumenta el valor del umbral de una alarma, es posible que no detecte un problema subyacente. Comente los cambios propuestos con el soporte técnico antes de cambiar la configuración de una alarma.

Pasos

1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Global Alarms**.
2. Agregue una nueva fila a la tabla Alarmas globales personalizadas:
   - Para añadir una nueva alarma, haga clic en **Editar** (Si ésta es la primera entrada) o **Insertar**.



   - Para modificar una alarma predeterminada, busque la alarma predeterminada.
     i. En Filtrar por, seleccione **código de atributo** o **Nombre de atributo**.
     ii. Escriba una cadena de búsqueda.

     Especifique cuatro caracteres o utilice caracteres comodín (por ejemplo, A???? O AB*). Asteriscos (*) representan múltiples caracteres y signos de interrogación (?) representa un solo carácter.

     iii. Haga clic en la flecha O pulse **Intro**.
     iv. En la lista de resultados, haga clic en **Copiar** junto a la alarma que desea modificar.

     La alarma predeterminada se copia en la tabla Alarmas globales personalizadas.

3. Realice los cambios necesarios en la configuración de alarmas personalizadas globales:

Título	Descripción
Activado	Active o desactive la casilla de verificación para activar o desactivar la alarma.
Atributo	Seleccione el nombre y el código del atributo que se supervisa en la lista de todos los atributos aplicables al servicio o componente seleccionado. Para ver información sobre el atributo, haga clic en **Info** junto al nombre del atributo.
Gravedad	El icono y el texto que indican el nivel de la alarma.
Mensaje	El motivo de la alarma (pérdida de conexión, espacio de almacenamiento inferior al 10%, etc.).
Operador	Operadores para probar el valor del atributo actual con respecto al umbral de valor: • = equivale a • > mayor que • < menor que • >= mayor o igual que • <= menor o igual que • ≠ no igual a.
Valor	El valor de umbral de la alarma utilizado para comprobar el valor real del atributo mediante el operador. La entrada puede ser un solo número, un intervalo de números especificado con dos puntos (1:3) o una lista de números y rangos con una coma.
Otros destinatarios	Una lista complementaria de direcciones de correo electrónico que se notificarán cuando se active la alarma. Esto se suma a la lista de correo configurada en la página **Alarmas** > **Configuración de correo electrónico**. Las listas están delimitadas por comas. **Nota:** Las listas de correo requieren la configuración del servidor SMTP para funcionar. Antes de agregar listas de correo, confirme que SMTP está configurado. Las notificaciones de alarmas personalizadas pueden anular las notificaciones de las alarmas Global Custom o predeterminadas.

Título	Descripción
Acciones	Botones de control para: Editar una fila + Insertar una fila + Eliminar una fila + Arrastre una fila hacia arriba o hacia abajo + Copiar una fila

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

Desactivar alarmas (sistema heredado)

Las alarmas del sistema de alarmas heredado están activadas de forma predeterminada, pero puede desactivar las alarmas que no sean necesarias. También puede desactivar las alarmas heredadas una vez que haya pasado completamente al nuevo sistema de alertas.

> Aunque el sistema de alarma heredado sigue siendo compatible, el sistema de alerta ofrece importantes ventajas y es más fácil de usar.

Desactivar una alarma predeterminada (sistema heredado)

Puede desactivar una de las alarmas predeterminadas heredadas para todo el sistema.

Antes de empezar

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

Acerca de esta tarea

La desactivación de una alarma para un atributo que actualmente tiene una alarma activada no borra la alarma actual. La alarma se desactivará la próxima vez que el atributo cruce el umbral de alarma o se pueda borrar la alarma activada.

> No deshabilite ninguna de las alarmas heredadas hasta que haya realizado la transición completa al nuevo sistema de alertas. De lo contrario, es posible que no detecte un problema subyacente hasta que no se complete una operación crucial.

Pasos

1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Global Alarms**.
2. Busque la alarma predeterminada para desactivarla.
   a. En la sección Alarmas predeterminadas, seleccione **Filtrar por** > **Código de atributo** o **Nombre de atributo**.

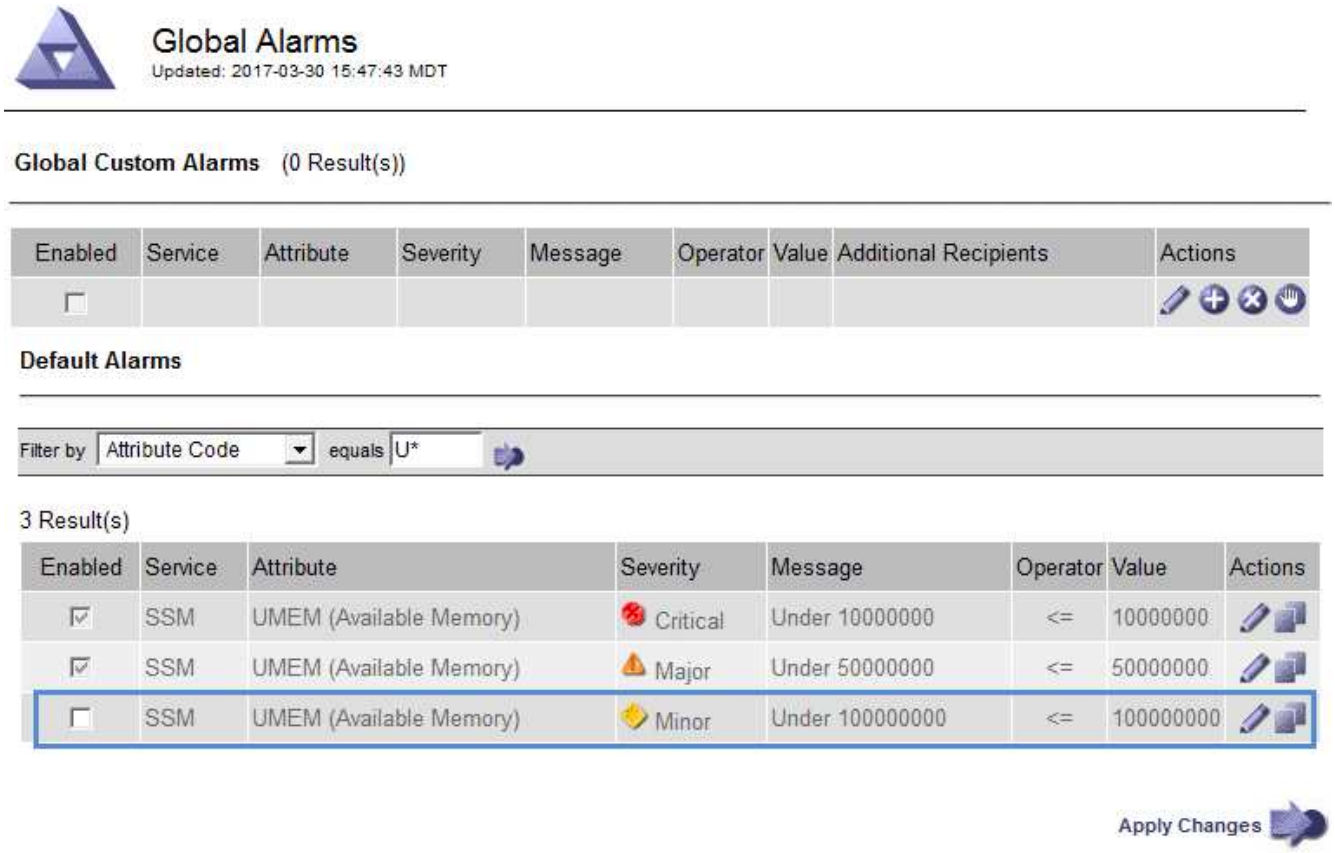
b. Escriba una cadena de búsqueda.

   Especifique cuatro caracteres o utilice caracteres comodín (por ejemplo, A???? O AB*). Asteriscos (*) representan múltiples caracteres y signos de interrogación (?) representa un solo carácter.

c. Haga clic en la flecha O pulse **Intro**.

> Al seleccionar **valores predeterminados desactivados** se muestra una lista de todas las alarmas predeterminadas actualmente desactivadas.

3. En la tabla de resultados de búsqueda, haga clic en el icono Editar para la alarma que desea desactivar.



   La casilla de verificación **enabled** para la alarma seleccionada se activa.

4. Desactive la casilla de verificación **enabled**.
5. Haga clic en **aplicar cambios**.

   La alarma predeterminada está desactivada.

Desactivar alarmas personalizadas globales (sistema heredado)

Puede desactivar una alarma Global Custom heredada para todo el sistema.

Antes de empezar

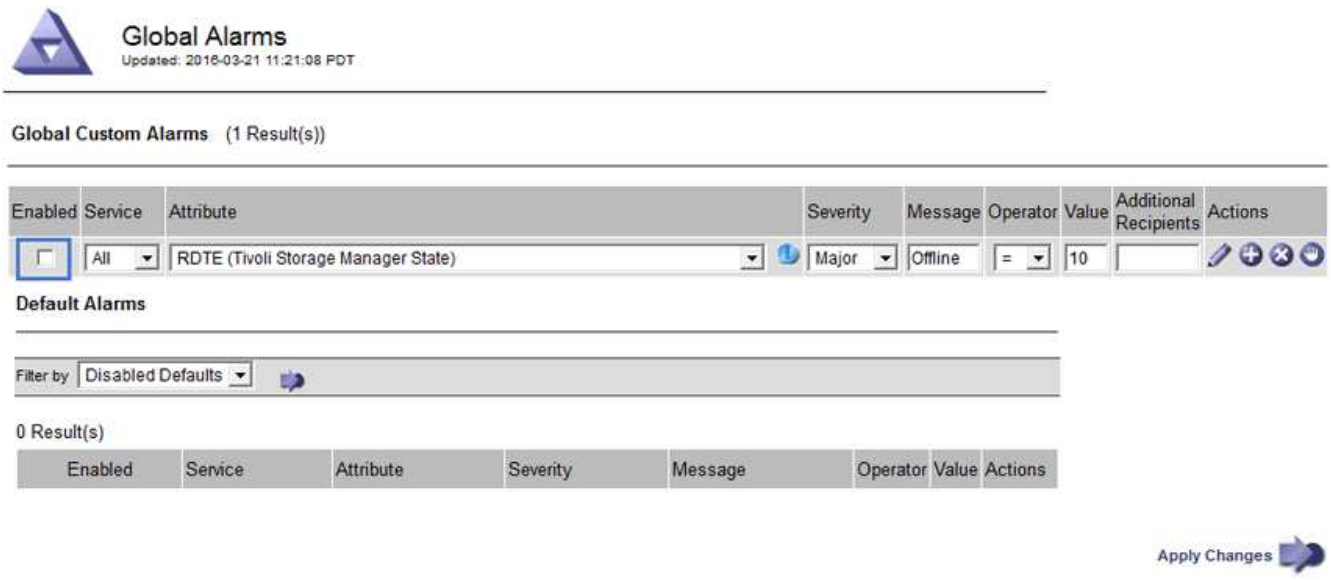
- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".

Acerca de esta tarea

La desactivación de una alarma para un atributo que actualmente tiene una alarma activada no borra la alarma actual. La alarma se desactivará la próxima vez que el atributo cruce el umbral de alarma o se pueda borrar la alarma activada.

Pasos

1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Global Alarms**.
2. En la tabla Alarmas globales personalizadas, haga clic en **Editar** junto a la alarma que desea desactivar.
3. Desactive la casilla de verificación **enabled**.



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

   La alarma Global Custom está desactivada.

Borrar alarmas activadas (sistema heredado)

Si se activa una alarma heredada, puede borrarla en lugar de reconocerla.

Antes de empezar

- Debe tener la `Passwords.txt` archivo.

La desactivación de una alarma para un atributo que actualmente tiene una alarma activada contra él no borra la alarma. La alarma se desactivará la próxima vez que cambie el atributo. Puede reconocer la alarma o, si desea borrar inmediatamente la alarma en lugar de esperar a que cambie el valor del atributo (lo que provoca un cambio en el estado de la alarma), puede borrar la alarma activada. Puede resultarle útil si desea borrar una alarma inmediatamente frente a un atributo cuyo valor no cambia con frecuencia (por ejemplo, atributos de estado).

1. Desactive la alarma.
2. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: *`ssh admin@primary_Admin_Node_IP`*
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

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

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

3. Reinicie el servicio NMS: `service nms restart`
4. Cierre la sesión del nodo de administración: `exit`

La alarma se borra.

Configurar notificaciones para alarmas (sistema heredado)

El sistema StorageGRID puede enviar automáticamente correo electrónico y. "Notificaciones SNMP" cuando se activa una alarma o cambia el estado de servicio.

De forma predeterminada, las notificaciones por correo electrónico de alarma no se envían. Para las notificaciones por correo electrónico, debe configurar el servidor de correo electrónico y especificar los destinatarios de correo electrónico. Para las notificaciones SNMP, debe configurar el agente SNMP.

Tipos de notificaciones de alarma (sistema heredado)

Cuando se activa una alarma heredada, el sistema StorageGRID envía dos tipos de notificaciones de alarma: Nivel de gravedad y estado de servicio.

Notificaciones de nivel de gravedad

Se envía una notificación por correo electrónico de alarma cuando se activa una alarma heredada en un nivel de gravedad seleccionado:

- Aviso
- Menor
- Importante
- Crítico

Una lista de correo recibe todas las notificaciones relacionadas con la alarma para la gravedad seleccionada. También se envía una notificación cuando la alarma sale del nivel de alarma, ya sea solucionándose o introduciendo un nivel de gravedad de alarma diferente.

Notificaciones de estado de servicio

Se envía una notificación de estado de servicio cuando un servicio (por ejemplo, el servicio LDR o el servicio NMS) entra en el estado de servicio seleccionado y cuando sale del estado de servicio seleccionado. Las notificaciones de estado de servicio se envían cuando un servicio entra o deja uno de los siguientes estados de servicio:

- Desconocido
- Administrativamente abajo

Una lista de correo recibe todas las notificaciones relacionadas con los cambios en el estado seleccionado.

Configurar los ajustes del servidor de correo electrónico para las alarmas (sistema heredado)

Si desea que StorageGRID envíe notificaciones por correo electrónico cuando se active una alarma heredada, debe especificar la configuración del servidor de correo SMTP. El sistema StorageGRID solo envía correo electrónico; no puede recibir correo electrónico.

Antes de empezar

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

Acerca de esta tarea

Utilice estos ajustes para definir el servidor SMTP utilizado para las notificaciones de correo electrónico de alarmas antiguas y los mensajes de correo electrónico AutoSupport. Esta configuración no se utiliza para las notificaciones de alerta.

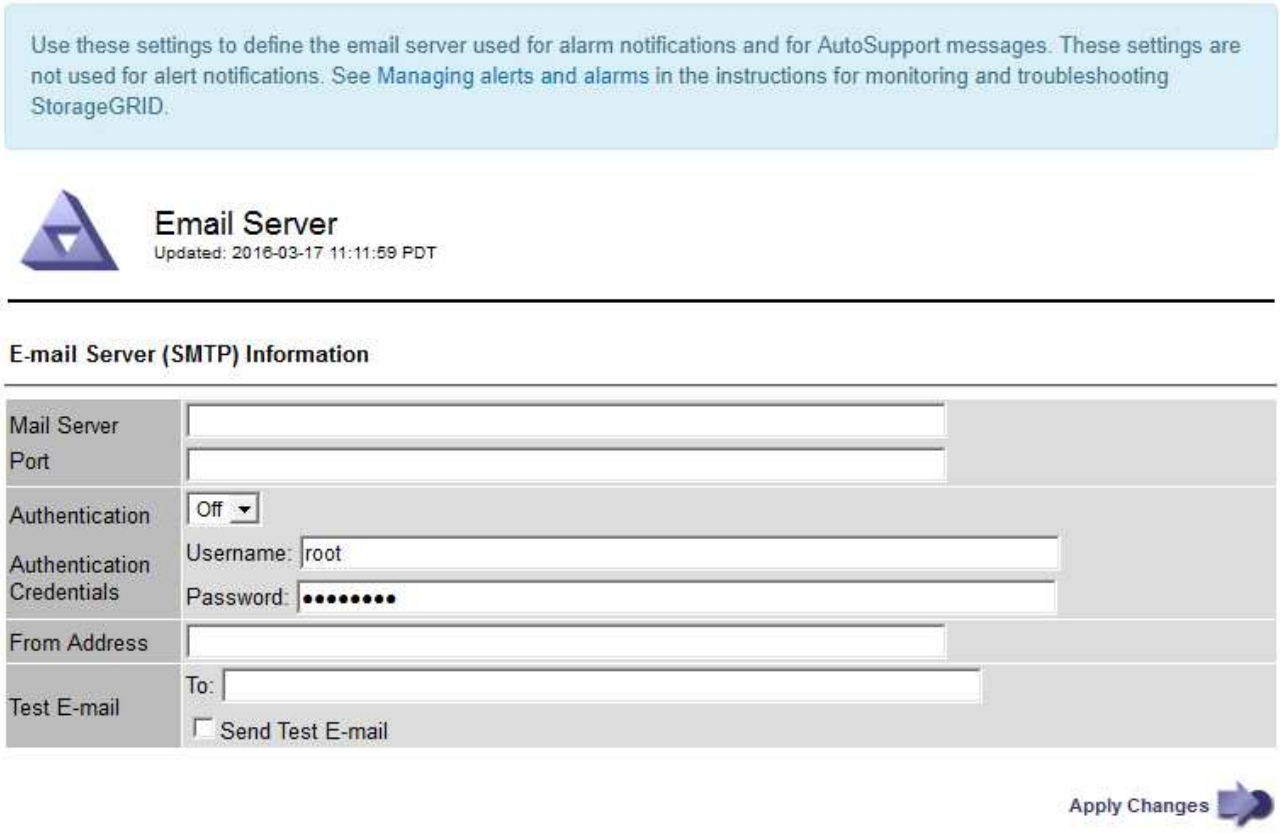
> Si utiliza SMTP como protocolo para paquetes de AutoSupport, es posible que ya haya configurado un servidor de correo SMTP. El mismo servidor SMTP se utiliza para notificaciones de correo electrónico de alarma, por lo que puede omitir este procedimiento. Consulte "Instrucciones para administrar StorageGRID".

SMTP es el único protocolo compatible para enviar correo electrónico.

Pasos

1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Configuración de correo electrónico heredado**.
2. En el menú correo electrónico, seleccione **servidor**.

   Aparece la página servidor de correo electrónico. Esta página también se utiliza para configurar el servidor de correo electrónico para los paquetes AutoSupport.



3. Añada la siguiente configuración del servidor de correo SMTP:

Elemento	Descripción
Servidor de correo	Dirección IP del servidor de correo SMTP. Puede introducir un nombre de host en lugar de una dirección IP si ha configurado previamente los ajustes de DNS en el nodo de administración.
Puerto	Número de puerto para acceder al servidor de correo SMTP.
Autenticación	Permite la autenticación del servidor de correo SMTP. De forma predeterminada, la autenticación está desactivada.
Credenciales de autenticación	Nombre de usuario y contraseña del servidor de correo SMTP. Si autenticación está activada, se debe proporcionar un nombre de usuario y una contraseña para acceder al servidor de correo SMTP.

4. En **Dirección de remitente**, introduzca una dirección de correo electrónico válida que el servidor SMTP reconocerá como la dirección de correo electrónico de envío. Esta es la dirección de correo electrónico oficial desde la que se envía el mensaje de correo electrónico.
5. De manera opcional, envíe un mensaje de correo electrónico de prueba para confirmar que la configuración del servidor de correo SMTP es correcta.
   a. En el cuadro **probar correo electrónico** > **a**, agregue una o más direcciones a las que pueda acceder.

      Puede introducir una sola dirección de correo electrónico o una lista de direcciones de correo

electrónico con comas. Puesto que el servicio NMS no confirma que el mensaje de correo electrónico de prueba se ha enviado correctamente o no se ha realizado correctamente, debe poder comprobar la bandeja de entrada del destinatario de la prueba.

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

6. Haga clic en **aplicar cambios**.

   Se guarda la configuración del servidor de correo SMTP. Si introdujo información para un correo electrónico de prueba, ese correo electrónico se envía. Los correos electrónicos de prueba se envían al servidor de correo inmediatamente y no se envían a través de la cola de notificaciones. En un sistema con varios nodos de administrador, cada nodo de administrador envía un correo electrónico. La recepción del mensaje de correo electrónico de prueba confirma que la configuración del servidor de correo SMTP es correcta y que el servicio NMS se conecta correctamente al servidor de correo. Un problema de conexión entre el servicio NMS y el servidor de correo activa la alarma DE MINUTOS heredados (estado de notificación NMS) en el nivel de gravedad menor.

Crear plantillas de correo electrónico de alarma (sistema heredado)

Las plantillas de correo electrónico le permiten personalizar el encabezado, el pie de página y la línea de asunto de una notificación de correo electrónico de alarma heredada. Puede utilizar plantillas de correo electrónico para enviar notificaciones únicas que contengan el mismo texto principal a distintas listas de correo.

Antes de empezar

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

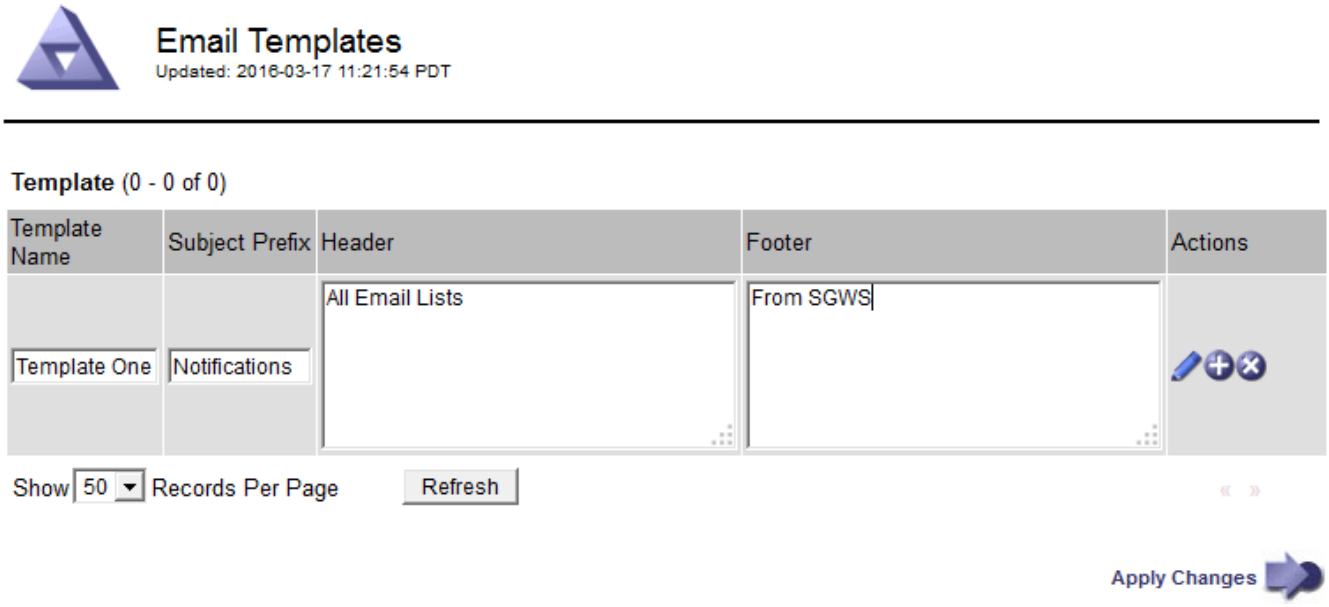
Acerca de esta tarea

Utilice estos ajustes para definir las plantillas de correo electrónico utilizadas para las notificaciones de alarmas heredadas. Esta configuración no se utiliza para las notificaciones de alerta.

Las diferentes listas de correo pueden requerir otra información de contacto. Las plantillas no incluyen el texto del cuerpo del mensaje de correo electrónico.

Pasos

1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Configuración de correo electrónico heredado**.
2. En el menú correo electrónico, seleccione **Plantillas**.
3. Haga clic en **Editar** (O **Insertar** si no es la primera plantilla).



4. En la nueva fila, añada lo siguiente:

Elemento	Descripción
Nombre de plantilla	Nombre exclusivo utilizado para identificar la plantilla. Los nombres de plantilla no se pueden duplicar.
Prefijo de asunto	Opcional. Prefijo que aparecerá al principio de la línea de asunto de un correo electrónico. Los prefijos se pueden utilizar para configurar fácilmente los filtros de correo electrónico y organizar las notificaciones.
Encabezado	Opcional. Texto de encabezado que aparece al principio del cuerpo del mensaje de correo electrónico. El texto de encabezado se puede utilizar para previsualizar el contenido del mensaje de correo electrónico con información como el nombre y la dirección de la empresa.
Pie de página	Opcional. Texto del pie de página que aparece al final del cuerpo del mensaje de correo electrónico. El texto del pie de página se puede utilizar para cerrar el mensaje de correo electrónico con información de recordatorio, como un número de teléfono de contacto o un enlace a un sitio Web.

5. Haga clic en **aplicar cambios**.

   Se agrega una nueva plantilla para notificaciones.

Crear listas de correo para las notificaciones de alarma (sistema heredado)

Las listas de correo le permiten notificar a los destinatarios cuando se activa una alarma heredada o cuando cambia el estado de un servicio. Debe crear al menos una lista de correo para poder enviar notificaciones por correo electrónico de alarma. Para enviar una notificación a un único destinatario, cree una lista de correo con una dirección de correo electrónico.

Antes de empezar

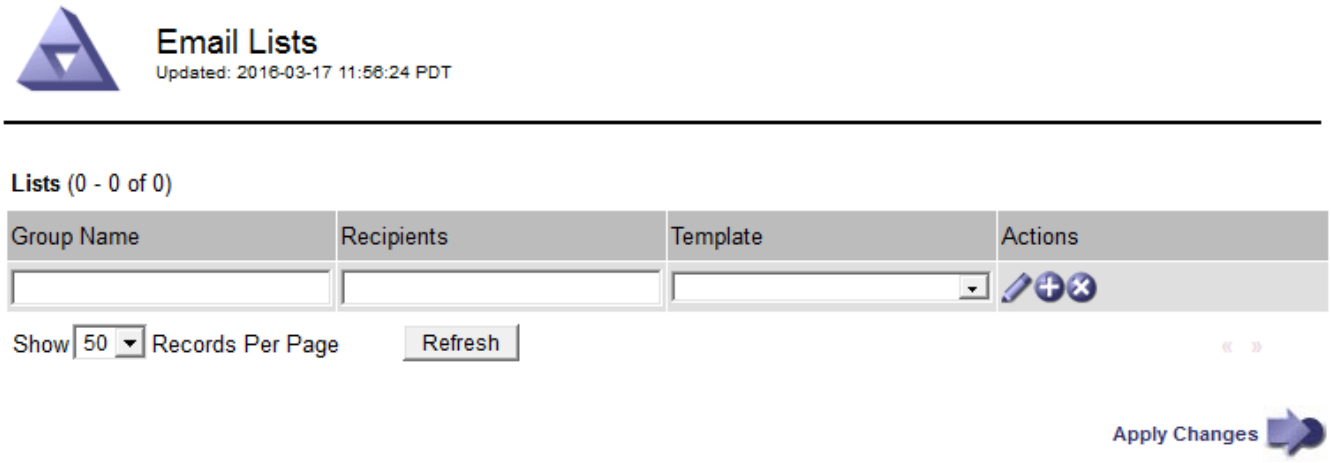
- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Si desea especificar una plantilla de correo electrónico para la lista de correo (encabezado personalizado, pie de página y línea de asunto), debe haber creado la plantilla.

Acerca de esta tarea

Utilice estos ajustes para definir las listas de correo utilizadas para las notificaciones de correo electrónico de alarmas antiguas. Esta configuración no se utiliza para las notificaciones de alerta.

Pasos

1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Configuración de correo electrónico heredado**.
2. En el menú correo electrónico, seleccione **Listas**.
3. Haga clic en **Editar** (O *Insertar* si no es la primera lista de correo).



4. En la nueva fila, añada lo siguiente:

Elemento	Descripción
Nombre del grupo	Nombre único utilizado para identificar la lista de correo. Los nombres de las listas de correo no se pueden duplicar. **Nota:** Si cambia el nombre de una lista de correo, el cambio no se propaga a las otras ubicaciones que utilizan el nombre de la lista de correo. Debe actualizar manualmente todas las notificaciones configuradas para utilizar el nuevo nombre de la lista de correo.
Destinatarios	Una única dirección de correo electrónico, una lista de correo configurada previamente o una lista definida por comas de direcciones de correo electrónico y listas de correo a las que se enviarán notificaciones. **Nota:** Si una dirección de correo electrónico pertenece a varias listas de correo, sólo se envía una notificación por correo electrónico cuando se produce un evento de activación de notificación.

Elemento	Descripción
Plantilla	Opcionalmente, seleccione una plantilla de correo electrónico para agregar un encabezado, pie de página y línea de asunto exclusivos a las notificaciones enviadas a todos los destinatarios de esta lista de correo.

5. Haga clic en **aplicar cambios**.

   Se crea una nueva lista de correo.

Configurar notificaciones de correo electrónico para alarmas (sistema heredado)

Para recibir notificaciones por correo electrónico para el sistema de alarma heredado, los destinatarios deben ser miembros de una lista de correo y esa lista debe añadirse a la página Notificaciones. Las notificaciones se configuran para enviar correo electrónico a los destinatarios sólo cuando se activa una alarma con un nivel de gravedad especificado o cuando cambia el estado de un servicio. Por lo tanto, los destinatarios sólo reciben las notificaciones que necesitan recibir.

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Debe haber configurado una lista de correo electrónico.

Acerca de esta tarea

Utilice estos ajustes para configurar notificaciones de alarmas heredadas. Esta configuración no se utiliza para las notificaciones de alerta.

Si una dirección de correo electrónico (o lista) pertenece a varias listas de correo, sólo se envía una notificación de correo electrónico cuando se produce un evento de activación de notificación. Por ejemplo, se puede configurar un grupo de administradores dentro de la organización para recibir notificaciones de todas las alarmas independientemente de su gravedad. Es posible que otro grupo sólo requiera notificaciones para las alarmas con una gravedad crítica. Puede pertenecer a ambas listas. Si se activa una alarma crítica, solo recibirá una notificación.

Pasos

1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Configuración de correo electrónico heredado**.
2. En el menú correo electrónico, seleccione **Notificaciones**.
3. Haga clic en *Editar* (O *Insertar* si no es la primera notificación).
4. En Lista de correo electrónico, seleccione la lista de correo.
5. Seleccione uno o más niveles de gravedad de alarma y estados de servicio.
6. Haga clic en **aplicar cambios**.

   Las notificaciones se enviarán a la lista de correo cuando se activen o cambien las alarmas con el nivel de gravedad de alarma o el estado de servicio seleccionado.

Suprimir notificaciones de alarma de una lista de correo (sistema heredado)

Puede suprimir las notificaciones de alarma de una lista de correo cuando ya no desee que la lista de correo reciba notificaciones sobre alarmas. Por ejemplo, se recomienda suprimir notificaciones sobre alarmas heredadas después de pasar a utilizar notificaciones por correo electrónico de alerta.

Antes de empezar

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

Utilice esta configuración para suprimir las notificaciones por correo electrónico del sistema de alarmas heredado. Esta configuración no se aplica a las notificaciones por correo electrónico de alertas.

> Aunque el sistema de alarma heredado sigue siendo compatible, el sistema de alerta ofrece importantes ventajas y es más fácil de usar.

Pasos

1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Configuración de correo electrónico heredado**.
2. En el menú correo electrónico, seleccione **Notificaciones**.
3. Haga clic en **Editar** junto a la lista de correo para la que desea suprimir notificaciones.
4. En Suprimir, seleccione la casilla de verificación situada junto a la lista de correo que desea suprimir o seleccione **Suprimir** en la parte superior de la columna para suprimir todas las listas de correo.
5. Haga clic en **aplicar cambios**.

   Las notificaciones de alarmas heredadas se suprimen para las listas de correo seleccionadas.

Ver alarmas heredadas

Las alarmas (sistema heredado) se activan cuando los atributos del sistema alcanzan los valores de umbral de alarma. Puede ver las alarmas activas actualmente desde la página Alarmas actuales.

> Aunque el sistema de alarma heredado sigue siendo compatible, el sistema de alerta ofrece importantes ventajas y es más fácil de usar.

Antes de empezar

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

Pasos

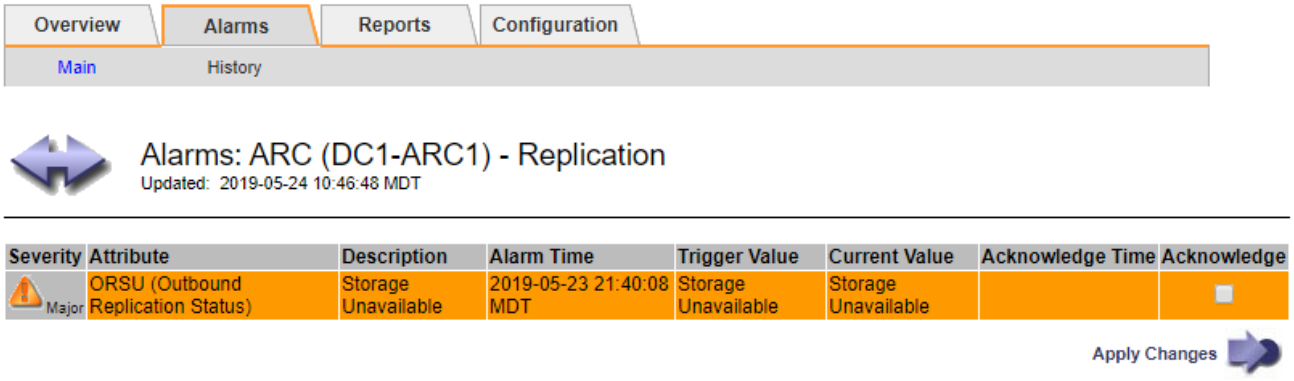
1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Current Alarms**.

El icono de alarma indica la gravedad de cada alarma de la siguiente manera:

.	Color	Gravedad de alarma	Significado
	Amarillo	Aviso	El nodo está conectado a la cuadrícula, pero existe una condición poco habitual que no afecta a las operaciones normales.
	Naranja claro	Menor	El nodo está conectado a la cuadrícula, pero existe una condición anormal que podría afectar al funcionamiento en el futuro. Debe investigar para evitar el escalado.
	Naranja oscuro	Importante	El nodo está conectado a la cuadrícula, pero existe una condición anormal que afecta actualmente al funcionamiento. Esto requiere atención inmediata para evitar un escalado.
	Rojo	Crítico	El nodo está conectado a la cuadrícula, pero existe una condición anormal que ha detenido las operaciones normales. Debe abordar el problema de inmediato.

2. Para obtener información acerca del atributo que provocó la activación de la alarma, haga clic con el botón secundario del ratón en el nombre del atributo de la tabla.
3. Para ver detalles adicionales acerca de una alarma, haga clic en el nombre del servicio en la tabla.

   Aparece la ficha Alarmas para el servicio seleccionado (**SUPPORT** > **Tools** > **Topología de cuadrícula** > ***nodo de cuadrícula*** > ***Servicio*** > **Alarmas**).



4. Si desea borrar el número de alarmas actuales, puede realizar lo siguiente de forma opcional:
   - Reconozca la alarma. Una alarma confirmada ya no se incluye en el recuento de alarmas heredadas, a menos que se active en el siguiente nivel de gravedad o se resuelva y se vuelva a producir.
   - Desactive una alarma predeterminada o Global Custom particular para todo el sistema para evitar que se active de nuevo.

Información relacionada

"Referencia de alarmas (sistema heredado)"

"Confirmar alarmas actuales (sistema heredado)"

"Desactivar alarmas (sistema heredado)"

Referencia de alarmas (sistema heredado)

En la siguiente tabla se enumeran todas las alarmas predeterminadas heredadas. Si se activa una alarma, puede buscar el código de alarma en esta tabla para encontrar las acciones recomendadas.

Aunque el sistema de alarma heredado sigue siendo compatible, el sistema de alerta ofrece importantes ventajas y es más fácil de usar.

Codificación	Nombre	Servicio	Acción recomendada
ABRL	Relés de atributos disponibles	BDC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Restaure la conectividad a un servicio (un servicio ADC) que ejecuta un atributo Lo antes posible. de servicio de retransmisión. Si no hay relés de atributos conectados, el nodo de cuadrícula no puede informar de los valores de atributos al servicio NMS. Por lo tanto, el servicio NMS ya no puede supervisar el estado del servicio ni actualizar los atributos del servicio. Si el problema persiste, póngase en contacto con el soporte técnico.

Codificación	Nombre	Servicio	Acción recomendada
ACMS	Servicios de metadatos disponibles	BARC, BLDR, BCMN	Se activa una alarma cuando un servicio LDR o ARC pierde la conexión con un servicio DDS. Si esto ocurre, las transacciones de procesamiento o recuperación no se pueden procesar. Si la falta de disponibilidad de los servicios de DDS es sólo un breve problema transitorio, las transacciones pueden retrasarse. Compruebe y restaure las conexiones a un servicio DDS para borrar esta alarma y devolver el servicio a su funcionalidad completa.
HECHOS	Estado del servicio de organización en niveles del cloud	ARCO	Solo disponible para nodos de archivado con un tipo objetivo de organización en niveles en cloud: Simple Storage Service (S3). Si el atributo ACTS del nodo de archivado está establecido en Read-only Enabled o Read-Write Disabled, debe establecer el atributo en Read-Write Enabled. Si se activa una alarma principal debido a un fallo de autenticación, compruebe las credenciales asociadas con el bloque de destino y los valores de actualización, si es necesario. Si se activa una alarma importante por cualquier otro motivo, póngase en contacto con el soporte técnico.
ADCA	Estado de ADC	ADC	Si se activa una alarma, seleccione **SOPORTE** > **Herramientas** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **ADC** > **Overview** > **Main** y **ADC** > **Alarms** > **Main** para determinar la causa de la alarma. Si el problema persiste, póngase en contacto con el soporte técnico.
ADCE	Estado ADC	ADC	Si el valor del estado de ADC es en espera, continúe supervisando el servicio y si el problema persiste, póngase en contacto con el soporte técnico. Si el valor de Estado de ADC es sin conexión, reinicie el servicio. Si el problema persiste, póngase en contacto con el soporte técnico.

Codificación	Nombre	Servicio	Acción recomendada
AITE	Recuperar estado	BARC	Sólo disponible para nodos de archivado con un tipo de destino de Tivoli Storage Manager (TSM). Si el valor de Retrieve State está esperando a Target, compruebe el servidor de middleware TSM y asegúrese de que funciona correctamente. Si el nodo de archivado se acaba de agregar al sistema StorageGRID, asegúrese de que la conexión del nodo de archivado con el sistema de almacenamiento de archivado externo objetivo esté configurada correctamente. Si el valor del Estado de recuperación de archivo es sin conexión, intente actualizar el estado a en línea. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuración** > **Principal**, seleccione **Archivo recuperar estado** > **Online** y haga clic en **aplicar cambios**. Si el problema persiste, póngase en contacto con el soporte técnico.
UIT	Recuperar estado	BARC	Si el valor de Estado de recuperación es error de destino, compruebe si el sistema de almacenamiento de archivos externo objetivo presenta errores. Si se pierde el valor del estado de recuperación de archivo, compruebe el sistema de almacenamiento de archivo externo objetivo para asegurarse de que está en línea y funciona correctamente. Compruebe la conexión de red con el destino. Si el valor de Archive Retrieve Status es Unknown error, póngase en contacto con el soporte técnico.
ALIS	Sesiones de atributos entrantes	ADC	Si el número de sesiones de atributos entrantes en un relé de atributos aumenta demasiado, puede ser una indicación de que el sistema StorageGRID se ha desequilibrado. En condiciones normales, las sesiones de atributos deben distribuirse uniformemente entre los servicios ADC. Un desequilibrio puede producir problemas de rendimiento. Si el problema persiste, póngase en contacto con el soporte técnico.
ALOS	Sesiones de atributos salientes	ADC	El servicio ADC tiene un gran número de sesiones de atributos y se está sobrecargando. Si se activa esta alarma, póngase en contacto con el soporte técnico.

Codificación	Nombre	Servicio	Acción recomendada
ALUR	Repositorios de atributos inaccesibles	ADC	Compruebe la conectividad de red con el servicio NMS para asegurarse de que el servicio puede ponerse en contacto con el repositorio de atributos. Si se activa esta alarma y la conectividad de red es buena, póngase en contacto con el servicio técnico.
AQS	Mensajes de auditoría en cola	BDC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Si los mensajes de auditoría no se pueden reenviar inmediatamente a un relé de auditoría o repositorio, los mensajes se almacenan en una cola de discos. Si la cola de discos se llena, pueden producirse interrupciones. Para permitirle responder en tiempo para evitar una interrupción, las alarmas AMQS se activan cuando el número de mensajes en la cola de discos alcanza los siguientes umbrales: • Aviso: Más de 100,000 mensajes • Menor: Al menos 500,000 mensajes • Importante: Al menos 2,000,000 mensajes • Crítico: Al menos 5,000,000 mensajes Si se activa una alarma AMQS, compruebe la carga en el sistema. Si ha habido un número significativo de transacciones, la alarma debe resolverse con el tiempo. En este caso, puede ignorar la alarma. Si la alarma persiste y aumenta su gravedad, vea un gráfico del tamaño de la cola. Si el número aumenta constantemente durante horas o días, es probable que la carga de auditoría haya superado la capacidad de auditoría del sistema. Reduzca la tasa de operaciones del cliente o disminuya el número de mensajes de auditoría registrados cambiando el nivel de auditoría a error o Desactivado. Consulte "Configurar los mensajes de auditoría y los destinos de registro".

Codificación	Nombre	Servicio	Acción recomendada
AOTE	Estado de la tienda	BARC	Sólo disponible para nodos de archivado con un tipo de destino de Tivoli Storage Manager (TSM). Si el valor de Estado de tienda está esperando a Target, compruebe el sistema de almacenamiento de archivos externo y asegúrese de que funciona correctamente. Si el nodo de archivado se acaba de agregar al sistema StorageGRID, asegúrese de que la conexión del nodo de archivado con el sistema de almacenamiento de archivado externo objetivo esté configurada correctamente. Si el valor del estado del almacén es sin conexión, compruebe el valor del estado del almacén. Corrija cualquier problema antes de volver a poner el estado de la tienda en línea.
UOT	Estado de la tienda	BARC	Si el valor del estado del almacén es pérdida de sesión, compruebe que el sistema de almacenamiento de archivos externo está conectado y en línea. Si el valor de Target error (error de destino), compruebe si hay errores en el sistema de almacenamiento de archivos externo. Si el valor de estado de almacén es error desconocido, póngase en contacto con el soporte técnico.
APM	Conectividad de acceso múltiple de almacenamiento	SSM	Si la alarma de estado de acceso múltiple aparece como “Degradado” (seleccione **SUPPORT** > **Tools** > **Grid topology** y, a continuación, seleccione ***SITE*** > ***GRID node*** > **SSM** > **Events**), haga lo siguiente: 1. Conecte o sustituya el cable que no muestre ninguna luz indicadora. 2. Espere de uno a cinco minutos. No desenchufe el otro cable hasta al menos cinco minutos después de enchufar el primero. La desconexión demasiado temprana puede provocar que el volumen raíz pase a ser de solo lectura, lo que requiere reiniciar el hardware. 3. Vuelva a la página **SSM** > **Resources** y compruebe que el estado “Degradado” Multipath ha cambiado a “Nominal” en la sección Hardware de almacenamiento.

Codificación	Nombre	Servicio	Acción recomendada
ARCE	Estado DEL ARCO	ARCO	El servicio ARC tiene un estado de espera hasta que se hayan iniciado todos los componentes ARC (replicación, almacenamiento, recuperación, destino). A continuación, pasa a Online. Si el valor del estado ARC no pasa del modo en espera a en línea, compruebe el estado de los componentes del ARC. Si el valor del estado de ARC es sin conexión, reinicie el servicio. Si el problema persiste, póngase en contacto con el soporte técnico.
ROQ	Objetos en cola	ARCO	Esta alarma se puede activar si el dispositivo de almacenamiento extraíble se está ejecutando lentamente debido a problemas con el sistema de almacenamiento de archivos externo objetivo o si encuentra varios errores de lectura. Compruebe si hay errores en el sistema de almacenamiento de archivos externo y asegúrese de que funciona correctamente. En algunos casos, este error puede producirse como resultado de una alta tasa de solicitudes de datos. Supervise el número de objetos en cola a medida que disminuye la actividad del sistema.

Codificación	Nombre	Servicio	Acción recomendada
ARRF	Fallos de solicitudes	ARCO	Si se produce un error en una recuperación del sistema de almacenamiento de archivado externo objetivo, el nodo de archivado vuelve a intentar la recuperación, ya que el fallo puede deberse a un problema transitorio. Sin embargo, si los datos del objeto están dañados o se han marcado como no disponibles permanentemente, la recuperación no falla. En su lugar, el nodo de archivado vuelve a intentar la recuperación de forma continua y el valor de los fallos de solicitud continúa aumentando. Esta alarma puede indicar que el soporte de almacenamiento que contiene los datos solicitados está dañado. Compruebe el sistema de almacenamiento de archivos externo para diagnosticar el problema. Si determina que los datos del objeto ya no están en el archivado, el objeto tendrá que eliminarse del sistema StorageGRID. Para obtener más información, póngase en contacto con el soporte técnico. Una vez resuelto el problema que activó esta alarma, restablezca el número de fallos. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **Main**, seleccione **Reset Request Failure Count** y haga clic en **Apply Changes**.
ARRV	Errores de verificación	ARCO	Para diagnosticar y corregir este problema, póngase en contacto con el soporte técnico. Una vez solucionado el problema que desencadenó esta alarma, restablezca el recuento de fallos. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **Main**, seleccione **Reset Verification Failure Count** y haga clic en **Apply Changes**.

Codificación	Nombre	Servicio	Acción recomendada
ARVF	Errores de almacenamiento	ARCO	Esta alarma puede producirse como resultado de errores en el sistema de almacenamiento de archivos externo objetivo. Compruebe si hay errores en el sistema de almacenamiento de archivos externo y asegúrese de que funciona correctamente. Una vez resuelto el problema que activó esta alarma, restablezca el número de fallos. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **Main**, seleccione **Reset Store Failure Count** y haga clic en **Apply Changes**.
ASXP	Acciones de auditoría	AMS	Se activa una alarma si el valor de los recursos compartidos de auditoría es Desconocido. Esta alarma puede indicar un problema con la instalación o configuración del nodo de administración. Si el problema persiste, póngase en contacto con el soporte técnico.
AUMA	Estado AMS	AMS	Si el valor de Estado AMS es error de conectividad de BD, reinicie el nodo de cuadrícula. Si el problema persiste, póngase en contacto con el soporte técnico.
AUME	Estado AMS	AMS	Si el valor del estado AMS es Standby, continúe monitorizando el sistema StorageGRID. Si el problema persiste, póngase en contacto con el soporte técnico. Si el valor de Estado AMS es sin conexión, reinicie el servicio. Si el problema persiste, póngase en contacto con el soporte técnico.
AUXS	Estado de exportación de auditoría	AMS	Si se activa una alarma, corrija el problema subyacente y, a continuación, reinicie el servicio AMS. Si el problema persiste, póngase en contacto con el soporte técnico.
BADD	Número de unidades con errores del controlador de almacenamiento	SSM	Esta alarma se activa cuando una o varias unidades de un dispositivo StorageGRID presenta errores o no están en estado óptimo. Sustituya las unidades según sea necesario.

Codificación	Nombre	Servicio	Acción recomendada
BASF	Identificadores de objetos disponibles	CMN	Cuando se aprovisiona un sistema StorageGRID, al servicio CMN se le asigna un número fijo de identificadores de objeto. Esta alarma se activa cuando el sistema StorageGRID comienza a agotar su suministro de identificadores de objetos. Para asignar más identificadores, póngase en contacto con el soporte técnico.
GRAVES	Estado de asignación de bloque de identificador	CMN	De forma predeterminada, se activa una alarma cuando no se pueden asignar identificadores de objeto porque no se puede alcanzar el quórum ADC. La asignación de bloques de identificador en el servicio CMN requiere que haya un quórum (50% + 1) de los servicios ADC conectado y conectado. Si el quórum no está disponible, el servicio CMN no puede asignar nuevos bloques de identificador hasta que se restablezca el quórum ADC. Si se pierde el quórum de ADC, por lo general no se produce un impacto inmediato en el sistema StorageGRID (los clientes todavía pueden procesar y recuperar contenido), ya que el suministro de identificadores de aproximadamente un mes se almacena en caché en otro lugar del grid; Sin embargo, si la condición continúa, el sistema StorageGRID perderá la capacidad para procesar contenido nuevo. Si se activa una alarma, investigue el motivo de la pérdida de quórum de ADC (por ejemplo, puede ser un fallo de red o nodo de almacenamiento) y tome medidas correctivas. Si el problema persiste, póngase en contacto con el soporte técnico.
BRDT	Temperatura del chasis de la controladora de computación	SSM	Se activa una alarma si la temperatura de la controladora de computación en un dispositivo StorageGRID supera un umbral nominal. Compruebe los componentes de hardware y los problemas medioambientales si hay un sobrecalentamiento. Si es necesario, sustituir el componente.

Codificación	Nombre	Servicio	Acción recomendada
BTOF	Desviación	BDC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Se activa una alarma si el tiempo de servicio (segundos) difiere significativamente del tiempo del sistema operativo. En condiciones normales, el servicio deberá volver a resincronizarse. Si el tiempo de servicio se desvía demasiado lejos del tiempo del sistema operativo, el funcionamiento del sistema puede verse afectado. Confirme que el origen de la hora del sistema StorageGRID es correcto. Si el problema persiste, póngase en contacto con el soporte técnico.
BTSE	Estado del reloj	BDC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Se activa una alarma si el tiempo del servicio no está sincronizado con el tiempo de seguimiento del sistema operativo. En condiciones normales, el servicio deberá volver a resincronizarse. Si el tiempo se desvía demasiado lejos del tiempo del sistema operativo, el funcionamiento del sistema puede verse afectado. Confirme que el origen de la hora del sistema StorageGRID es correcto. Si el problema persiste, póngase en contacto con el soporte técnico.
CAHP	Porcentaje de uso de Java Heap	DDS	Se activa una alarma si Java no puede realizar la recolección de basura a una velocidad que permita suficiente espacio de pila para que el sistema funcione correctamente. Una alarma podría indicar una carga de trabajo de usuario que supere los recursos disponibles en todo el sistema para el almacén de metadatos de DDS. Compruebe la actividad de ILM en el panel de control o seleccione **SUPPORT** > **Herramientas** > **Topología de cuadrícula** y, a continuación, seleccione ***SITE*** > ***GRID NODE*** > **DDS** > **Recursos** > **Descripción general** > **Principal**. Si el problema persiste, póngase en contacto con el soporte técnico.

Codificación	Nombre	Servicio	Acción recomendada
CASA	Estado del almacén de datos	DDS	Se genera una alarma si el almacén de metadatos de Cassandra deja de estar disponible. Compruebe el estado de Cassandra: 1. En el nodo de almacenamiento, inicie sesión como admin y. `su` A root utilizando la contraseña que aparece en el archivo Passwords.txtl. 2. Introduzca: `service cassandra status` 3. Si Cassandra no se está ejecutando, reinicie: `service cassandra restart` Esta alarma también puede indicar que el almacén de metadatos (base de datos Cassandra) para un nodo de almacenamiento debe recompilarse. Consulte la información sobre cómo solucionar problemas de los Servicios: Estado - alarma Cassandra (SVST) en "Solucionar problemas de metadatos". Si el problema persiste, póngase en contacto con el soporte técnico.
CASO	Estado del almacén de datos	DDS	Esta alarma se activa durante la instalación o expansión para indicar que un nuevo almacén de datos se está uniendo a la cuadrícula.
CCNA	Hardware de computación	SSM	Esta alarma se activa si el estado del hardware de la controladora de computación en un dispositivo StorageGRID requiere atención.

Codificación	Nombre	Servicio	Acción recomendada
CDLP	Espacio usado de metadatos (porcentaje)	DDS	Esta alarma se activa cuando el espacio efectivo de metadatos (CEMS) alcanza un 70% de lleno (alarma secundaria), un 90% de lleno (alarma principal) y un 100% de lleno (alarma crítica). Si esta alarma alcanza el umbral del 90%, aparecerá una advertencia en el panel de control de Grid Manager. Debe realizar un procedimiento de ampliación para añadir un nuevo Lo antes posible. a los nodos de almacenamiento. Consulte "Expanda una cuadrícula". Si esta alarma alcanza el umbral del 100%, debe detener la incorporación de objetos y añadir nodos de almacenamiento inmediatamente. Cassandra requiere una cierta cantidad de espacio para realizar operaciones esenciales, como la compactación y la reparación. Estas operaciones se verán afectadas si los metadatos de los objetos utilizan más del 100 % del espacio permitido. Pueden producirse resultados no deseados. **Nota**: Póngase en contacto con el servicio de asistencia técnica si no puede agregar nodos de almacenamiento. Una vez que se añaden nodos de almacenamiento nuevos, el sistema reequilibra automáticamente los metadatos de los objetos en todos los nodos de almacenamiento y la alarma se borra. Consulte también información sobre la solución de problemas de la alerta de almacenamiento de metadatos bajos en "Solucionar problemas de metadatos". Si el problema persiste, póngase en contacto con el soporte técnico.

Codificación	Nombre	Servicio	Acción recomendada
CMNA	Estado de CMN	CMN	Si el valor de CMN Status es error, seleccione **SUPPORT** > **Tools** > **Grid topolog** y seleccione ***site*** > ***grid node*** > **CMN** > **Overview** > **Main** y **CMN** > **Alarms** > **Main** para determinar la causa del error y solucionar el problema. Se activa una alarma y el valor de CMN Status es no Online CMN durante una actualización de hardware del nodo de administración principal cuando se cambian los CMN (el valor del estado antiguo de CMN es Standby y el nuevo es Online). Si el problema persiste, póngase en contacto con el soporte técnico.
CPRC	La capacidad restante	NMS	Se activa una alarma si la capacidad restante (número de conexiones disponibles que se pueden abrir a la base de datos NMS) cae por debajo de la gravedad de alarma configurada. Si se activa una alarma, póngase en contacto con el soporte técnico.
CPSA	Suministro de alimentación De la controladora de computación a	SSM	Se activa una alarma si hay un problema con el suministro De alimentación A en el controlador de computación de un dispositivo StorageGRID. Si es necesario, sustituir el componente.
CPSB	Suministro de alimentación B de la controladora de computación	SSM	Se activa una alarma si existe un problema con la alimentación B en el controlador de computación de un dispositivo StorageGRID. Si es necesario, sustituir el componente.
CPUT	Temperatura de CPU de la controladora de computación	SSM	Se activa una alarma si la temperatura de la CPU en la controladora de computación de un dispositivo StorageGRID supera un umbral nominal. Si el nodo de almacenamiento es un dispositivo StorageGRID, el sistema StorageGRID indica que la controladora requiere atención. Compruebe los componentes de hardware y los problemas de entorno si hay un sobrecalentamiento. Si es necesario, sustituir el componente.

Codificación	Nombre	Servicio	Acción recomendada
DNST	Estado de DNS	SSM	Una vez finalizada la instalación, se activa una alarma DNST en el servicio SSM. Una vez configurado el DNS y la nueva información del servidor llega a todos los nodos de la cuadrícula, la alarma se cancela.
ECCD	Se han detectado fragmentos dañados	LDR	Se activa una alarma cuando el proceso de verificación en segundo plano detecta un fragmento con código de borrado dañado. Si se detecta un fragmento dañado, se intenta reconstruir el fragmento. Restablezca los fragmentos dañados detectados y copia los atributos perdidos a cero y monitoréelos para ver si los recuentos vuelven a subir. Si el número aumenta, es posible que haya un problema con el almacenamiento subyacente del nodo de almacenamiento. No se considera ausente una copia de los datos de objetos con código de borrado hasta que el número de fragmentos perdidos o dañados incumpla la tolerancia a fallos del código de borrado; por lo tanto, es posible tener fragmentos dañados y seguir pudiendo recuperar el objeto. Si el problema persiste, póngase en contacto con el soporte técnico.
ECST	Estado de verificación	LDR	Esta alarma indica el estado actual del proceso de verificación en segundo plano para los datos de objetos codificados de borrado en este nodo de almacenamiento. Se activa una alarma importante si hay un error en el proceso de verificación en segundo plano.
FONP	Abra Descriptores de archivo	BDC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	La FONP puede hacerse grande durante la actividad pico. Si no disminuye durante períodos de actividad lenta, póngase en contacto con el soporte técnico.
HSTE	Estado HTTP	LDR	Consulte acciones recomendadas para HSTU.

Codificación	Nombre	Servicio	Acción recomendada
HSTU	Estado HTTP	LDR	HSTE y HSTU están relacionados con HTTP para todo el tráfico LDR, incluido S3, Swift y otro tráfico StorageGRID interno. Una alarma indica que se ha producido una de las siguientes situaciones: • HTTP se ha desconectado manualmente. • Se ha deshabilitado el atributo HTTP de inicio automático. • El servicio LDR se está cerrando. El atributo HTTP de inicio automático está habilitado de forma predeterminada. Si se cambia esta configuración, HTTP podría permanecer sin conexión después de un reinicio. Si es necesario, espere a que el servicio LDR se reinicie. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***Storage Node*** > **LDR** > **Configuración**. Si HTTP está sin conexión, colóquelo en línea. Compruebe que el atributo HTTP de inicio automático está habilitado. Si HTTP sigue sin conexión, póngase en contacto con el soporte técnico.
HTA	HTTP de inicio automático	LDR	Especifica si se deben iniciar los servicios HTTP automáticamente al iniciar. Es una opción de configuración especificada por el usuario.
IRSU	Estado de replicación entrante	BLDR, BARC	Una alarma indica que se ha desactivado la replicación de entrada. Confirmar ajustes de configuración: Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuración** > **Principal**.

Codificación	Nombre	Servicio	Acción recomendada
LATA	Latencia media	NMS	Compruebe si hay problemas de conectividad. Compruebe la actividad del sistema para confirmar que hay un aumento en la actividad del sistema. Un aumento en la actividad del sistema provocará un aumento de la actividad de los datos de atributos. Este aumento de la actividad dará lugar a un retraso en el procesamiento de datos de atributos. Esto puede ser una actividad normal del sistema y se resta. Compruebe si hay varias alarmas. Un aumento en los tiempos de latencia medios se puede indicar mediante un número excesivo de alarmas activadas. Si el problema persiste, póngase en contacto con el soporte técnico.
LDRE	Estado LDR	LDR	Si el valor de LDR State es Standby, continúe supervisando la situación y, si el problema persiste, póngase en contacto con el soporte técnico. Si el valor del estado LDR es sin conexión, reinicie el servicio. Si el problema persiste, póngase en contacto con el soporte técnico.
PERDIDO	Objetos perdidos	DDS, LDR	Se activa cuando el sistema StorageGRID no logra recuperar una copia del objeto solicitado desde cualquier lugar del sistema. Antes de que se active una alarma PERDIDA (objetos perdidos), el sistema intenta recuperar y reemplazar un objeto que falta desde cualquier otro lugar del sistema. Los objetos perdidos representan una pérdida de datos. El atributo objetos perdidos se incrementa siempre que el número de ubicaciones de un objeto caiga a cero sin que el servicio DDS purice el contenido de forma intencionada para satisfacer la política ILM. Investigar inmediatamente las alarmas PERDIDAS (OBJETOS PERDIDOS). Si el problema persiste, póngase en contacto con el soporte técnico. "Solucionar problemas de datos de objetos perdidos o faltantes"

Codificación	Nombre	Servicio	Acción recomendada
MCEP	Caducidad del certificado de la interfaz de gestión	CMN	Se activa cuando el certificado utilizado para acceder a la interfaz de gestión está a punto de expirar. 1. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**. 2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**. 3. "Cargue un nuevo certificado de interfaz de gestión."
MINQ	Notificaciones de correo electrónico en cola	NMS	Compruebe las conexiones de red de los servidores que alojan el servicio NMS y el servidor de correo externo. Confirme también que la configuración del servidor de correo electrónico sea correcta. "Configurar los ajustes del servidor de correo electrónico para las alarmas (sistema heredado)"
MIN	Estado de las notificaciones por correo electrónico	BNMS	Se activa una alarma menor si el servicio NMS no puede conectarse al servidor de correo. Compruebe las conexiones de red de los servidores que alojan el servicio NMS y el servidor de correo externo. Confirme también que la configuración del servidor de correo electrónico sea correcta. "Configurar los ajustes del servidor de correo electrónico para las alarmas (sistema heredado)"
SRA.	Estado del motor de la interfaz NMS	BNMS	Se activa una alarma si el motor de interfaz NMS del nodo de administración que recopila y genera contenido de interfaz se desconecta del sistema. Compruebe el Administrador del servidor para determinar si la aplicación individual del servidor está inactiva.
NANG	Configuración de negociación automática de red	SSM	Compruebe la configuración del adaptador de red. La configuración debe coincidir con las preferencias de los routers y switches de red. Un ajuste incorrecto puede tener un impacto grave en el rendimiento del sistema.
NDUP	Configuración dúplex de red	SSM	Compruebe la configuración del adaptador de red. La configuración debe coincidir con las preferencias de los routers y switches de red. Un ajuste incorrecto puede tener un impacto grave en el rendimiento del sistema.

Codificación	Nombre	Servicio	Acción recomendada
NLNK	Detección de enlace de red	SSM	Compruebe las conexiones de los cables de red en el puerto y en el conmutador. Compruebe las configuraciones del router de red, del switch y del adaptador. Reinicie el servidor. Si el problema persiste, póngase en contacto con el soporte técnico.
NRER	Recibir errores	SSM	Las siguientes pueden ser las causas de las alarmas NRER: • La corrección de errores de avance (FEC) no coincide • Discrepancia entre el puerto del switch y la MTU de NIC • Índices altos de errores de enlace • Desbordamiento del búfer de anillo NIC Consulte la información sobre cómo solucionar problemas de la alarma error de recepción de red (NRER) en "Solucionar problemas de red, hardware y plataforma".
NRLY	Relés de auditoría disponibles	BDC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Si los relés de auditoría no están conectados a los servicios ADC, los eventos de auditoría no se pueden informar. Los usuarios se ponen en cola y no están disponibles hasta que se restaura la conexión. Restaure la conectividad a un Lo antes posible. de servicio de ADC. Si el problema persiste, póngase en contacto con el soporte técnico.
SCA	Estado de NMS	NMS	Si el valor de Estado de NMS es error de conectividad de BD, reinicie el servicio. Si el problema persiste, póngase en contacto con el soporte técnico.
NSCE	Estado de NMS	NMS	Si el valor del estado de NMS es en espera, continúe la monitorización y si el problema persiste, póngase en contacto con el servicio técnico. Si el valor de NMS State es Offline, reinicie el servicio. Si el problema persiste, póngase en contacto con el soporte técnico.

Codificación	Nombre	Servicio	Acción recomendada
NSPD	Velocidad	SSM	Esto puede deberse a problemas de conectividad de red o de compatibilidad de controladores. Si el problema persiste, póngase en contacto con el soporte técnico.
NBR	Tablespace gratis	NMS	Si se activa una alarma, compruebe la rapidez con la que ha cambiado el uso de la base de datos. Una caída repentina (a diferencia de un cambio gradual a lo largo del tiempo) indica una condición de error. Si el problema persiste, póngase en contacto con el soporte técnico. El ajuste del umbral de alarma permite gestionar de manera proactiva cuándo se debe asignar más almacenamiento. Si el espacio disponible alcanza un umbral bajo (consulte umbral de alarma), póngase en contacto con el soporte técnico para cambiar la asignación de la base de datos.
NTER	Errores de transmisión	SSM	Estos errores se pueden borrar sin que se restablezcan manualmente. Si no se borran, compruebe el hardware de la red. Compruebe que el hardware y el controlador del adaptador están correctamente instalados y configurados para funcionar con los routers y switches de la red. Cuando se resuelva el problema subyacente, restablezca el contador. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **SSM** > **Recursos** > **Configuración** > **Principal**, seleccione **Restablecer recuento de errores de transmisión** y haga clic en **aplicar cambios**.
NTFQ	Compensación de frecuencia NTP	SSM	Si el desvío de frecuencia supera el umbral configurado, es probable que haya un problema de hardware con el reloj local. Si el problema persiste, póngase en contacto con el soporte técnico para arreglar un reemplazo.
NTLK	Bloqueo NTP	SSM	Si el daemon NTP no está bloqueado en una fuente de hora externa, compruebe la conectividad de red con los orígenes de tiempo externos designados, su disponibilidad y su estabilidad.

Codificación	Nombre	Servicio	Acción recomendada
NOTF	Ajuste de tiempo NTP	SSM	Si el desfase de tiempo supera el umbral configurado, es probable que haya un problema de hardware con el oscilador del reloj local. Si el problema persiste, póngase en contacto con el soporte técnico para arreglar un reemplazo.
NTSJ	Variación de origen de tiempo seleccionada	SSM	Este valor indica la fiabilidad y estabilidad del origen de tiempo que NTP utiliza en el servidor local como referencia. Si se activa una alarma, puede ser una indicación de que el oscilador de la fuente de tiempo está defectuoso, o de que hay un problema con el enlace WAN al origen de tiempo.
NTSU	Estado de NTP	SSM	Si el valor del estado de NTP no está en ejecución, póngase en contacto con el soporte técnico.
OPST	Estado general de la alimentación	SSM	Se activa una alarma si la alimentación de un dispositivo StorageGRID se desvía del voltaje de funcionamiento recomendado. Compruebe el estado de la fuente de alimentación A o B para determinar qué fuente de alimentación funciona de forma anormal. Si es necesario, sustituya la fuente de alimentación.
OQRT	Objetos en cuarentena	LDR	Una vez que el sistema StorageGRID restaura automáticamente los objetos, los objetos en cuarentena se pueden quitar del directorio de cuarentena. 1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. 2. Seleccione **sitio** > **nodo de almacenamiento** > **LDR** > **verificación** > **Configuración** > **Principal**. 3. Seleccione **Eliminar objetos en cuarentena**. 4. Haga clic en **aplicar cambios**. Los objetos en cuarentena se eliminan y el recuento se restablece a cero.

Codificación	Nombre	Servicio	Acción recomendada
ORSU	Estado de replicación saliente	BLDR, BARC	Una alarma indica que la replicación saliente no es posible: El almacenamiento está en un estado en el que los objetos no se pueden recuperar. Se activa una alarma si la replicación saliente se desactiva manualmente. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuración**. Se activa una alarma si el servicio LDR no está disponible para la replicación. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **LDR** > **almacenamiento**.
OSLF	Estado de la bandeja	SSM	Se activa una alarma si el estado de uno de los componentes de la bandeja de almacenamiento de un dispositivo de almacenamiento está degradado. Los componentes de la bandeja de almacenamiento incluyen los IOM, los ventiladores, los suministros de alimentación y los cajones de unidades.Si esta alarma se activa, consulte las instrucciones de mantenimiento del dispositivo.
PMEM	Uso de memoria de servicio (porcentaje)	BDC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Puede tener un valor superior al y% de RAM, donde y representa el porcentaje de memoria que utiliza el servidor. Las cifras por debajo del 80% son normales. Más del 90% se considera un problema. Si el uso de la memoria es elevado para un único servicio, supervise la situación e investigue. Si el problema persiste, póngase en contacto con el soporte técnico.
PSA	Estado del suministro de alimentación de	SSM	Se activa una alarma si la fuente De alimentación A de un dispositivo StorageGRID se desvía del voltaje de funcionamiento recomendado. Si es necesario, sustituya la fuente de alimentación A.
PSBS	Estado de la fuente de alimentación B	SSM	Se activa una alarma si la fuente de alimentación B de un dispositivo StorageGRID se desvía del voltaje de funcionamiento recomendado. Si es necesario, sustituya la fuente de alimentación B.

Codificación	Nombre	Servicio	Acción recomendada
RDTE	Estado de Tivoli Storage Manager	BARC	Sólo disponible para nodos de archivado con un tipo de destino de Tivoli Storage Manager (TSM). Si el valor de Estado de Tivoli Storage Manager es sin conexión, compruebe el estado de Tivoli Storage Manager y resuelva cualquier problema. Vuelva a conectar el componente. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **ARC** > **Target** > **Configuration** > **Main**, seleccione **Tivoli Storage Manager State** > **Online** y haga clic en **Apply Changes**.
RDTU	Estado de Tivoli Storage Manager	BARC	Sólo disponible para nodos de archivado con un tipo de destino de Tivoli Storage Manager (TSM). Si el valor de Estado de Tivoli Storage Manager es error de configuración y el nodo de archivado se acaba de agregar al sistema StorageGRID, asegúrese de que el servidor de middleware TSM está configurado correctamente. Si el valor de Estado de Tivoli Storage Manager es error de conexión o error de conexión, Retraer, comprobar la configuración de red en el servidor de middleware TSM y la conexión de red entre el servidor de middleware TSM y el sistema StorageGRID. Si el valor de Estado de Tivoli Storage Manager es Fallo de autenticación o Fallo de autenticación, Reconexión, el sistema StorageGRID puede conectarse al servidor de middleware TSM, pero no puede autenticar la conexión. Compruebe que el servidor de middleware TSM está configurado con el usuario, la contraseña y los permisos correctos y reinicie el servicio. Si el valor de Estado de Tivoli Storage Manager es error de sesión, se ha perdido inesperadamente una sesión establecida. Compruebe la conexión de red entre el servidor de middleware TSM y el sistema StorageGRID. Compruebe si hay errores en el servidor de middleware. Si el valor de Estado de Tivoli Storage Manager es error desconocido, póngase en contacto con el soporte técnico.

Codificación	Nombre	Servicio	Acción recomendada
RIRF	Replicaciones entrantes — no se han podido realizar	BLDR, BARC	Se puede producir una alarma de réplicas entrantes — fallo durante periodos de altas cargas o interrupciones temporales de la red. Una vez que la actividad del sistema se reduce, esta alarma debe eliminarse. Si el número de repeticiones fallidas continúa aumentando, busque problemas de red y compruebe que los servicios LDR y ARC de origen y destino están en línea y disponibles. Para restablecer el recuento, seleccione **SUPPORT** > **Tools** > **Grid topolog** y, a continuación, seleccione ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **Main**. Seleccione **Restablecer recuento de fallos de replicación entrante** y haga clic en **aplicar cambios**.
RIRQ	Replicaciones entrantes — en cola	BLDR, BARC	Las alarmas pueden producirse durante períodos de carga alta o interrupción temporal de la red. Una vez que la actividad del sistema se reduce, esta alarma debe eliminarse. Si el recuento de réplicas en cola continúa aumentando, busque problemas de red y compruebe que los servicios LDR y ARC de origen y destino están en línea y disponibles.
RORQ	Replicaciones salientes — en cola	BLDR, BARC	La cola de replicación saliente contiene datos de objeto que se copian para cumplir las reglas de ILM y los objetos solicitados por los clientes. Una alarma puede ocurrir como resultado de una sobrecarga del sistema. Espere a ver si la alarma se borra cuando disminuye la actividad del sistema. Si la alarma vuelve a producirse, añada capacidad añadiendo nodos de almacenamiento.
VICEPRESIDENTE	Espacio útil total (porcentaje)	LDR	Si el espacio útil alcanza un umbral bajo, las opciones incluyen expandir el sistema StorageGRID o mover datos de objeto para archivar a través de un nodo de archivado.

Codificación	Nombre	Servicio	Acción recomendada
CA	Estado	CMN	Si el valor de Estado de la tarea de cuadrícula activa es error, busque el mensaje de tarea de cuadrícula. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **CMN** > **Grid Tasks** > **Overview** > **Main**. El mensaje de tarea de cuadrícula muestra información sobre el error (por ejemplo, “check failed on node 12130011”). Después de investigar y corregir el problema, reinicie la tarea de cuadrícula. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **CMN** > **Grid Tasks** > **Configuration** > **Main** y seleccione **Actions** > **Run**. Si el valor de Estado de una tarea de cuadrícula que se está deteniendo es Error, vuelva a intentar finalizar la tarea de cuadrícula. Si el problema persiste, póngase en contacto con el soporte técnico.
SCEP	Storage API Service finaliza la caducidad del certificado	CMN	Se desencadena cuando el certificado utilizado para acceder a extremos de API de almacenamiento está a punto de expirar. 1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**. 2. En la ficha **Global**, seleccione **S3 y Swift API Certificate**. 3. "Cargue un nuevo certificado API S3 y Swift."
SCHR	Estado	CMN	Si se cancela el valor de Estado de la tarea de cuadrícula histórica, investigue el motivo y vuelva a ejecutar la tarea si es necesario. Si el problema persiste, póngase en contacto con el soporte técnico.
SCSA	Controladora de almacenamiento A	SSM	Se activa una alarma si hay un problema con la controladora A de almacenamiento en un dispositivo StorageGRID. Si es necesario, sustituir el componente.

Codificación	Nombre	Servicio	Acción recomendada
SCSB	Controladora de almacenamiento B	SSM	Se activa una alarma si hay un problema con la controladora B de almacenamiento en un dispositivo StorageGRID. Si es necesario, sustituir el componente. Algunos modelos de dispositivos no tienen una controladora de almacenamiento B.
SHLH	Salud	LDR	Si el valor de Estado de un almacén de objetos es error, compruebe y corrija: • problemas con el volumen que se está montando • errores del sistema de archivos
SLSA	Promedio de carga de CPU	SSM	Cuanto mayor sea el valor, mayor será el número de bus del sistema. Si la media de carga de la CPU persiste en un valor alto, se debe investigar el número de transacciones del sistema para determinar si esto se debe a una carga pesada en ese momento. Vea un gráfico del promedio de carga de CPU: Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **SSM** > **Recursos** > **Informes** > **Cartas**. Si la carga del sistema no es pesada y el problema persiste, póngase en contacto con el soporte técnico.
SMST	Estado del monitor de registro	SSM	Si el valor de Estado del Monitor de registro no está conectado durante un período de tiempo persistente, póngase en contacto con el soporte técnico.

Codificación	Nombre	Servicio	Acción recomendada
SMTT	Total de eventos	SSM	Si el valor total de eventos es mayor que cero, compruebe si hay eventos conocidos (como errores de red) que puedan ser la causa. A menos que se hayan borrado estos errores (es decir, el recuento se ha restablecido a 0), se pueden activar las alarmas de eventos totales. Cuando se resuelve un problema, restablezca el contador para borrar la alarma. Seleccione **NODES** > ***site*** > ***grid node*** > **Eventos** > **Restablecer recuentos de eventos**. Para restablecer los recuentos de eventos, debe tener el permiso de configuración de la página de topología de cuadrícula. Si el valor total de eventos es cero o el número aumenta y el problema persiste, póngase en contacto con el soporte técnico.
SNST	Estado	CMN	Una alarma indica que hay un problema al almacenar los paquetes de tareas de la cuadrícula. Si el valor de Estado es error de punto de comprobación o quórum no alcanzado, confirme que la mayoría de los servicios de ADC están conectados al sistema StorageGRID (50% más uno) y espere unos minutos. Si el problema persiste, póngase en contacto con el soporte técnico.
SEDA	Estado del sistema operativo de almacenamiento	SSM	Se activa una alarma si SANtricity OS indica que hay un problema que requiere atención con un componente de un dispositivo StorageGRID. Selecciona **NODOS**. A continuación, seleccione **Appliance Storage Node** > **hardware**. Desplácese hacia abajo para ver el estado de cada componente. En SANtricity OS, compruebe otros componentes del dispositivo para aislar el problema.
SSMA	Estado del SSM	SSM	Si el valor del estado del SSM es error, seleccione **SUPPORT** > **Tools** > **Grid topolog** y seleccione ***site*** > ***grid node*** > **SSM** > **Overview** > **Main** y **SSM** > **Overview** > **Alarms** para determinar la causa de la alarma. Si el problema persiste, póngase en contacto con el soporte técnico.

Codificación	Nombre	Servicio	Acción recomendada
SSME	Estado de SSM	SSM	Si el valor del estado del SSM es en espera, continúe la monitorización y si el problema persiste, póngase en contacto con el servicio técnico. Si el valor de Estado de SSM es Fuera de línea, reinicie el servicio. Si el problema persiste, póngase en contacto con el soporte técnico.
SST	Estado del almacenamiento	LDR	Si el valor del Estado de almacenamiento es espacio útil insuficiente, no hay más almacenamiento disponible en el nodo de almacenamiento y los ingestos datos se redirigen a otro nodo de almacenamiento disponible. Las solicitudes de recuperación pueden seguir suministrándose desde este nodo de grid. Debe añadirse almacenamiento adicional. No afecta al funcionamiento del usuario final, pero la alarma permanece hasta que se añade almacenamiento adicional. Si el valor del estado del almacenamiento es volúmenes no disponibles, una parte del almacenamiento no está disponible. No es posible almacenar ni recuperar datos de estos volúmenes. Compruebe el estado del volumen para obtener más información: Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **LDR** > **Storage** > **Overview** > **Main**. El estado del volumen se enumera en almacenes de objetos. Si el valor del estado del almacenamiento es error, póngase en contacto con el soporte técnico. "Solucione los problemas de la alarma de estado de almacenamiento (SST)"

Codificación	Nombre	Servicio	Acción recomendada
VST DE NETAPP	Estado	SSM	Esta alarma se borra cuando se resuelven otras alarmas relacionadas con un servicio no en ejecución. Realice un seguimiento de las alarmas del servicio de origen para restaurar la operación. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **SSM** > **Servicios** > **Descripción general** > **Principal**. Cuando el estado de un servicio se muestra como no se está ejecutando, su estado es administrativamente inactivo. El estado del servicio puede aparecer como no en ejecución por los siguientes motivos: • El servicio se ha detenido manualmente (`/etc/init.d/<service\> stop`). • Hay un problema con la base de datos de MySQL y Server Manager cierra EL servicio MI. • Se añadió un nodo de cuadrícula, pero no se inició. • Durante la instalación, un nodo de grid aún no se ha conectado al nodo de administrador. Si un servicio aparece como no en ejecución, reinicie el servicio (`/etc/init.d/<service\> restart`). Esta alarma también puede indicar que el almacén de metadatos (base de datos Cassandra) para un nodo de almacenamiento debe recompilarse. Si el problema persiste, póngase en contacto con el soporte técnico. "Solucione los problemas de la alarma Servicios: Estado - Cassandra (SVST)"
TMEM	Memoria instalada	SSM	Los nodos que se ejecutan con menos de 24 GIB de memoria instalada pueden provocar problemas de rendimiento e inestabilidad del sistema. La cantidad de memoria instalada en el sistema debe aumentarse a al menos 24 GIB.
TPOP	Operaciones pendientes	ADC	Una cola de mensajes puede indicar que el servicio ADC está sobrecargado. Se pueden conectar muy pocos servicios ADC al sistema StorageGRID. En una puesta en marcha de gran tamaño, el servicio de ADC puede requerir la adición de recursos computacionales o el sistema puede requerir servicios de ADC adicionales.

Codificación	Nombre	Servicio	Acción recomendada
UMEM	Memoria disponible	SSM	Si la RAM disponible es baja, determine si se trata de un problema de hardware o software. Si no se trata de un problema de hardware, o si la memoria disponible cae por debajo de los 50 MB (el umbral de alarma predeterminado), póngase en contacto con el soporte técnico.
VMFI	Entradas disponibles	SSM	Esto indica que se requiere almacenamiento adicional. Póngase en contacto con el soporte técnico.
VMFR	Espacio disponible	SSM	Si el valor de espacio disponible es demasiado bajo (consulte umbrales de alarma), debe investigarse si hay archivos de registro que crecen desproporcionalmente o si los objetos ocupan demasiado espacio en disco (consulte umbrales de alarma) que se deben reducir o eliminar. Si el problema persiste, póngase en contacto con el soporte técnico.
VMST	Estado	SSM	Se activa una alarma si el valor de Estado del volumen montado es Desconocido. Un valor de Unknown o Sin conexión puede indicar que no se puede montar o acceder al volumen debido a un problema con el dispositivo de almacenamiento subyacente.
VPRI	Prioridad de verificación	BLDR, BARC	De forma predeterminada, el valor de prioridad de verificación es adaptable. Si la prioridad de verificación está establecida en Alta, se activa una alarma porque la verificación del almacenamiento puede ralentizar las operaciones normales del servicio.
VSTU	Estado de verificación de objetos	LDR	Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***site*** > ***grid node*** > **LDR** > **Storage** > **Overview** > **Main**. Compruebe si hay signos de errores en el sistema de archivos o en el dispositivo de bloqueo. Si el valor de Estado de verificación de objetos es error desconocido, normalmente indica un problema de hardware o del sistema de archivos de bajo nivel (error de E/S) que impide que la tarea verificación de almacenamiento acceda al contenido almacenado. Póngase en contacto con el soporte técnico.

Codificación	Nombre	Servicio	Acción recomendada
XAMS	Repositorios de auditoría inalcanzables	BDC, BARC, BCLB, BCMN, BLDR, BNMS	Compruebe la conectividad de red al servidor que aloja el nodo de administración. Si el problema persiste, póngase en contacto con el soporte técnico.

Referencia de archivos de registro

Referencia de archivos de registro: Descripción general

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"
- "Registros del software de terceros"
- "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 varios nodos como archivo de registro único. O bien, si el nodo de administrador principal no está disponible o no puede conectarse a un nodo específico, puede acceder a los archivos de registro individuales de cada nodo de grid las siguientes formas:

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

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).
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 generales de la cuadrícula, incluida la depuración (`bycast.log`) y. `servermanager` registros.
grid.xml	Archivo de configuración de grid compartido en todos los nodos.
regatroups	Métricas y registros de grupos de alta disponibilidad.
instale	`Gdu-server` e instalar los registros.
lumberjack.log	Depurar mensajes relacionados con la colección de registros.
Árbitro lambda	Registros relacionados con la solicitud de proxy de S3 Select.
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	Archivos y registros de configuración de federación de grid y equilibrador de carga.
ntp	Registros y archivo de configuración NTP.

Ubicación del archivo	Descripción
so	Archivos de estado de nodo y de grid, incluidos los servicios `pid`.
otros	Archivos de registro en `/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 y listas de permiso/denegación de alarma utilizadas 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.

Registros del software StorageGRID

Los registros de StorageGRID se pueden usar para solucionar problemas.

> Si desea enviar los registros a un servidor de syslog externo o cambiar el destino de información de auditoría, como el `bycast.log` y.. `nms.log`, consulte "Configurar los mensajes de auditoría y los destinos de registro".

Registros de StorageGRID generales

Nombre de archivo	Notas	Encontrado en
/var/local/log/bycast.log	El archivo principal de solución de problemas de StorageGRID. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***Site*** > ***Node*** > **SSM** > **Eventos**.	Todos los nodos

Nombre de archivo	Notas	Encontrado en
/var/local/log/bycast-err.log	Contiene un subconjunto de `bycast.log` (Mensajes con ERROR grave Y CRÍTICO). Los mensajes CRÍTICOS también se muestran en el sistema. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***Site*** > ***Node*** > **SSM** > **Eventos**.	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 subprocesos. **Nota**: El archivo `` `/var/local/core/kexec_cmd `` normalmente 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	• Captura las notificaciones de Grid Manager y del arrendatario Manager. • Captura eventos relacionados con el funcionamiento del servicio NMS, por ejemplo, el procesamiento de alarmas, notificaciones de 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	Contiene mensajes de error relacionados con las actualizaciones de la base de datos de MySQL. 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 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

Nombre de archivo	Notas	Encontrado en
/Var/local/log/GridstatBackend.errlog	Archivo de registro para la aplicación de back-end GUI de Server Manager.	Todos los nodos
/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/arc.errlog		Nodos de archivado
/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

Nombre de archivo	Notas	Encontrado en
/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
/var/local/log/cts.errlog	Este archivo de registro sólo se crea si el tipo de destino es **Cloud Tiering - simple Storage Service (S3).**	Nodos de archivado
/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

Nombre de archivo	Notas	Encontrado en
/var/local/log/lambda*	Contiene registros del servicio S3 Select.	Nodos de administración y puerta de enlace Solo algunos nodos Admin y Gateway contienen este registro. Consulte "S3 Select requisitos y limitaciones para los nodos de administración y puerta de enlace".
/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

Nombre de archivo	Notas	Encontrado en
/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 al servicio Load Balancer, que proporciona el equilibrio de carga de S3 y tráfico Swift 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
/var/local/log/prometheus.log	Para todos los nodos, contiene el registro de servicio del exportador de nodos y el registro del servicio de métricas del exportador de nodos. Para los nodos de administrador, también contiene registros de los servicios Prometheus y Alert Manager.	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

Nombre de archivo	Notas	Encontrado en
/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	Se ha creado al ejecutar el `pa-move.sh` guión.	Nodo de administrador principal
/var/local/log/pa-move-new_pa.log	Se ha creado al ejecutar el `pa-move.sh` guión.	Nodo de administrador principal
/var/local/log/pa-move-old_pa.log	Se ha creado al ejecutar el `pa-move.sh` guión.	Nodo de administrador principal

Nombre de archivo	Notas	Encontrado en
/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.	Nodo de administrador principal
/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

Registros del software de terceros

Puede utilizar los registros de software de terceros para solucionar problemas.

Categoría	Nombre de archivo	Notas	Encontrado en
Archivado	/var/local/log/dsierror.log	Información de errores para las API de TSM Client.	Nodos de archivado
MySQL	/var/local/log/mysql.err /var/local/log/mysql-slow.log	Archivos de registro generados por MySQL. `mysql.err` captura los errores y eventos de la base de datos, como startups y apagados. `mysql-slow.log` (El registro de consulta lento) captura las sentencias SQL que tardaron más de 10 segundos en ejecutarse.	Nodos de administración
De NetApp	/var/local/log/messages	Este directorio contiene archivos de registro para el sistema operativo. Los errores contenidos en estos registros también se muestran en Grid Manager. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione **Topología** > ***Site*** > ***Node*** > **SSM** > **Eventos**.	Todos los nodos

Categoría	Nombre de archivo	Notas	Encontrado en
NTP	/var/local/log/ntp.log /var/lib/ntp/var/log/ntpstats/	`/var/local/log/ntp.log` Contiene el archivo de registro de los mensajes de error de NTP. `/var/lib/ntp/var/log/ntpstats/` el directorio contiene estadísticas de sincronización NTP. `loopstats` registra información de estadísticas de filtro de bucle. `peerstats` registra la información de estadísticas del mismo nivel.	Todos los nodos

Acerca de bycast.log

El archivo `/var/local/log/bycast.log` Es el archivo principal de solución de problemas del software StorageGRID. Hay una `bycast.log` archivo para cada nodo de grid. El archivo contiene mensajes específicos de ese nodo de cuadrícula.

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

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. Consulte "Configurar los mensajes de auditoría y los destinos de registro".

Rotación de archivos para bycast.log

Cuando la `bycast.log` El archivo alcanza 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 1 GB `bycast.log.1` se cambia el nombre y se comprime para convertirse `bycast.log.2.gz`, y. `bycast.log` se cambia el nombre `bycast.log.1`.

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

El límite de rotación para `bycast-err.log` hay 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.

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. Consulte "Configurar los mensajes de

auditoría y los destinos de registro".

Información relacionada

"Recopilar archivos de registro y datos del sistema"

Mensajes en bycast.log

Mensajes en `bycast.log` Son escritos por el ADE (Ambiente 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
Hora del sistema UTC	2019-05-05T27T17:10:29.784677 (YYYYY-MM-DDTHH:MM:SS.UUUUUUUUUU)
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 de `bycast.log` se asignan 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. Los mensajes críticos también se muestran en Grid Manager. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione **Sitio** > **nodo** > **SSM** > **Eventos**.

códigos de error en `bycast.log`

La mayoría de los mensajes de error de `bycast.log` contiene códigos de error.

La siguiente tabla enumera los códigos no numéricos comunes en `bycast.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
VERS	Versión
CONF	Configuración
ERROR	Error
ICPL	Incompleto
LISTO	Listo
SVNU	Servicio no disponible

En la siguiente tabla se enumeran los códigos de error numéricos de `bycast.log`.

Número de error	Código de error	Significado
001	EPERM	Operación no permitida

Número de error	Código de error	Significado
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
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

Número de error	Código de error	Significado
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
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

Número de error	Código de error	Significado
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
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

Número de error	Código de error	Significado
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
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

Número de error	Código de error	Significado
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	EPROTORTOLPE	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
097	AFNOSTUPPORT	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

Número de error	Código de error	Significado
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		
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

Número de error	Código de error	Significado
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

Configure los destinos de los mensajes de auditoría y los registros

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, hasta 20 GB de registros locales de registros de auditoría (`localaudit.log`) se mantienen en cada nodo.

Cómo configurar un servidor de syslog externo

Para obtener información sobre cómo configurar un servidor de syslog externo, consulte "Configure los mensajes de auditoría y el servidor de 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 los registros de auditoría, las variables adicionales más importantes son el porcentaje de operaciones de S3 que se colocan (vs OBTIENE) y el tamaño medio, en bytes, de los siguientes campos S3 (las abreviaturas de 4 caracteres que se utilizan en la tabla son nombres de campos del 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.
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 ≤ P ≤ 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-8fbd-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):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

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 deberá manejar 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. En los registros de aplicaciones, las variables adicionales más importantes son la estrategia de protección de datos (replicación o Código de borrado), el porcentaje de operaciones de S3 que se colocan (frente a las Obtiene/otro) y el tamaño medio, en bytes, de los siguientes campos S3 (las abreviaturas de 4 caracteres que se utilizan en la tabla son 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.
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 ≤ P ≤ 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-8fbd-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 ≤ P ≤ 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-8fbd-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.

Configure los mensajes de auditoría y el servidor de syslog externo

Puede configurar una serie de valores relacionados con los mensajes de auditoría. Puede ajustar el número de mensajes de auditoría registrados; definir los encabezados de solicitud HTTP que desee incluir en los mensajes de auditoría de lectura y escritura del cliente; configurar un servidor de syslog externo; y especificar dónde se envían los registros de auditoría, los registros de eventos de seguridad y los registros de software de StorageGRID.

Los mensajes de auditoría y los registros registran las actividades del sistema y los eventos de seguridad, y son herramientas esenciales para la supervisión y solución de problemas. Todos los nodos de StorageGRID generan mensajes y registros de auditoría para realizar un seguimiento de la actividad y los eventos del sistema.

De manera opcional, se puede configurar un servidor de syslog externo para guardar la 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 un grid grande, utiliza varios tipos de aplicaciones S3 o desea conservar todos los datos de auditoría. Consulte "Consideraciones sobre el servidor de syslog externo" para obtener más detalles.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Si planea configurar un servidor de syslog externo, revisó el "consideraciones que tener en cuenta sobre el uso de un servidor de syslog externo" y se aseguró de que el servidor tiene suficiente capacidad para recibir y almacenar los archivos de registro.
- 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"
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"

Estos valores predeterminados se aplican si instaló inicialmente StorageGRID con la versión 10.3 o posterior. Si utilizó inicialmente una versión anterior de StorageGRID, el valor predeterminado para todas las categorías se establece en Normal.

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

Pasos

1. Seleccione **CONFIGURACIÓN** > **Supervisión** > **servidor de auditoría y syslog**.
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: Los mensajes de auditoría para los que el código de resultado no fue "correcto" (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 el número de mensajes de auditoría registrados en el registro de auditoría.

3. Seleccione **Guardar**.

   Un banner verde indica que la configuración se ha guardado.

Definir cabeceras de solicitud HTTP

Opcionalmente, puede definir cualquier cabecera de solicitud HTTP que desee incluir en los mensajes de auditoría de lectura y escritura del cliente. Estos encabezados de protocolo se aplican solo a solicitudes S3 y Swift.

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 la solicitud del protocolo de auditoría sólo se registran si el nivel de auditoría para **Lecturas de cliente** o **Escrituras de cliente** no es **Desactivada**.

3. Seleccione **Guardar**

   Un banner verde indica que la configuración se ha guardado.

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 usar un servidor de syslog externo, omita este paso y vaya a. Seleccione destinos de información de auditoría.

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 el `audit-destinations` Endpoints, 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. En la página servidor de auditoría y syslog, seleccione **Configurar servidor de 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 desee 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 desee 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 útiles para la solución de problemas, incluyendo:
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (Solo nodos de administración)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`

   Para obtener más información sobre los registros del software de StorageGRID, consulte "Registros del software StorageGRID".

2. Utilice los menús desplegables para seleccionar la gravedad y la utilidad (tipo de mensaje) para cada categoría de información de auditoría que desee 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: • 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».
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 **Facilty**, 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	Cada mensaje enviado al syslog externo para tener el mismo valor de instalación que cuando se registró localmente en el nodo: • 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: ◦ `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
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)
10	seguridad (mensajes de seguridad/autorización)
11	FTP

Centro	Descripción
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, corríjalo y vuelva a seleccionar **Enviar mensajes de prueba**.

   Consulte "Solucione problemas de un servidor de syslog externo" para ayudarle a resolver errores.

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, compruebe toda su infraestructura de recopilación de registros. El protocolo UDP no permite una detección de errores tan rigurosa como el otro 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 de syslog externo hasta que se seleccione un destino que incluya el servidor de syslog externo.

Seleccione destinos de información de auditoría

Es posible especificar dónde registros de auditoría, registros de eventos de seguridad y "Registros del software StorageGRID" se envían.

> Algunos destinos solo están disponibles si se configuró un servidor de syslog externo.

Pasos

1. En la página Audit and syslog server, seleccione el destino para obtener información de auditoría.

   > **Solo nodos locales** y **Servidor syslog externo** típicamente proporcionan un mejor rendimiento.

Opción	Descripción
Solo nodos locales	Los mensajes de auditoría, los registros de eventos de seguridad y los registros de aplicaciones no se envían a los nodos de administración. En su lugar, solo se guardan en los nodos que los han generado («el nodo local»). La información de auditoría generada en cada nodo local se almacena en `/var/local/log/localaudit.log` **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 para el registro es de 21 archivos. Cuando se crea la versión 22ª del archivo de registro, se elimina el archivo de registro más antiguo. De media, se almacenan unos 20 GB de datos de registro en cada nodo.
Nodos de administración/nodos locales	Se envían mensajes de auditoría al registro de auditoría (`/var/local/log/audit.log`) En los nodos de administración, los registros de eventos de seguridad y los registros de aplicaciones se almacenan en los nodos que los han generado.
Servidor de syslog externo	La información de auditoría se envía a un servidor de syslog externo y se guarda en los nodos locales. El tipo de información enviada depende de la forma en que se configure el servidor de syslog externo. Esta opción solo se habilita después de configurar un servidor de syslog externo.
Nodo de administrador y servidor de syslog externo	Se envían mensajes de auditoría al registro de auditoría (`/var/local/log/audit.log`) En los nodos de administración, y la información de auditoría se envía al servidor de syslog externo y se guarda en el nodo local. El tipo de información enviada depende de la forma en que se configure el servidor de syslog externo. Esta opción solo se habilita después de configurar un servidor de syslog externo.

2. Seleccione **Guardar**.

   Aparecerá un mensaje de advertencia.

3. Seleccione **OK** para confirmar que desea cambiar el destino para la información de auditoría.

   Un banner verde indica que se guardó la configuración de auditoría.

   Los nuevos registros se envían a los destinos seleccionados. Los registros existentes permanecen en su ubicación actual.

Usar supervisión de SNMP

Utilice la monitorización SNMP: Descripción general

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. El MIB de StorageGRID contiene definiciones de tablas y notificaciones para alertas y alarmas. 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

Las 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.

Las informa 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" para la alerta. Las notificaciones de alerta se envían mediante la "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 ver una lista de las alertas que pueden activar estos retos, consulte la "Referencia de alertas".

- Seguro "alarmas (sistema heredado)" se disparan en niveles de gravedad especificados o superiores.

  Las notificaciones SNMP no se envían para cada alarma o cada gravedad de alarma.

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	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	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 un "navegador web compatible".
- Usted tiene la "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** > **Supervisión** > **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	• 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	Use la comunidad de capturas predeterminada, si se especificó una o introduzca una cadena de comunidad personalizada para este destino de captura. La cadena de comunidad personalizada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

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	Use la comunidad de capturas predeterminada, si se especificó una o introduzca una cadena de comunidad personalizada para este destino de captura. La cadena de comunidad personalizada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

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	El usuario USM que se usará para la autenticación. • 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: i. Cree y guarde el destino de captura. ii. Vaya a. Crear usuarios USM y crear 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	Si esta dirección usará IPv4 o IPv6. De forma predeterminada, SNMP utiliza IPv4.
Protocolo de transporte	Si esta dirección usará UDP o TCP. De forma predeterminada, SNMP utiliza UDP.
Red StorageGRID	En qué red StorageGRID escuchará el agente. • Redes Grid, Admin y Client: El agente SNMP escuchará las consultas en las tres redes. • Red Grid • Red de administración • Red cliente **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.
Puerto	Opcionalmente, el número de puerto en el que debe recibir el agente SNMP. El puerto UDP predeterminado para un agente SNMP es 161, pero puede introducir cualquier número de puerto no utilizado. **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.

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.

> 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	Nombre único para este usuario USM. 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.
Acceso a la MIB de solo lectura	Si se selecciona, este usuario debe tener acceso de solo lectura a la MIB.
ID de motor autorizado	Si este usuario se va a utilizar en un destino de informe, el ID de motor autorizado para este usuario. 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. **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.
Nivel de seguridad	Nivel de seguridad del usuario USM: • **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 un "navegador web compatible".
- Usted tiene la "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** > **Supervisión** > **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 información detallada 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 información detallada sobre qué introducir, consulte "Crear direcciones de agente".

   - Para agregar una dirección de agente, seleccione **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 información detallada 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** > **Supervisión** > **Agente SNMP**.
2. En la página del agente SNMP, seleccione el archivo que desee 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)

   a. Grep para el OID de StorageGRID en todo el árbol (utilizando `paste` para unir líneas):

   ```
   root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
   ```

> La `snmptranslate` Command 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
iso.org.dod.internet. + empresas privadas. netapp.storagegrid		Módulo MIB para entidades de NetApp StorageGRID.

Objetos MIB

Nombre del objeto	ID Objeto (OID)	Descripción
Active AlertCount	**1,3.6,1.4,1. +** 789.28669.1.3	El número de alertas activas en activeAlertTable.
Active AlertTable	**1,3.6,1.4,1. +** 789.28669.1.4	Una tabla de alertas activas en StorageGRID.
Active AlertId	**1,3.6,1.4,1. +** 789.28669.1.4.1.1	El ID de la alerta. Solo es único en el conjunto actual de alertas activas.
Active AlertName	**1,3.6,1.4,1. +** 789.28669.1.4.1.2	El nombre de la alerta.
Active AlertInstance	**1,3.6,1.4,1. +** 789.28669.1.4.1.3	El nombre de la entidad que generó la alerta, generalmente el nombre del nodo.
Active AlertSeverity	**1,3.6,1.4,1. +** 789.28669.1.4.1.4	La gravedad de la alerta.
Active AlertStartTime	**1,3.6,1.4,1. +** 789.28669.1.4.1.5	La fecha y la hora en la que se activó la alerta.

Tipos de notificación (retos)

Todas las notificaciones incluyen las siguientes variables como varbinds:

- Active AlertId
- Active AlertName
- Active AlertInstance
- Active AlertSeverity
- Active AlertStartTime

Tipo de notificación	ID Objeto (OID)	Descripción
ActiveMinorAlert	**1,3.6,1.4,1. +** 789.28669.0.6	Una alerta de gravedad menor

Tipo de notificación	ID Objeto (OID)	Descripción
Active MajorAlert	**1,3.6,1.4,1. +** 789.28669.0.7	Una alerta de gravedad importante
ActiveCriticalAlert	**1,3.6,1.4,1. +** 789.28669.0.8	Una alerta con gravedad crítica

Recopilación de datos de StorageGRID adicionales

Utilice gráficos y gráficos

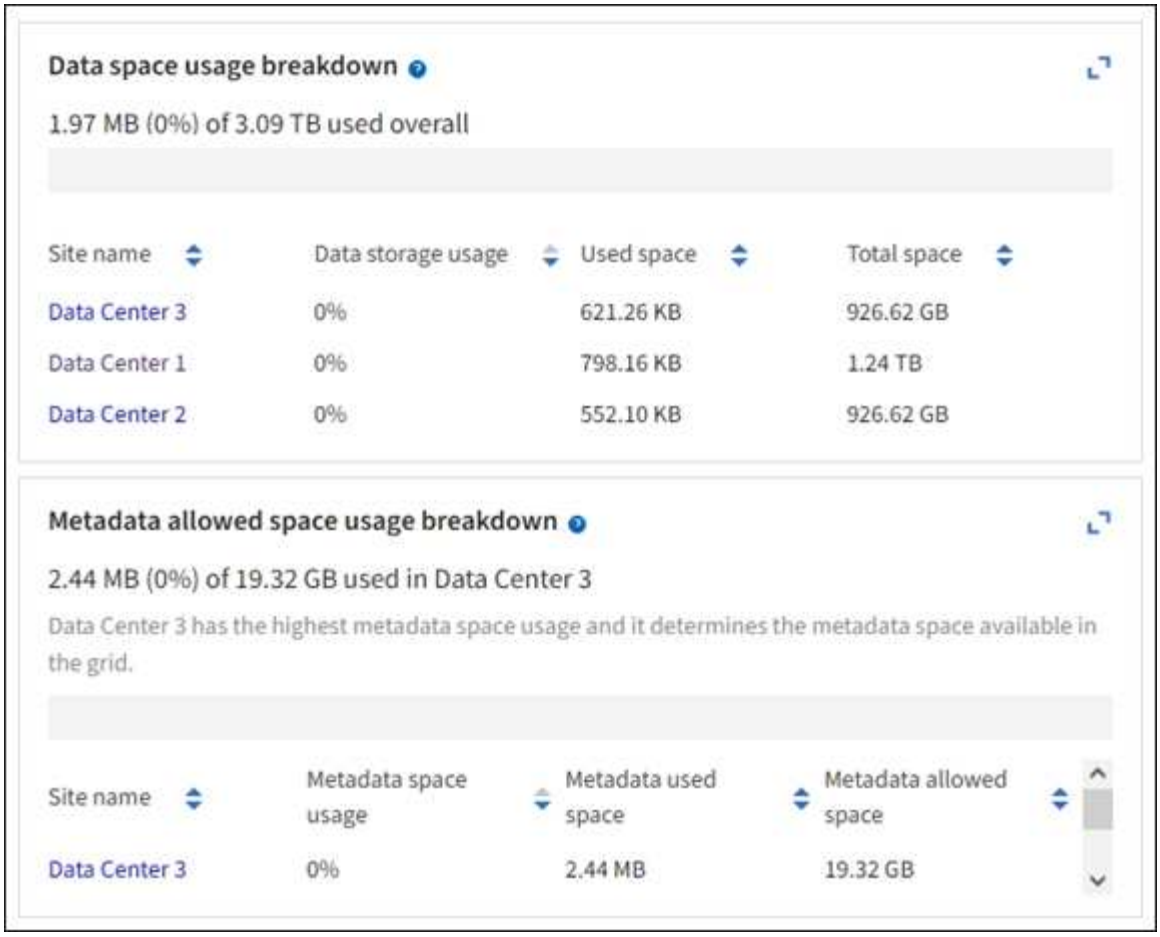
Puede utilizar gráficos e informes para supervisar el estado del sistema StorageGRID y solucionar problemas.

> 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.

Tipos de gráficos

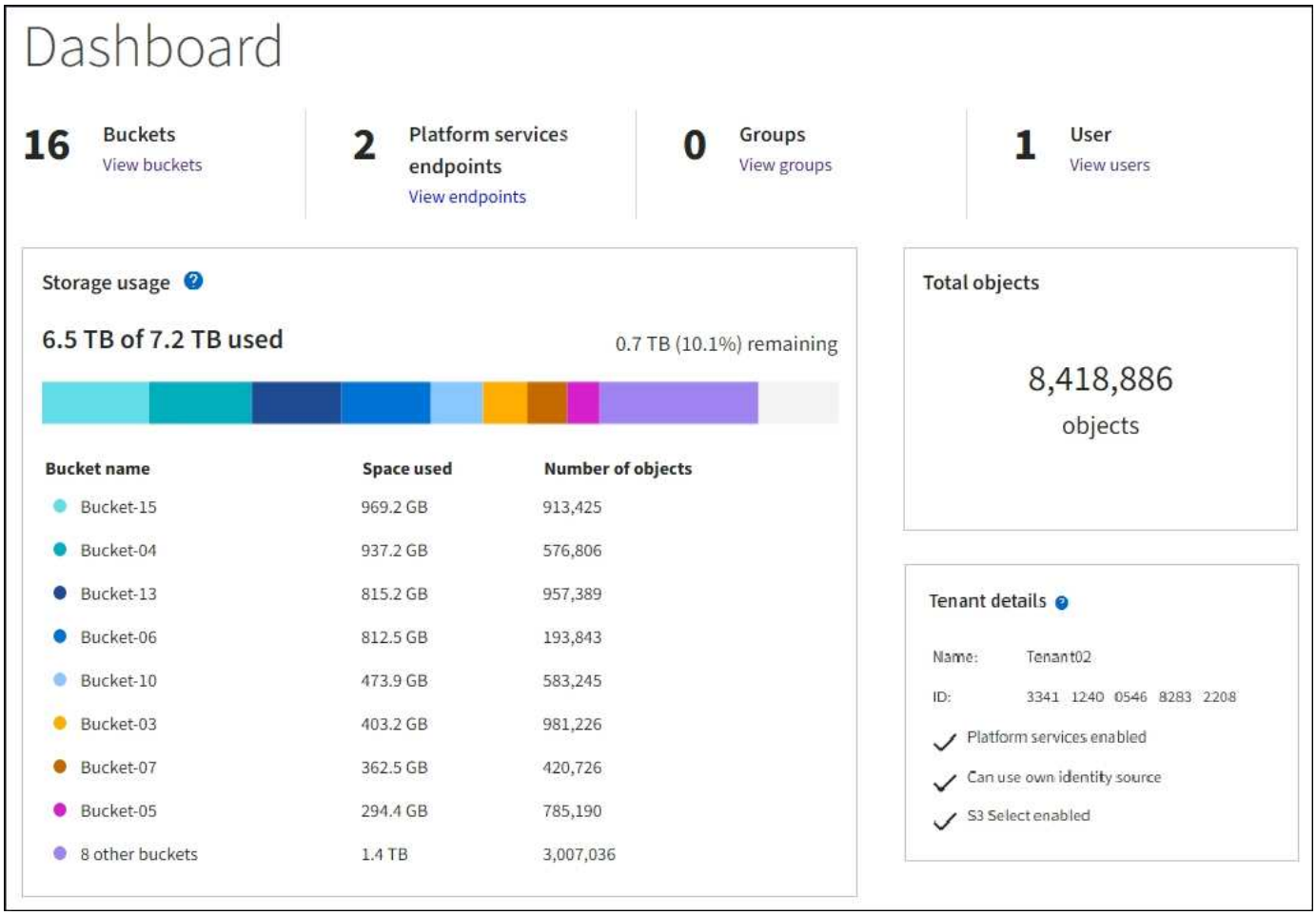
Los gráficos y los gráficos resumen los valores de métricas y atributos de StorageGRID específicos.

La consola de Grid Manager incluye tarjetas que resumen el almacenamiento disponible para el grid y cada sitio.



En el panel Uso del almacenamiento de la consola del administrador de inquilino se muestra lo siguiente:

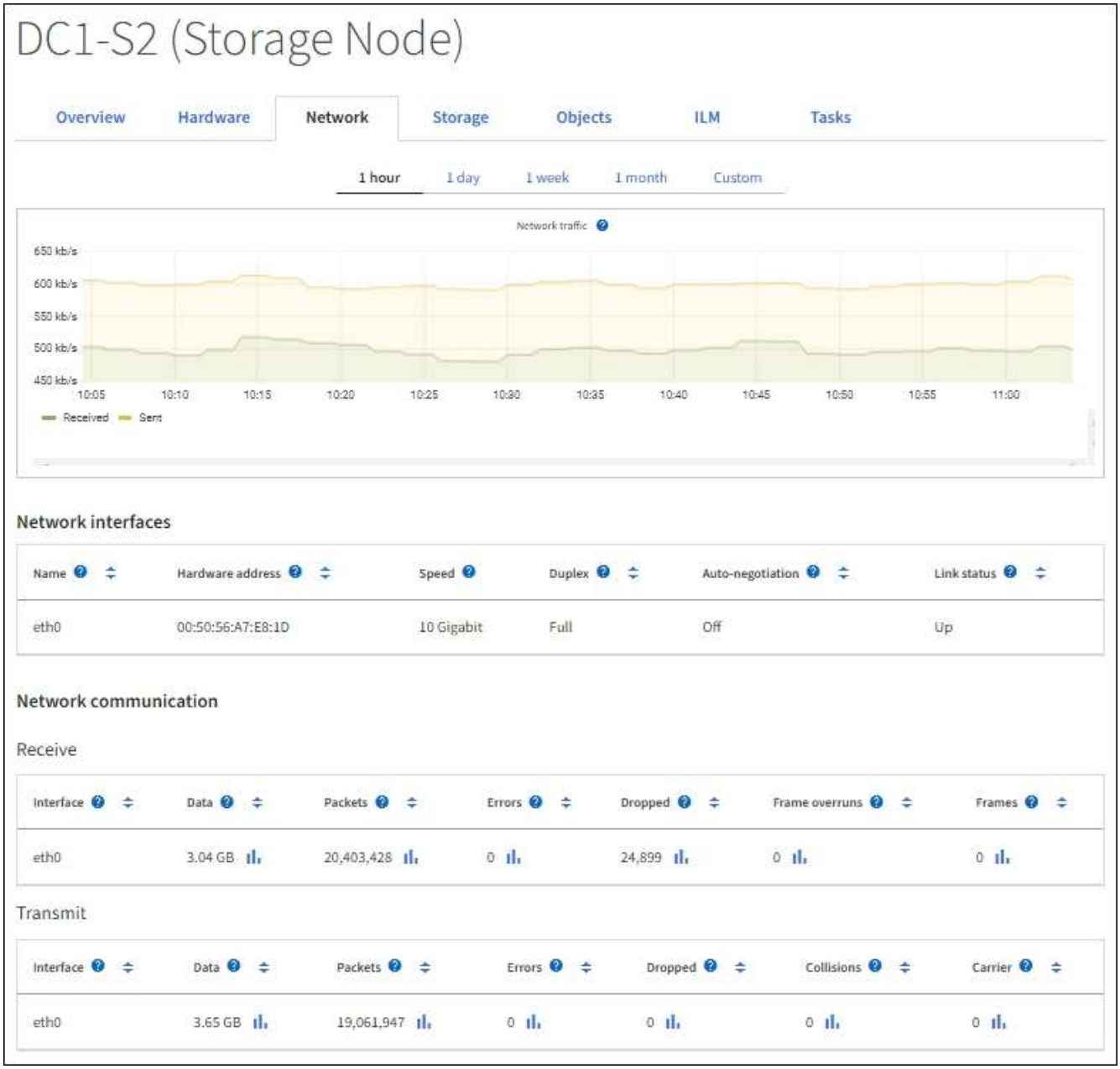
- Una lista de los bloques más grandes (S3) o los contenedores (Swift) para el inquilino
- Un gráfico de barras que representa los tamaños relativos de los cubos o contenedores más grandes
- La cantidad total de espacio utilizado y, si se establece una cuota, la cantidad y el porcentaje de espacio restante



Además, los gráficos que muestran cómo cambian las métricas y los atributos de StorageGRID con el tiempo están disponibles en la página Nodes y en la página **SUPPORT** > **Tools** > **Grid topolog**.

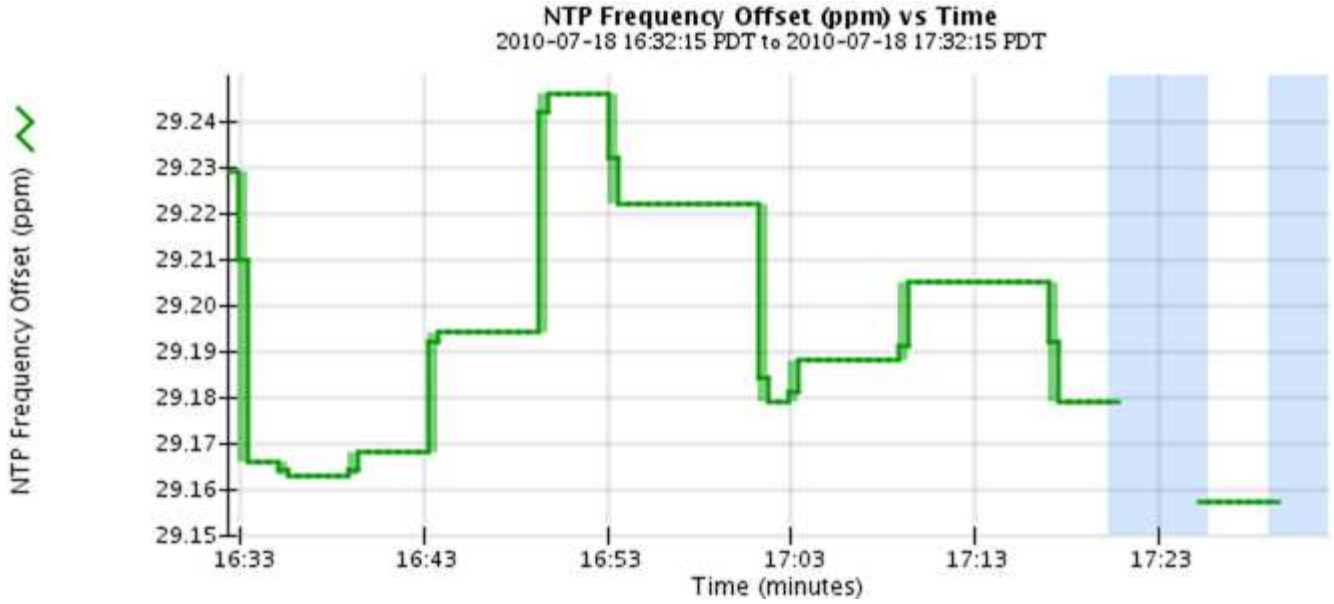
Existen cuatro tipos de gráficos:

- * Gráficos Grafana*: Se muestran en la página Nodes, los gráficos Grafana se utilizan para trazar los valores de las métricas Prometheus a lo largo del tiempo. Por ejemplo, la ficha **NODES** > **Network** de un nodo de almacenamiento incluye un gráfico Grafana para el tráfico de red.

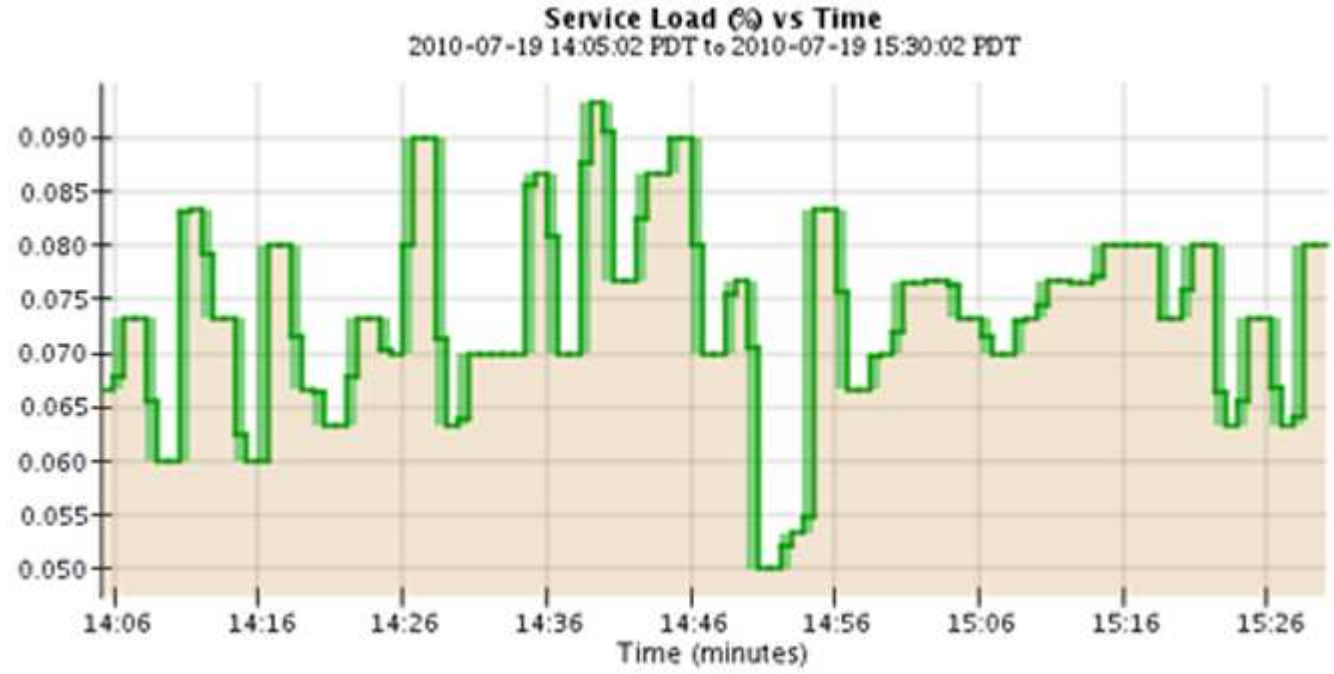


Los gráficos Grafana también se incluyen en los paneles preconstruidos disponibles en la página **SUPPORT** > **Tools** > **Metrics**.

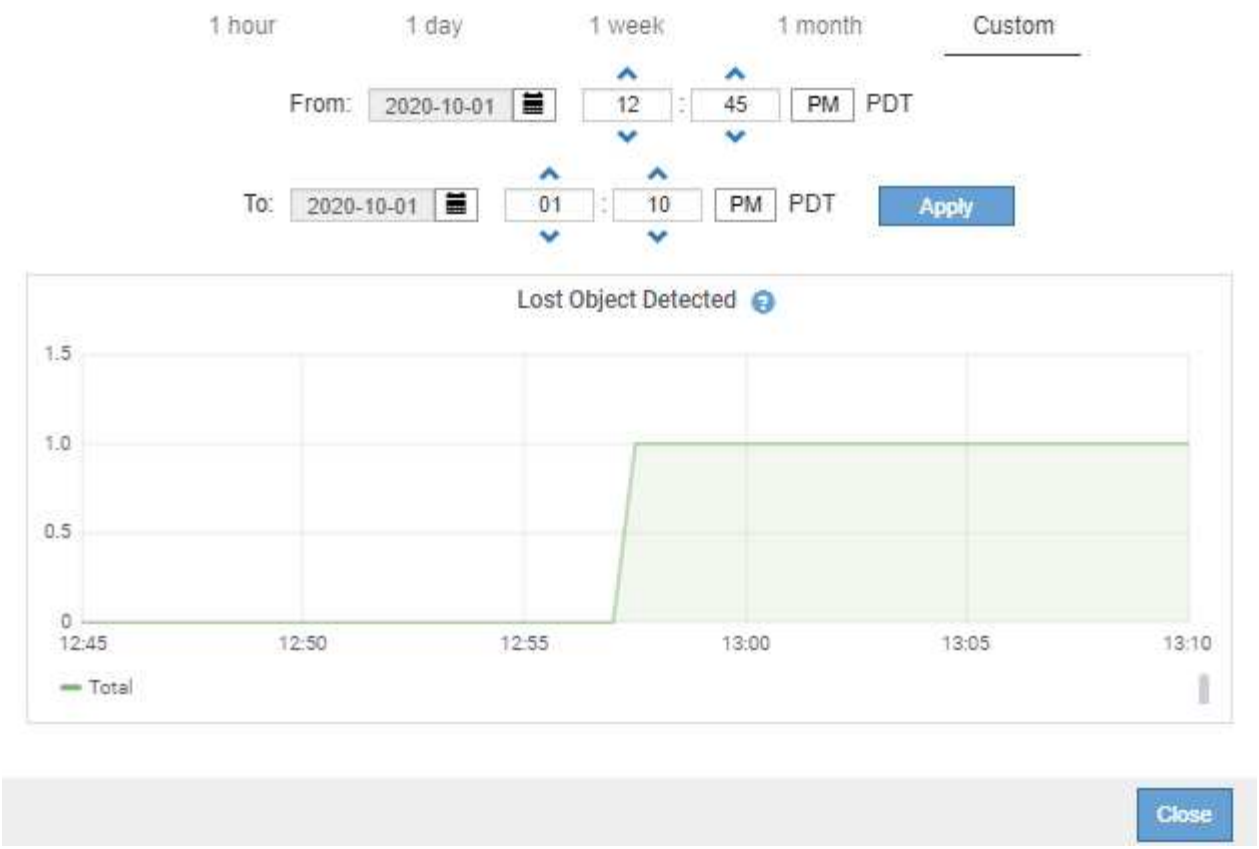
- **Gráficos de líneas**: Disponible en la página Nodes y en la página **SUPPORT** > **Tools** > **Topología de cuadrícula** (seleccione el icono de gráfico Después de un valor de datos), los gráficos de líneas se utilizan para trazar los valores de los atributos StorageGRID que tienen un valor de unidad (como el desplazamiento de frecuencia NTP, en ppm). Los cambios en el valor se representan en intervalos de datos regulares (bins) a lo largo del tiempo.



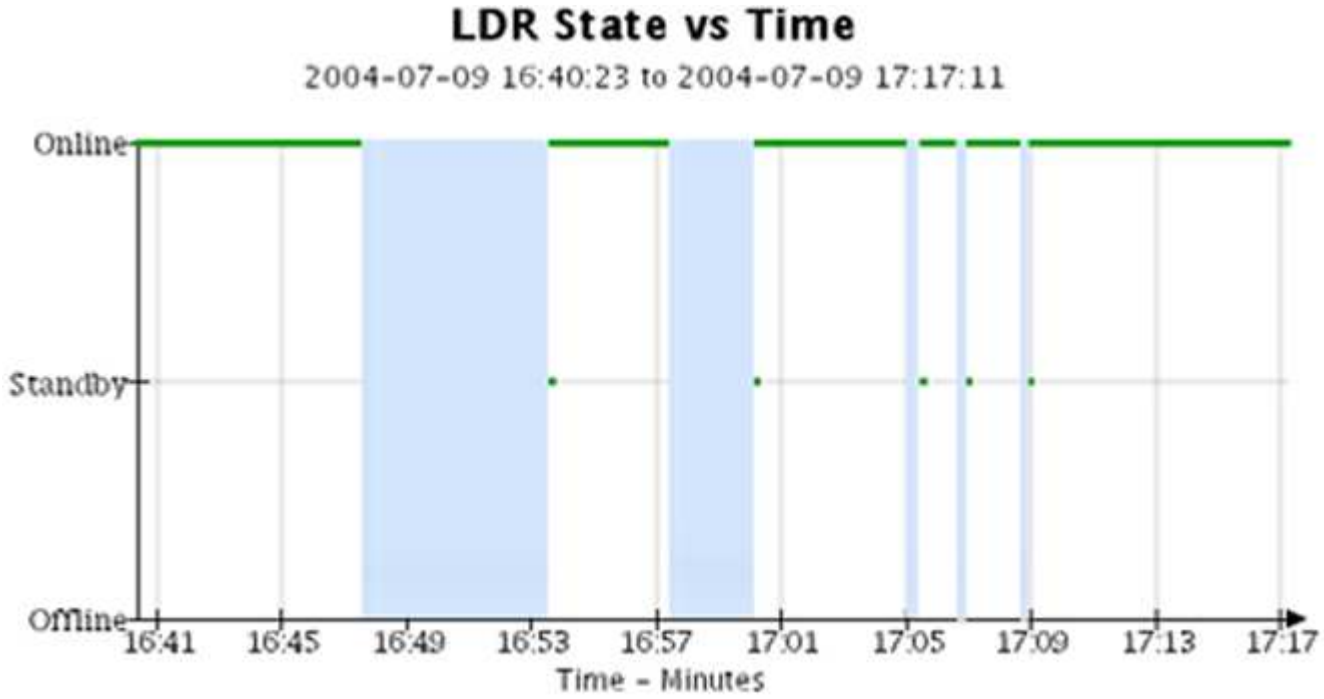
- **Gráficos de área**: Disponible en la página Nodes y en la página **SUPPORT** > **Tools** > **Grid topolog** (seleccione el icono del gráfico) después de un valor de datos), los gráficos de área se utilizan para trazar cantidades de atributos volumétricos, como recuentos de objetos o valores de carga de servicio. Los gráficos de área son similares a los gráficos de líneas, pero incluyen un sombreado marrón claro debajo de la línea. Los cambios en el valor se representan en intervalos de datos regulares (bins) a lo largo del tiempo.



- Algunos gráficos están marcados con un tipo diferente de icono de gráfico y tienen un formato diferente:



- **Gráfico de estado**: Disponible en la página **SUPPORT** > **Tools** > **Topología de cuadrícula** (seleccione el icono de gráfico después de un valor de datos), los gráficos de estado se utilizan para trazar valores de atributos que representan estados distintos, como un estado de servicio que puede estar en línea, en espera o sin conexión. Los gráficos de estado son similares a los gráficos de líneas, pero la transición es discontinua; es decir, el valor salta de un valor de estado a otro.



Información relacionada

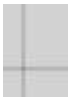
"Vea la página Nodes"

"Abra el árbol de topología de cuadrícula"

"Revisar las métricas de soporte"

Leyenda del gráfico

Las líneas y los colores utilizados para dibujar gráficos tienen un significado específico.

Ejemplo	Significado
	Los valores de atributo reportados se trazan utilizando líneas verdes oscuras.
	El sombreado verde claro alrededor de líneas verdes oscuras indica que los valores reales en ese rango de tiempo varían y se han “agrupado” para un trazado más rápido. La línea oscura representa la media ponderada. El rango en verde claro indica los valores máximo y mínimo dentro de la bandeja. El sombreado marrón claro se utiliza para gráficos de áreas para indicar datos volumétricos.
	Las áreas en blanco (sin datos representados) indican que los valores de atributo no estaban disponibles. El fondo puede ser azul, gris o una mezcla de gris y azul, dependiendo del estado del servicio que informa sobre el atributo.
	El sombreado de azul claro indica que algunos o todos los valores de atributo en ese momento eran indeterminados; el atributo no estaba informando de valores porque el servicio estaba en estado desconocido.
	El sombreado de gris indica que algunos o todos los valores de atributo en ese momento no se conocen porque el servicio que informa de los atributos estaba administrativamente inactivo.
	Una mezcla de sombreado de gris y azul indica que algunos de los valores de atributo en ese momento eran indeterminados (porque el servicio estaba en un estado desconocido), mientras que otros no se conocían porque el servicio que reportaba los atributos estaba administrativamente abajo.

Mostrar gráficos y gráficos

La página nodos contiene los gráficos y los gráficos a los que debe acceder de manera regular para supervisar atributos como la capacidad de almacenamiento y el rendimiento. En algunos casos, especialmente al trabajar con soporte técnico, puede utilizar la página **SUPPORT** > **Tools** > **Grid topolog** para acceder a gráficos adicionales.

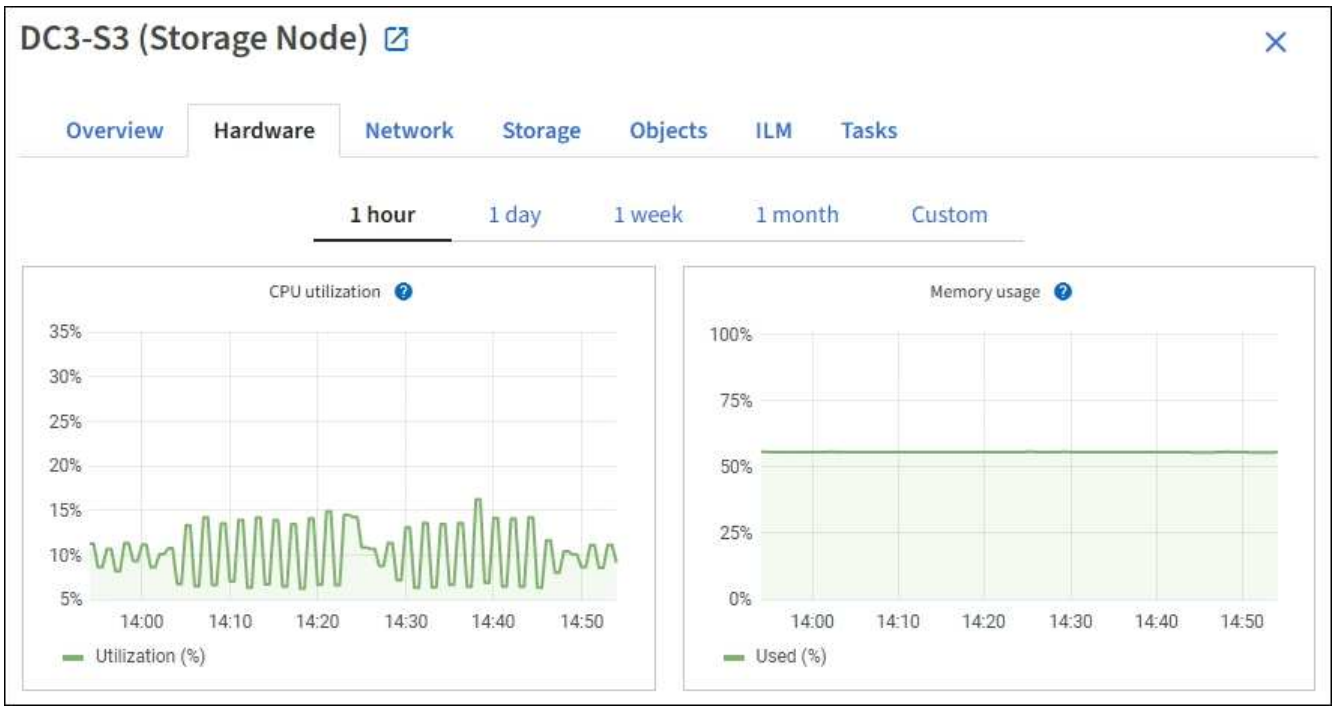
Antes de empezar

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

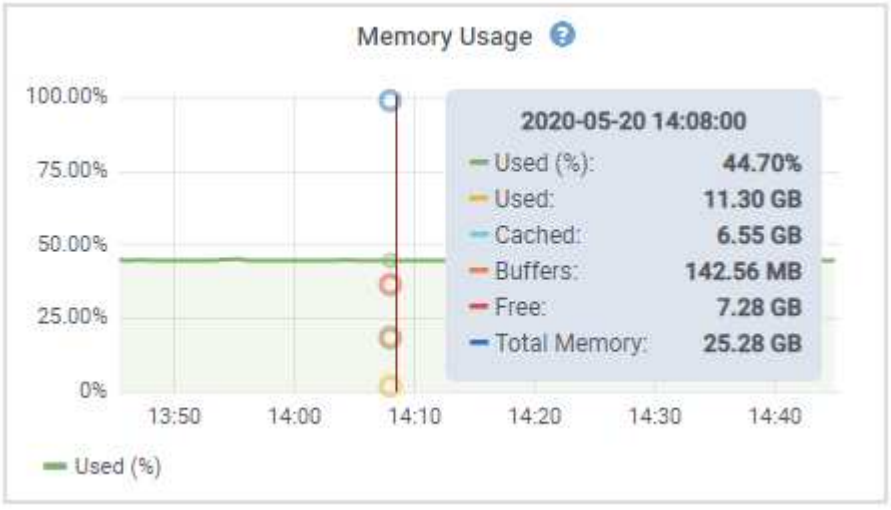
Pasos

1. Selecciona **NODOS**. A continuación, seleccione un nodo, un sitio o toda la cuadrícula.
2. Seleccione la ficha para la que desea ver información.

Algunas pestañas incluyen uno o más gráficos Grafana, que se utilizan para trazar los valores de las métricas Prometheus a lo largo del tiempo. Por ejemplo, la ficha **NODES** > **hardware** de un nodo incluye dos gráficos Grafana.



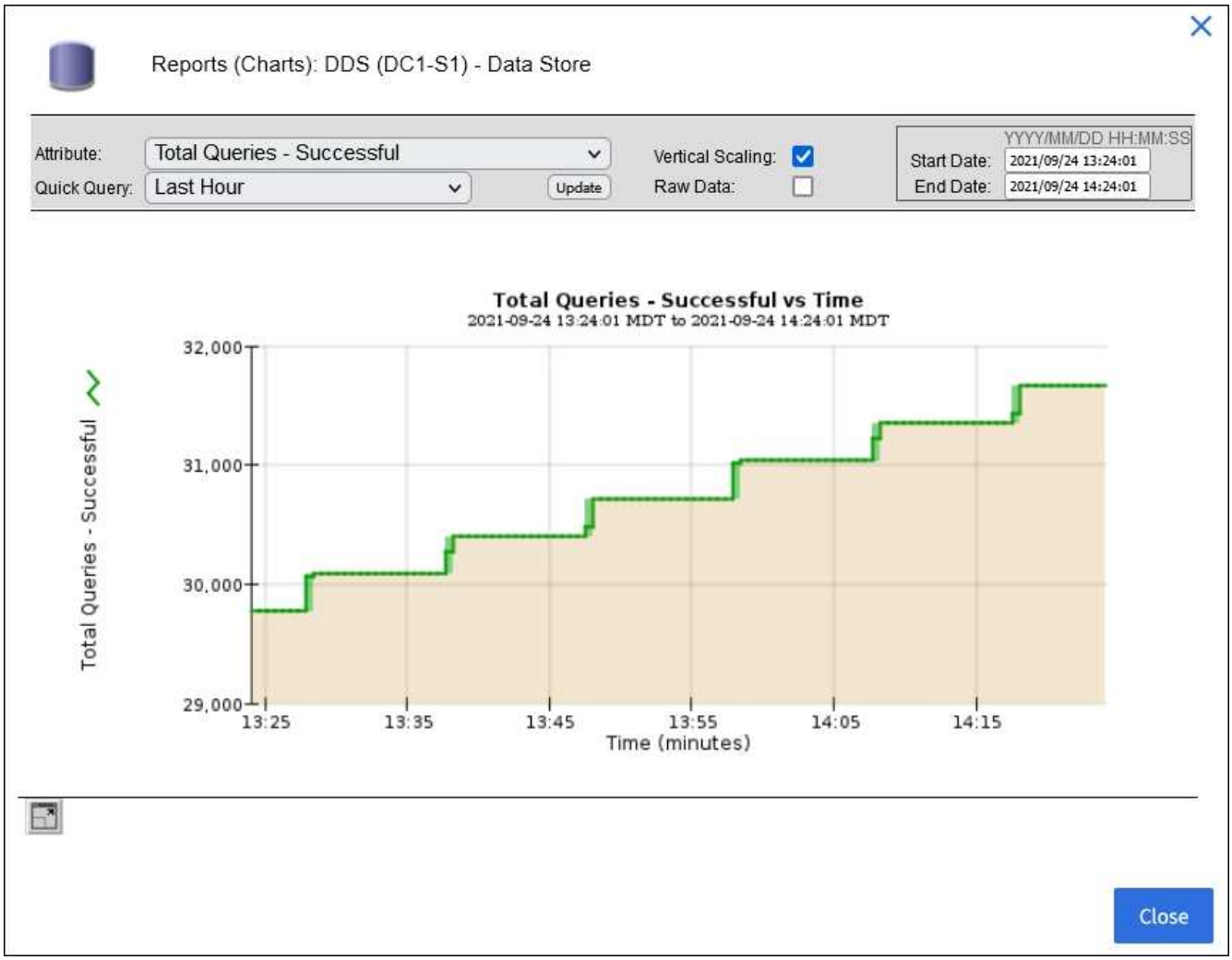
3. Opcionalmente, coloque el cursor sobre el gráfico para ver valores más detallados para un punto en el tiempo concreto.

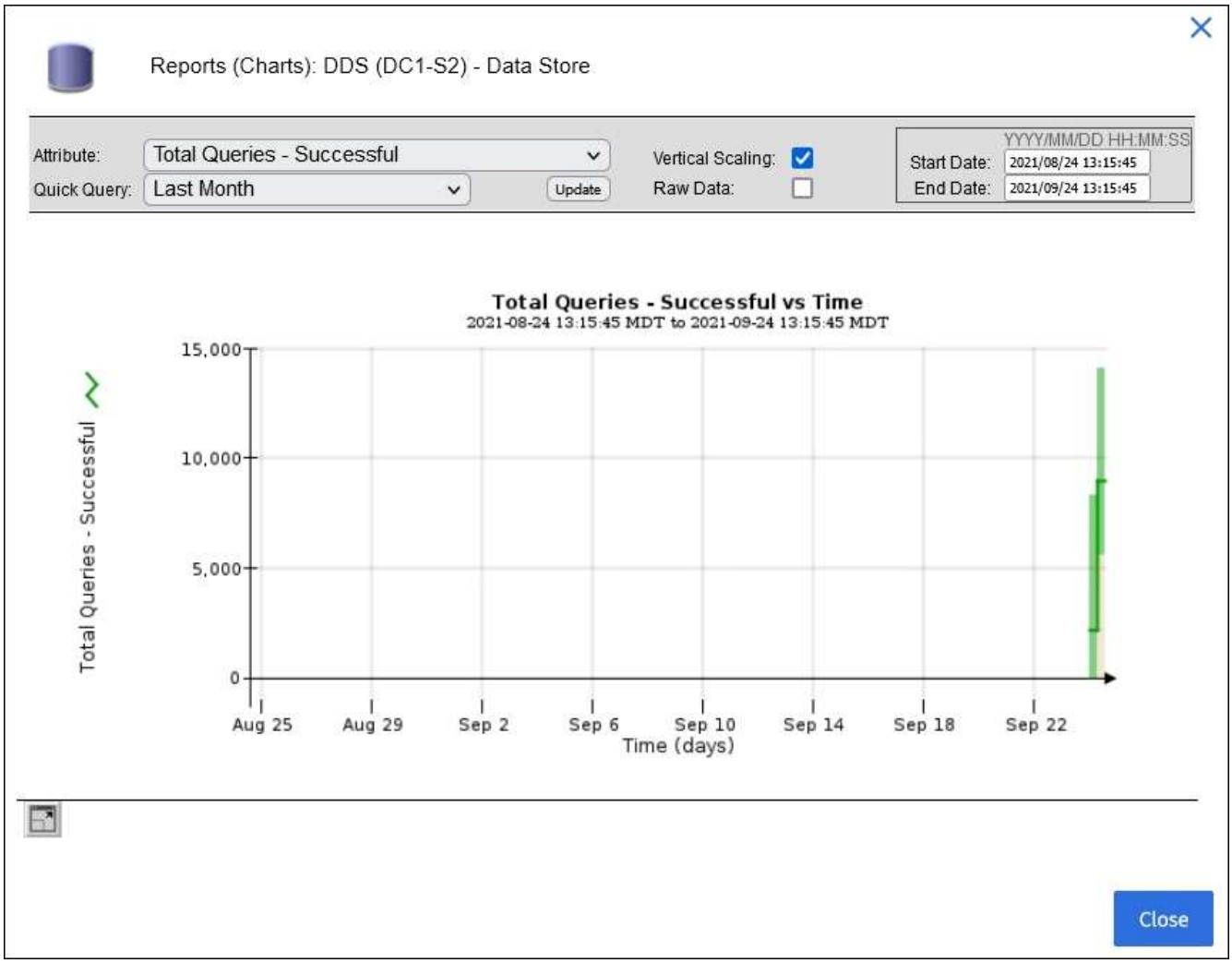


4. Según sea necesario, a menudo puede mostrar un gráfico para un atributo o métrica específicos. En la tabla de la página Nodes, seleccione el icono del gráfico a la derecha del nombre del atributo.

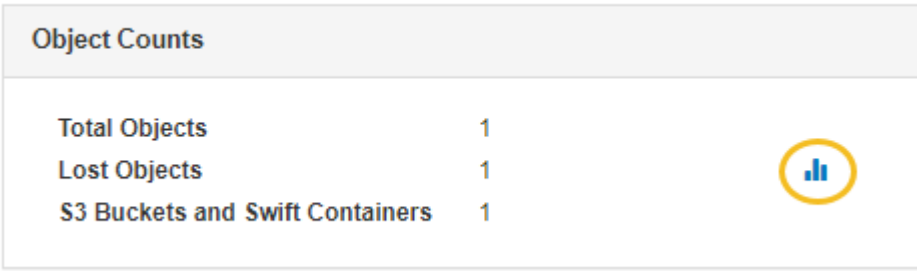
> Los gráficos no están disponibles para todas las métricas y atributos.

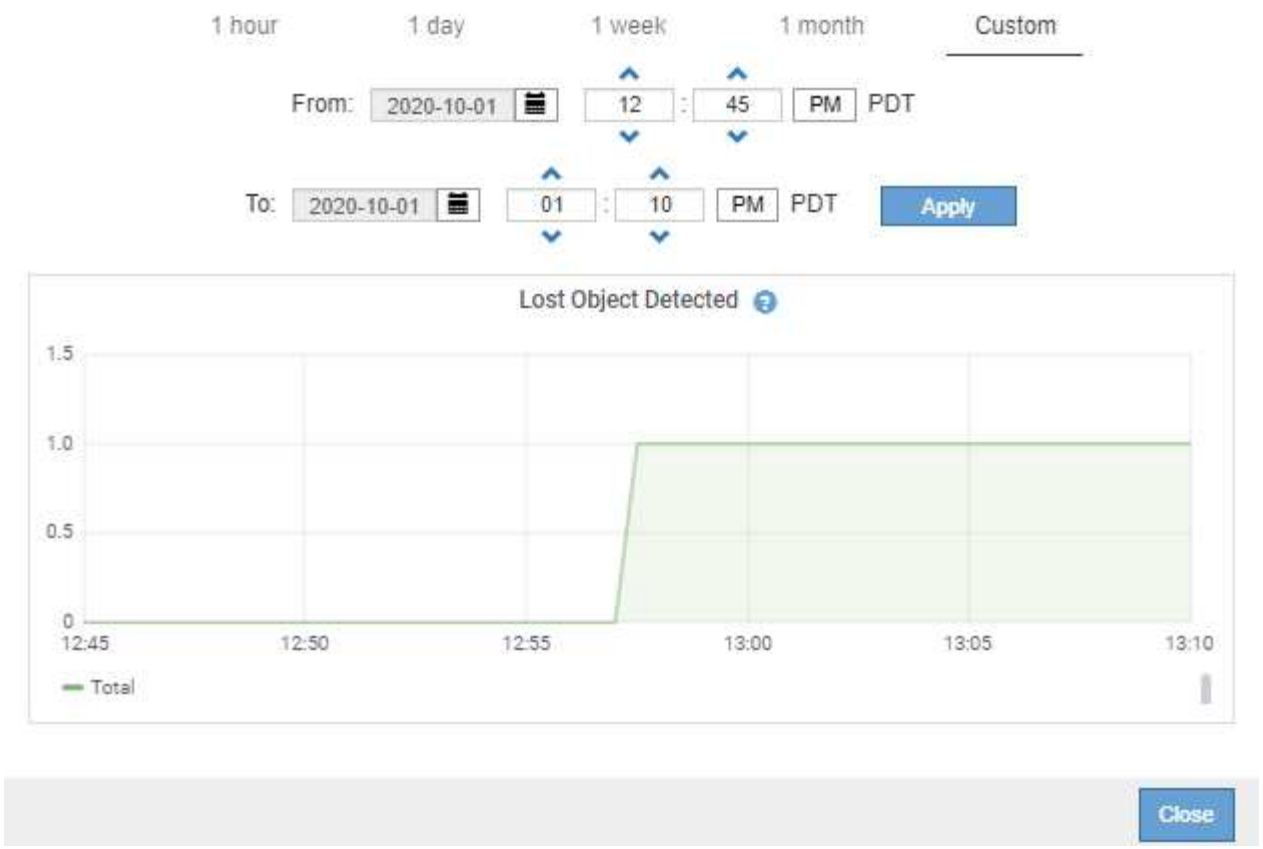
Ejemplo 1: En la ficha objetos de un nodo de almacenamiento, puede seleccionar el icono del gráfico Para ver el número total de consultas correctas del almacén de metadatos para el nodo de almacenamiento.


Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close

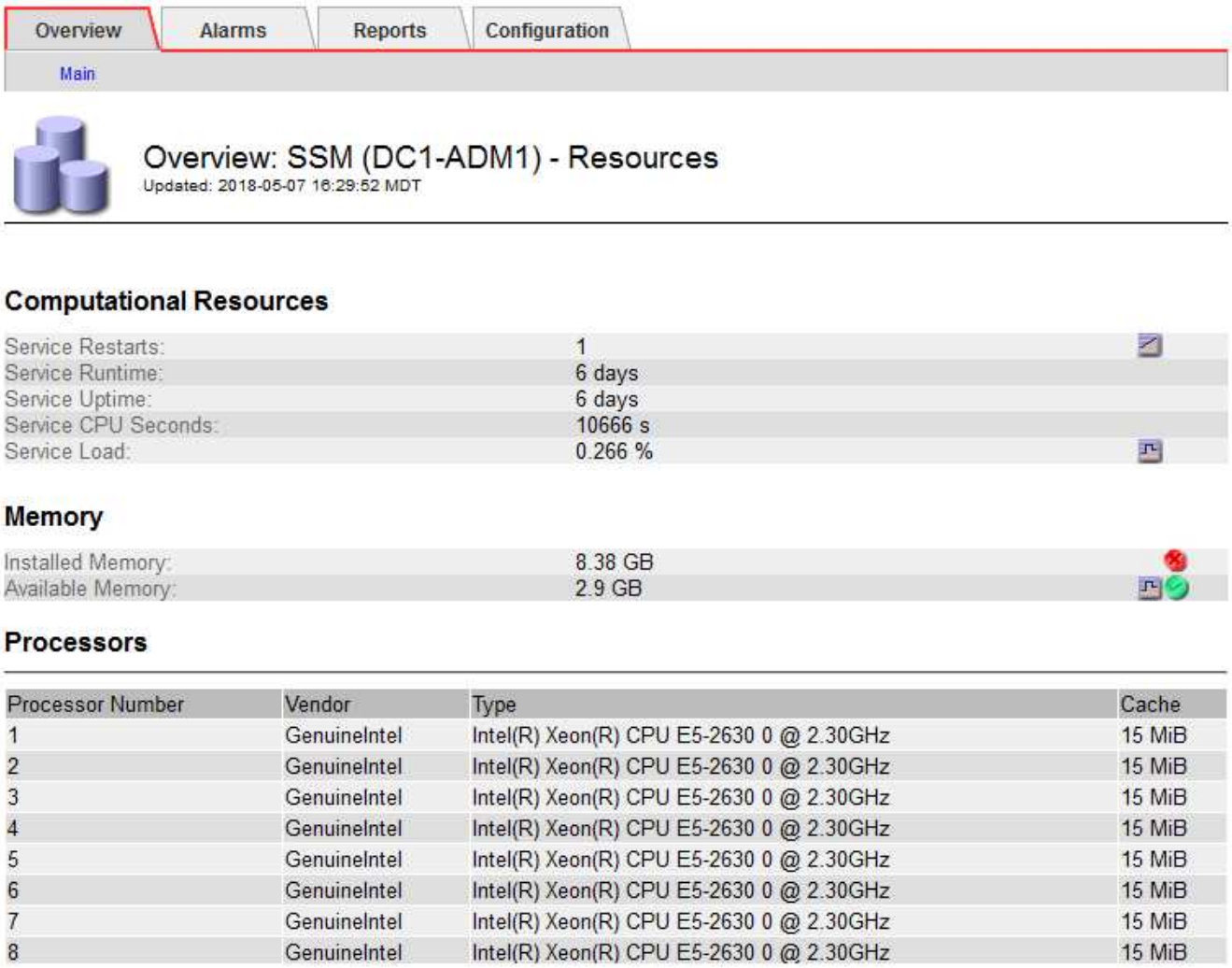


Ejemplo 2: En la pestaña Objetos de un nodo de almacenamiento, puede seleccionar el icono del gráfico Para ver el gráfico Grafana del número de objetos perdidos detectados con el tiempo.





5. Para mostrar gráficos de atributos que no se muestran en la página Nodo, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
6. Seleccione ***grid node*** > ***component o Service*** > **Descripción general** > **Principal**.



7. Seleccione el icono de gráfico junto al atributo.

   La pantalla cambia automáticamente a la página **Informes** > **gráficos**. El gráfico muestra los datos del atributo en el último día.

Generar gráficos

Los gráficos muestran una representación gráfica de los valores de datos de atributos. Puede generar informes en el sitio de un centro de datos, en el nodo de grid, en el componente o en el servicio.

Antes de empezar

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

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***grid node*** > ***component o Service*** > **Reports** > **Charts**.
3. Seleccione el atributo sobre el que desea informar en la lista desplegable **atributo**.
4. Para forzar que el eje Y comience en cero, desactive la casilla de verificación **Escalado vertical**.
5. Para mostrar valores con total precisión, seleccione la casilla de verificación **Datos sin procesar**, o para

redondear los valores a un máximo de tres posiciones decimales (por ejemplo, para los atributos reportados como porcentajes), desactive la casilla de verificación **Datos sin procesar**.

6. Seleccione el período de tiempo que desea generar el informe en la lista desplegable **Consulta rápida**.

   Seleccione la opción Consulta personalizada para seleccionar un intervalo de tiempo específico.

   El gráfico aparece después de unos momentos. Deje varios minutos para tabulación de intervalos de tiempo largos.

7. Si ha seleccionado Consulta personalizada, personalice el período de tiempo del gráfico introduciendo **Fecha de inicio** y **Fecha de finalización**.

   Utilice el formato *YYYY/MM/DDHH:MM:SS* en hora local. Se requieren ceros a la izquierda para que coincidan con el formato. Por ejemplo, 2017/4/6 7:30:00 falla en la validación. El formato correcto es: 2017/04/06 07:30:00.

8. Seleccione **Actualizar**.

   Un gráfico se genera después de unos segundos. Deje varios minutos para tabulación de intervalos de tiempo largos. Según el tiempo establecido para la consulta, se muestra un informe de texto sin procesar o un informe de texto agregado.

Usar informes de texto

Los informes de texto muestran una representación textual de los valores de datos de atributos que ha procesado el servicio NMS. Hay dos tipos de informes generados en función del período de tiempo en el que se informa: Informes de texto en bruto para períodos inferiores a una semana y informes de texto agregados para períodos de tiempo superiores a una semana.

Informes de texto sin formato

Un informe de texto sin procesar muestra detalles sobre el atributo seleccionado:

- Hora recibida: Fecha y hora local en la que el servicio NMS procesó un valor de muestra de los datos de un atributo.
- Hora de la muestra: Fecha y hora local en la que se muestreó o cambió un valor de atributo en el origen.
- Valor: Valor de atributo en el tiempo de la muestra.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Informes de texto agregados

Un informe de texto agregado muestra los datos durante un período de tiempo más largo (normalmente una semana) que un informe de texto en bruto. Cada entrada es el resultado de resumir varios valores de atributo (un agregado de valores de atributo) por el servicio NMS a lo largo del tiempo en una sola entrada con valores promedio, máximo y mínimo que se derivan de la agregación.

Cada entrada muestra la siguiente información:

- Hora agregada: Última fecha y hora local que el servicio NMS ha agregado (recopilado) un conjunto de valores de atributo modificados.
- Valor medio: Promedio del valor del atributo durante el período de tiempo agregado.
- Valor mínimo: Valor mínimo durante el período de tiempo agregado.
- Valor máximo: Valor máximo durante el período de tiempo agregado.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Generar informes de texto

Los informes de texto muestran una representación textual de los valores de datos de atributos que ha procesado el servicio NMS. Puede generar informes en el sitio de un centro de datos, en el nodo de grid, en el componente o en el servicio.

Antes de empezar

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

Acerca de esta tarea

Para los datos de atributos que se espera que cambien continuamente, el servicio NMS (en el origen) muestra estos datos de atributos a intervalos regulares. Para los datos de atributos que cambian con poca frecuencia (por ejemplo, datos basados en eventos como cambios de estado o de estado), se envía un valor de atributo al servicio NMS cuando cambia el valor.

El tipo de informe que se muestra depende del período de tiempo configurado. De forma predeterminada, se generan informes de texto agregados para períodos de tiempo superiores a una semana.

El texto gris indica que el servicio se ha reducido administrativamente durante el tiempo en que se realizó la muestra. El texto azul indica que el servicio estaba en un estado desconocido.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***grid node*** > ***component o Service*** > **Reports** > **Text**.
3. Seleccione el atributo sobre el que desea informar en la lista desplegable **atributo**.
4. Seleccione el número de resultados por página en la lista desplegable **resultados por página**.
5. Para redondear los valores a un máximo de tres posiciones decimales (por ejemplo, para los atributos reportados como porcentajes), desactive la casilla de verificación **Datos sin procesar**.
6. Seleccione el período de tiempo que desea generar el informe en la lista desplegable **Consulta rápida**.

   Seleccione la opción Consulta personalizada para seleccionar un intervalo de tiempo específico.

El informe aparece después de unos momentos. Deje varios minutos para tabulación de intervalos de tiempo largos.

7. Si ha seleccionado Consulta personalizada, debe personalizar el período de tiempo para informar introduciendo **Fecha de inicio** y **Fecha de finalización**.

   Utilice el formato `YYYY/MM/DDHH:MM:SS` en hora local. Se requieren ceros a la izquierda para que coincidan con el formato. Por ejemplo, 2017/4/6 7:30:00 falla en la validación. El formato correcto es: 2017/04/06 07:30:00.

8. Haga clic en **Actualizar**.

   Después de unos momentos se genera un informe de texto. Deje varios minutos para tabulación de intervalos de tiempo largos. Según el tiempo establecido para la consulta, se muestra un informe de texto sin procesar o un informe de texto agregado.

Exportar informes de texto

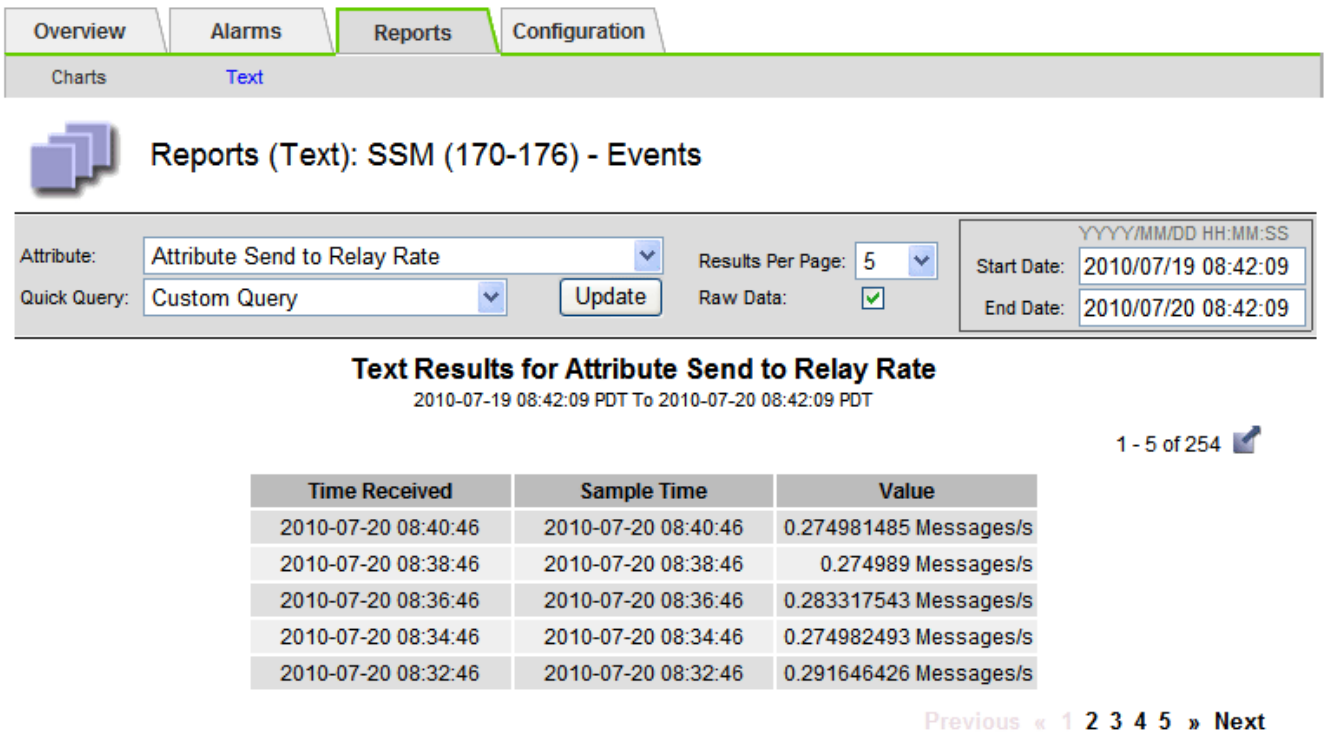
Los informes de texto exportados abren una nueva pestaña del navegador, que permite seleccionar y copiar los datos.

Acerca de esta tarea

A continuación, los datos copiados se pueden guardar en un documento nuevo (por ejemplo, una hoja de cálculo) y se pueden utilizar para analizar el rendimiento del sistema StorageGRID.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Cree un informe de texto.
3. Haga clic en *Exportar*.



Se abre la ventana Exportar informe de texto que muestra el informe.

Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U

4. Seleccione y copie el contenido de la ventana Exportar informe de texto.

   Estos datos se pueden pegar ahora en un documento de terceros, como una hoja de cálculo.

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 y Swift 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.

Mensajes del "registro de auditoría" indica 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 se puede encontrar el atributo TIME en los mensajes de auditoría de las siguientes operaciones:

- **S3**: BORRAR, OBTENER, CABEZA, metadatos actualizados, POST, PUESTO
- **SWIFT**: BORRAR, OBTENER, CABEZA, PONER

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 hacerlo "Descargue el probador S3del 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 un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".

Acerca de esta tarea

Dos "procesos de verificación" trabajar 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 nodos de archivado ni en objetos de un pool de almacenamiento en cloud.

  > ⓘ 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.

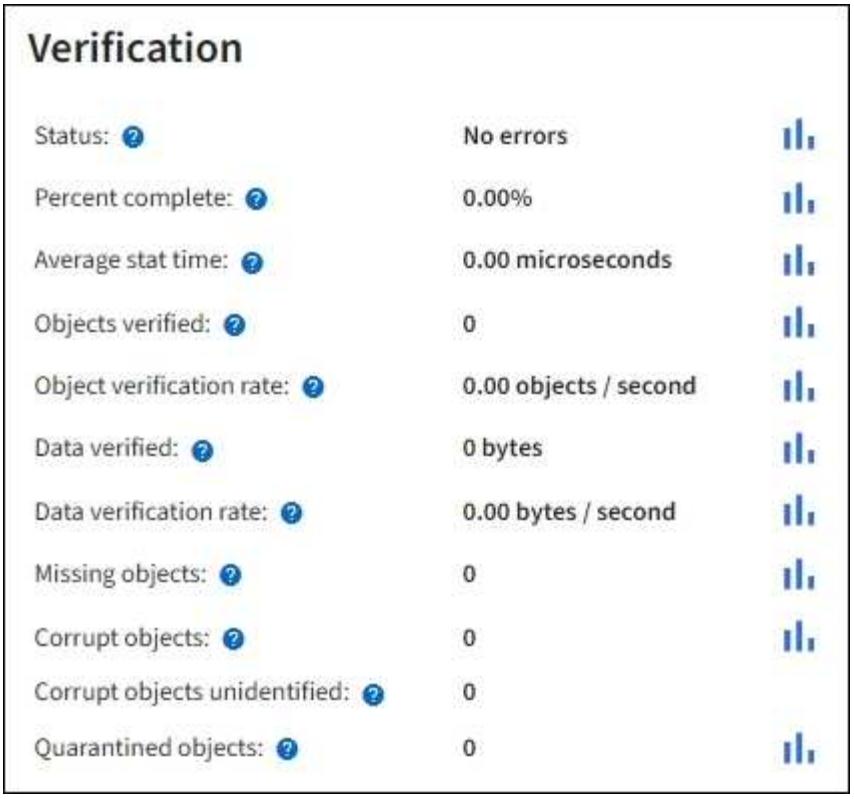
Pasos

1. Revise los resultados de las verificaciones de fondo:

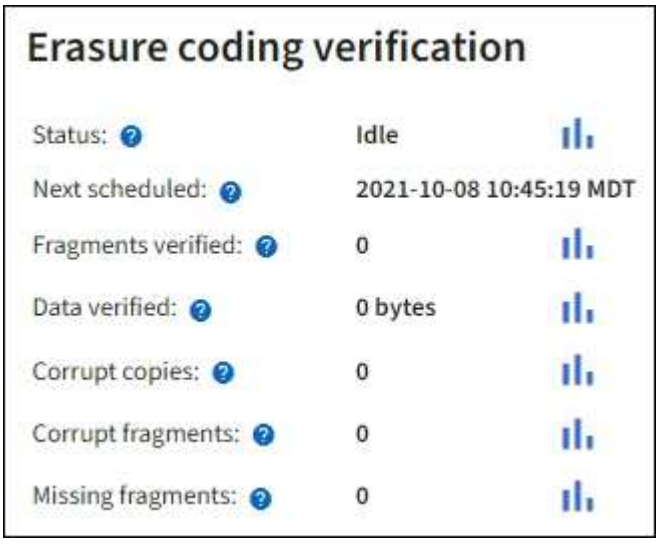
   a. Seleccione **NODES** > ***Storage Node*** > **Objects**.

   b. Compruebe los resultados de verificación:

      - Para comprobar la verificación de datos de objetos replicados, observe los atributos de la sección verificación.

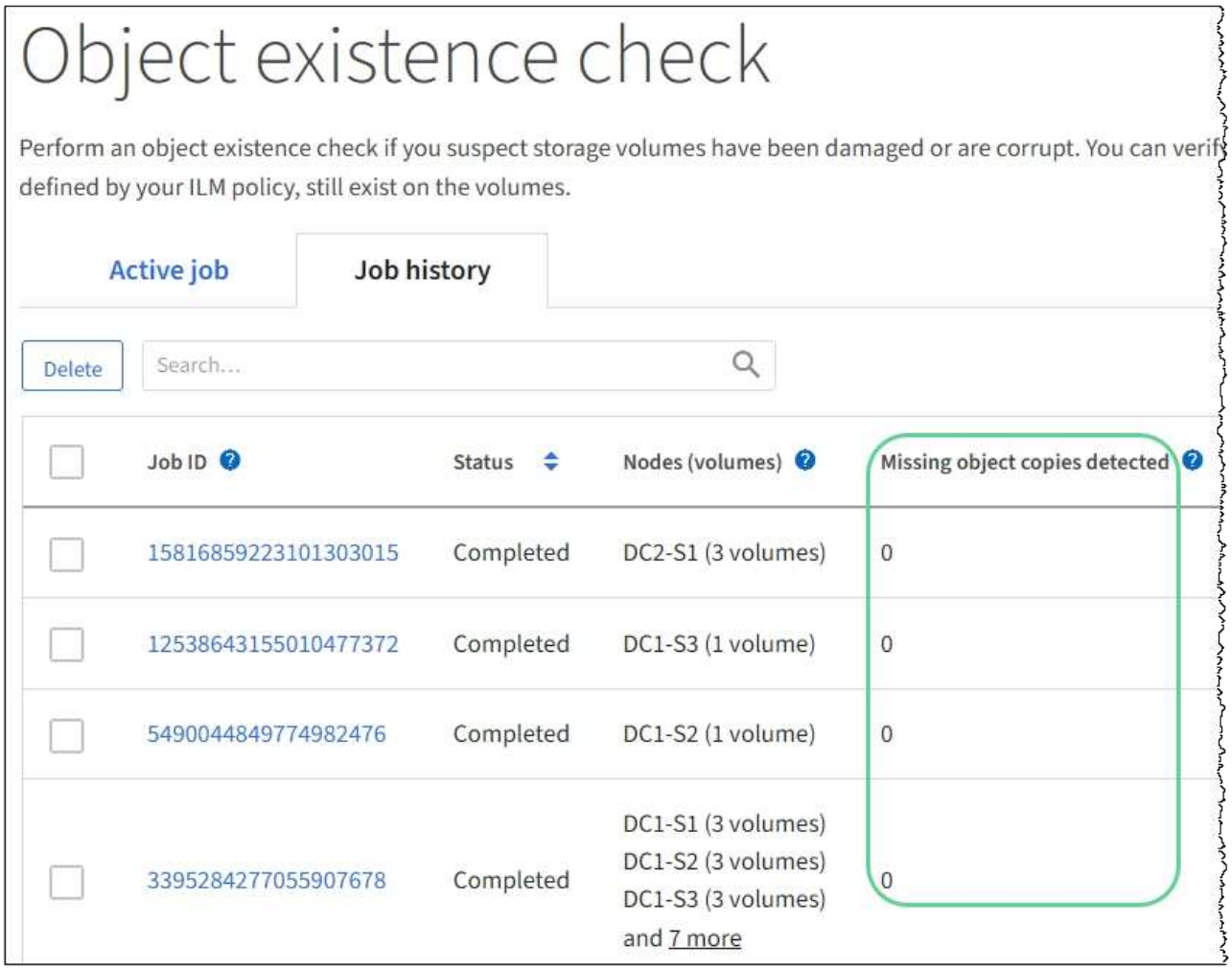


- Para comprobar la verificación de fragmentos codificados por borrado, seleccione ***Storage Node*** > **ILM** y observe los atributos de la sección verificación de códigos de borrado.



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** > **verificación de existencia de objetos** > **Historial de trabajos**.
   b. Analice la columna copias detectadas de objetos que faltan. Si algún trabajo resultó en 100 o más copias de objetos faltantes y se ha activado la alerta de **Objetos perdidos**, póngase en contacto con el soporte técnico.



Supervisar eventos

Es posible supervisar los eventos que detecta un nodo de grid, incluidos los eventos personalizados que se crearon para realizar el seguimiento de los eventos que se registran en el servidor de syslog. El mensaje último evento que se muestra en Grid Manager proporciona más información acerca del evento más reciente.

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

La alarma SMTT (total de eventos) puede activarse repetidamente por problemas como problemas de red, cortes de energía o actualizaciones. Esta sección contiene información sobre la investigación de eventos para que pueda comprender mejor por qué se han producido estas alarmas. Si se ha producido un evento debido a un problema conocido, es seguro restablecer los contadores de eventos.

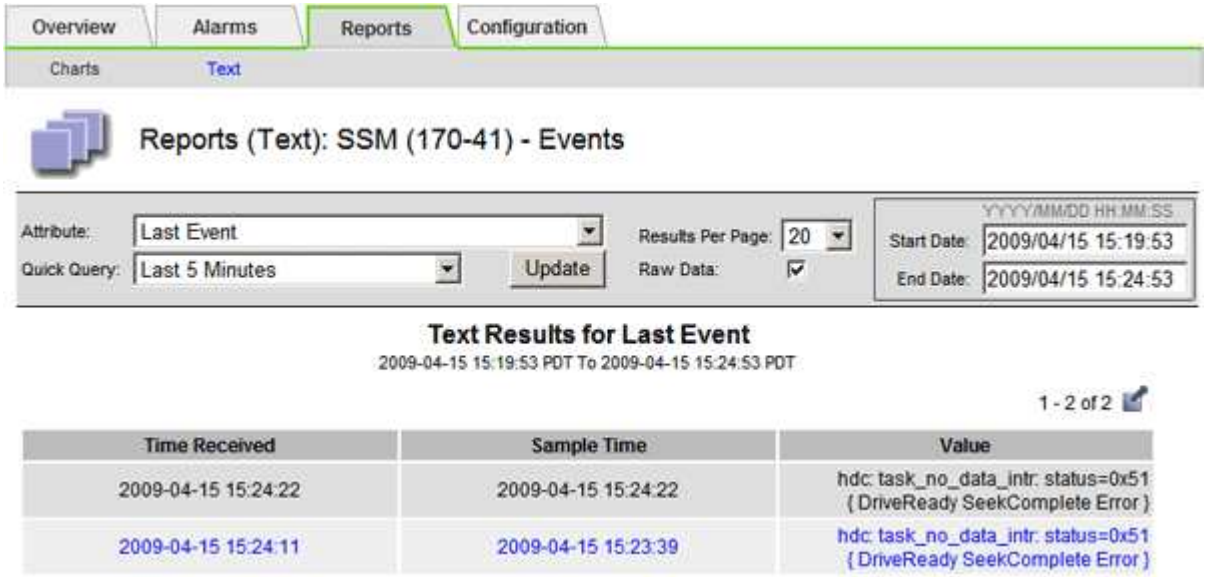
Pasos

1. Revise los eventos del sistema para cada nodo de grid:
   a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
   b. Seleccione ***site*** > ***grid node*** > **SSM** > **Eventos** > **Descripción general** > **Principal**.
2. Generar una lista de mensajes de eventos anteriores para ayudar a aislar los problemas que ocurrieron en el pasado:

a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
b. Seleccione ***site*** > ***grid node*** > **SSM** > **Eventos** > **Informes**.
c. Seleccione **texto**.

   El atributo **último evento** no se muestra en la "vista de gráficos". Para verlo:

d. Cambie **atributo** a **último evento**.
e. Opcionalmente, seleccione un período de tiempo para **Consulta rápida**.
f. Seleccione **Actualizar**.



Cree eventos de syslog personalizados

Los eventos personalizados permiten realizar el seguimiento de todos los eventos de usuario del kernel, del daemon, de los errores y de nivel crítico que se hayan registrado en el servidor de syslog. Un evento personalizado puede ser útil para supervisar la aparición de mensajes de registro del sistema (y por lo tanto, eventos de seguridad de la red y fallos de hardware).

Acerca de esta tarea

Considere la posibilidad de crear eventos personalizados para supervisar problemas recurrentes. Las siguientes consideraciones se aplican a eventos personalizados.

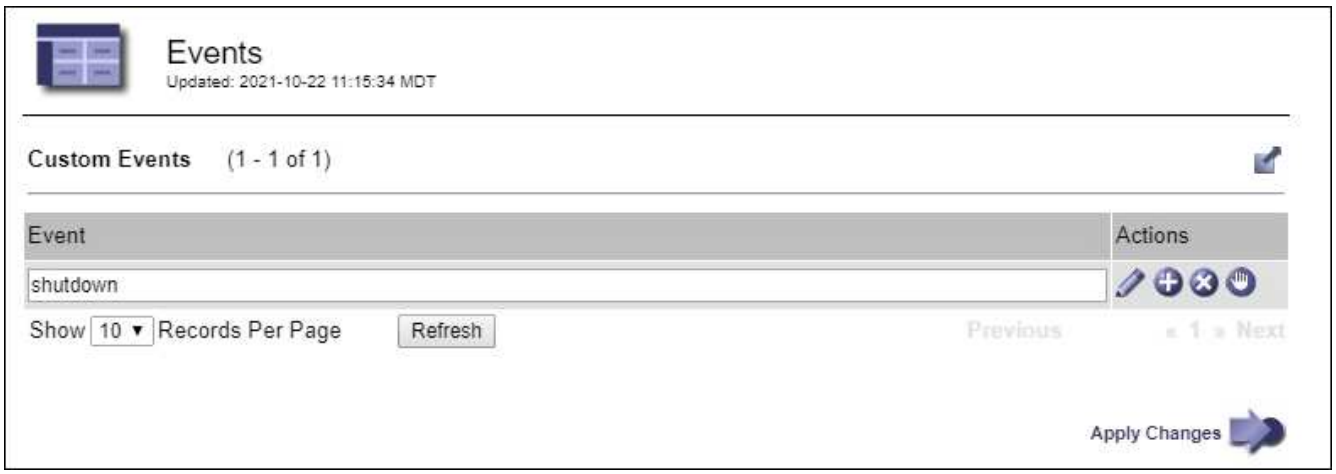
- Después de crear un evento personalizado, se supervisa cada incidencia de él.
- Para crear un evento personalizado basado en palabras clave de `/var/local/log/messages` los registros de dichos archivos deben ser:
  - Generado por el núcleo
  - Generado por daemon o programa de usuario en el nivel de error o crítico

Nota: no todas las entradas del `/var/local/log/messages` los archivos se emparejarán a menos que cumplan los requisitos indicados anteriormente.

Pasos

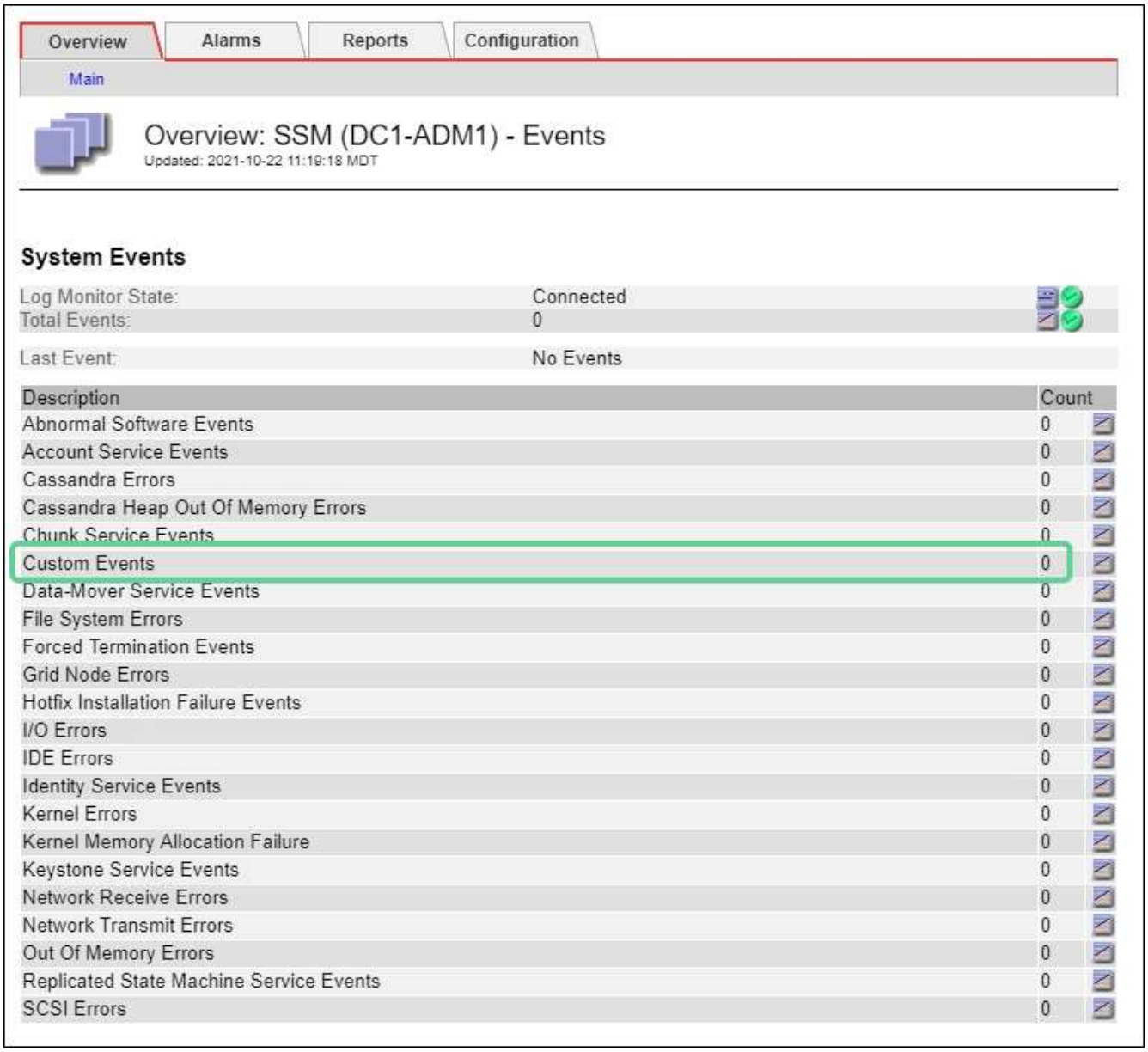
1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Eventos personalizados**.

2. Haga clic en **Editar** (O **Insertar** si no es el primer evento).
3. Escriba una cadena de evento personalizada, por ejemplo, shutdown



4. Seleccione **aplicar cambios**.
5. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
6. Seleccione ***Grid node*** > **SSM** > **Eventos**.
7. Busque la entrada Eventos personalizados en la tabla Eventos y supervise el valor de **Count**.

   Si aumenta el número, se activará un evento personalizado que supervise en ese nodo de grid.



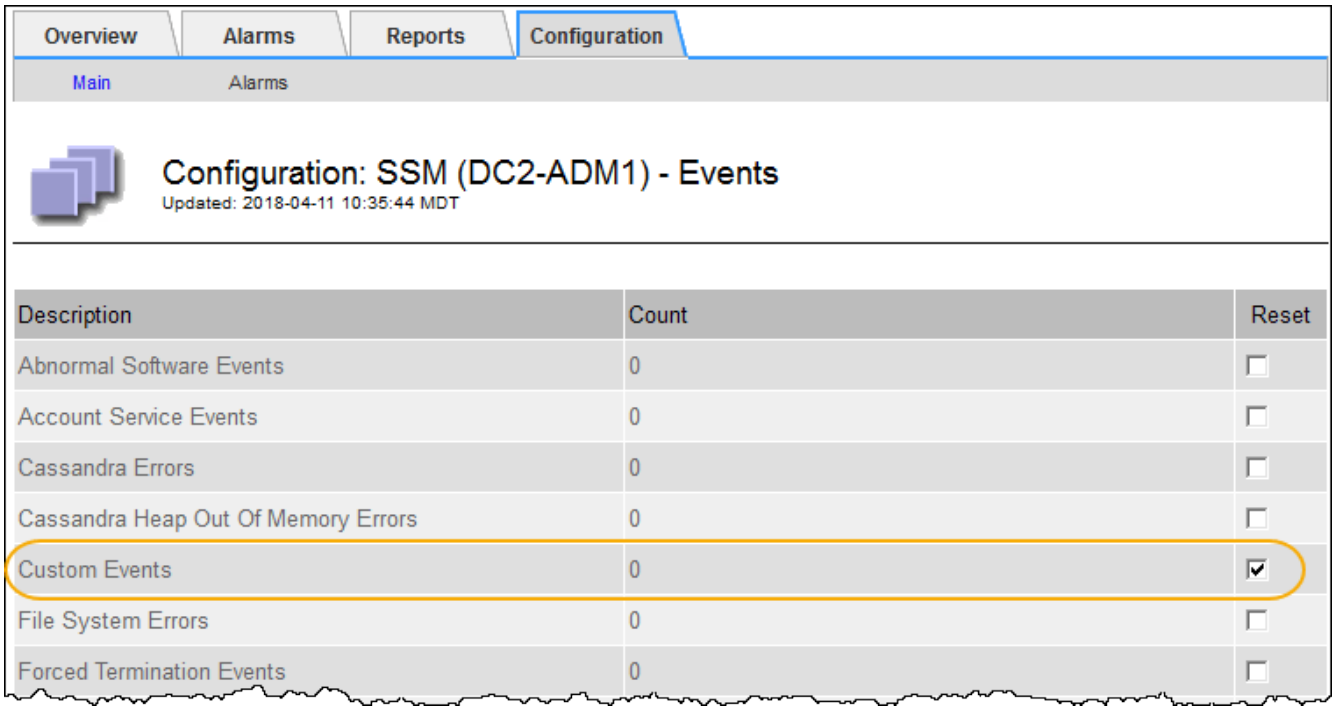
Restablece el número de eventos personalizados a cero

Si desea restablecer el contador solo para eventos personalizados, debe usar la página Grid Topology del menú de soporte.

El restablecimiento de un contador hace que la alarma se active en el siguiente evento. Por el contrario, cuando se reconoce una alarma, esa alarma sólo se vuelve a activar si se alcanza el siguiente nivel de umbral.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***grid node*** > **SSM** > **Eventos** > **Configuración** > **Principal**.
3. Seleccione la casilla de verificación **Reset** para eventos personalizados.



4. Seleccione **aplicar cambios**.

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 o Swift hace 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.

Para facilitar el acceso a los registros de auditoría, usted podrá "Configure el acceso del cliente de auditoría para NFS". También es posible acceder a los archivos del registro de auditoría directamente desde la línea de comandos del nodo de administración.

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. Consulte "Configurar los mensajes de

auditoría y los destinos de registro".

Para obtener detalles sobre el archivo de registro 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 utilizar Grid Manager para recuperar los archivos de registro y los datos del sistema (incluidos los datos de configuración) del sistema StorageGRID.

Antes de empezar

- Debe haber iniciado sesión en Grid Manager en el nodo de administración principal mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Debe tener la clave de acceso de aprovisionamiento.

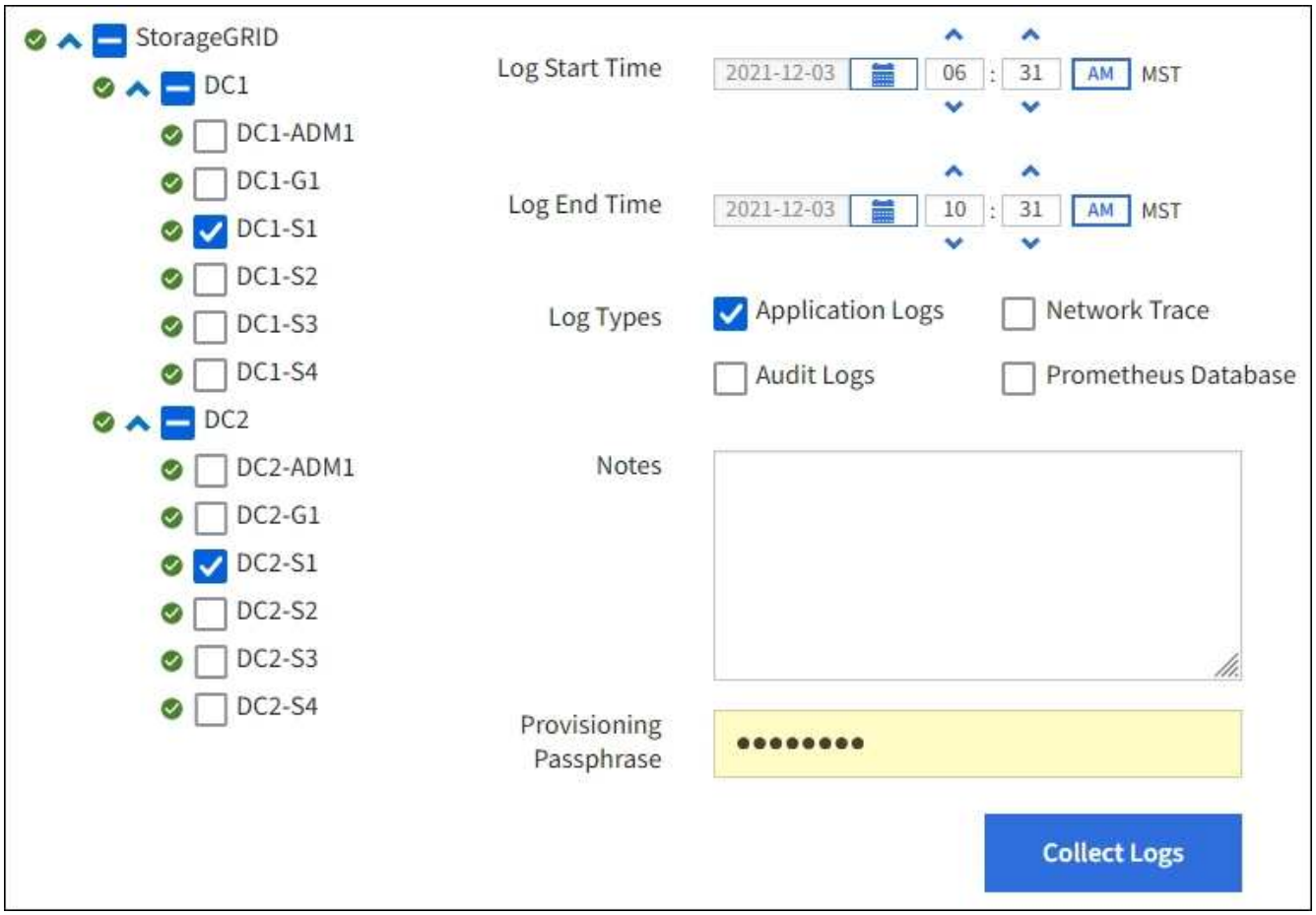
Acerca de esta tarea

Puede utilizar Grid Manager para recopilar "archivos de registro", datos del sistema y datos de configuración de cualquier nodo de cuadrícula durante el período de tiempo seleccionado. Los datos se recopilan y archivan en un archivo .tar.gz que se puede descargar en el equipo local.

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. Consulte "Configurar los mensajes de auditoría y los destinos de registro".

Pasos

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



2. Seleccione los nodos de grid para los que desea recoger archivos de registro.

   Según sea necesario, puede recopilar archivos de registro de toda la cuadrícula o de la ubicación del centro de datos.

3. Seleccione **Hora de inicio** y **Hora de finalización** para establecer el intervalo de tiempo 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 de un grid grande, el archivo de registro puede ser demasiado grande para almacenarse en un nodo o demasiado grande para recogerlo en el nodo de administración principal para su descarga. Si esto ocurre, debe reiniciar la recopilación de registros con un conjunto de datos más pequeño.

4. Seleccione los tipos de registros que desea recoger.
   - **Registros de aplicaciones**: Registros específicos de aplicaciones que el soporte técnico utiliza con mayor frecuencia para la resolución de problemas. Los registros recopilados son un subconjunto de los registros de aplicación disponibles.
   - **Registros de auditoría**: Registros que contienen los mensajes de auditoría generados durante el funcionamiento normal del sistema.
   - **Traza de red**: Registros utilizados para la depuración de red.
   - **Prometheus Database**: Métricas de series temporales de los servicios en todos los nodos.
5. Opcionalmente, introduzca notas sobre los archivos de registro que está recopilando en el cuadro de texto **Notas**.

   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 acerca de la colección de archivos de registro. La `info.txt` el archivo se guarda en el paquete de archivo de registro.

6. Introduzca la frase de acceso de aprovisionamiento del sistema StorageGRID en el cuadro de texto **frase de paso** de aprovisionamiento.
7. Seleccione **recopilar registros**.

   Al enviar una nueva solicitud, se elimina la colección anterior de archivos de registro.

   Puede utilizar la página Logs para supervisar el progreso de la recopilación de archivos de registro de cada nodo de cuadrícula.

   Si recibe un mensaje de error acerca del tamaño del registro, intente recopilar registros por un periodo más corto de tiempo o para menos nodos.

8. Seleccione **Descargar** cuando se haya completado la recopilación de archivos de registro.

   El archivo *.tar.gz* contiene todos los archivos de registro de todos los nodos de grid en los que la recopilación de registros se realizó correctamente. Dentro del archivo combinado *.tar.gz*, hay un archivo de registro para cada nodo de cuadrícula.

Después de terminar

Puede volver a descargar el paquete de archivo de registro más adelante si lo necesita.

Opcionalmente, puede seleccionar **Eliminar** para eliminar el paquete de archivo de registro y liberar espacio en disco. El paquete de archivo de registro actual se elimina automáticamente la próxima vez que se recopilan archivos de registro.

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

- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Debe tener el acceso root u otro permiso de configuración de grid.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. En la pestaña **Acciones**, selecciona **Enviar AutoSupport activado por el usuario**.

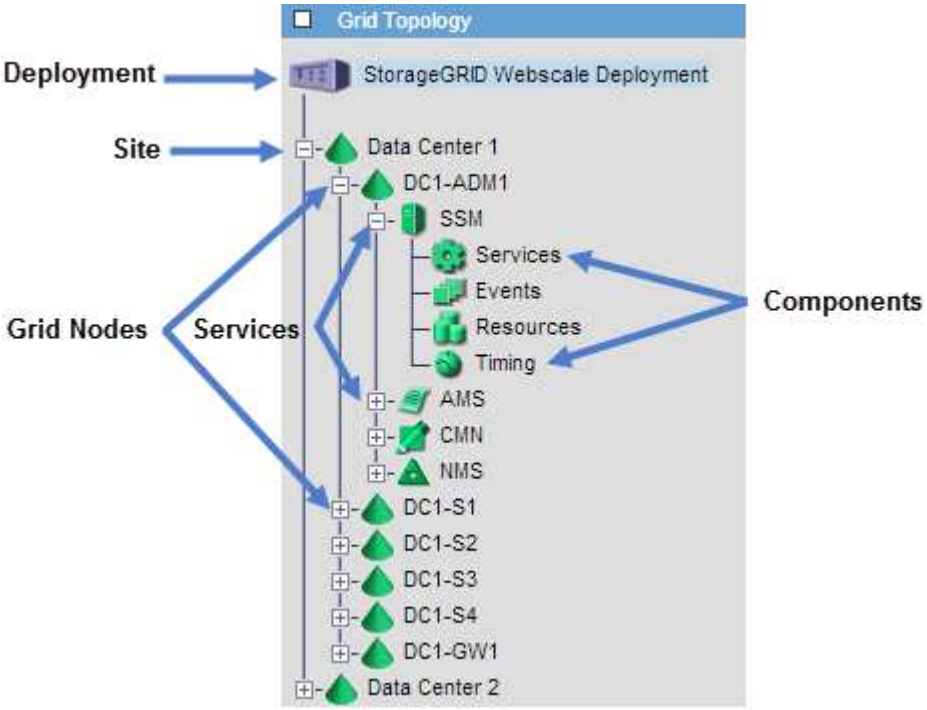
   StorageGRID intenta enviar un paquete de AutoSupport al sitio de soporte de NetApp. Si el intento se realiza correctamente, se actualizan los valores **resultado más reciente** y **tiempo más reciente** de la ficha **resultados**. Si hay un problema, el valor **Resultado más reciente** se actualiza a “Error” y StorageGRID no intenta enviar el paquete AutoSupport de nuevo.

   > Después de enviar un paquete AutoSupport activado por el usuario, actualice la página AutoSupport en el explorador al cabo de 1 minuto para acceder a los resultados más recientes.

Abra el árbol de topología de cuadrícula

El árbol de topología de cuadrícula proporciona acceso a información detallada sobre los elementos del sistema StorageGRID, incluidos los sitios, los nodos de cuadrícula, los servicios y los componentes. En la mayoría de los casos, sólo necesita acceder al árbol de topología de cuadrícula cuando se le indique en la documentación o cuando trabaje con soporte técnico.

Para acceder al árbol de topología de cuadrícula, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.



Para expandir o contraer el árbol de topología de cuadrícula, haga clic en ⊞ o. ⊟ en el nivel del sitio, nodo o servicio. Para expandir o contraer todos los elementos de todo el sitio o de cada nodo, mantenga pulsada la tecla **<Ctrl>** y haga clic en.

Atributos de la StorageGRID

Los atributos notifican valores y Estados para muchas de las funciones del sistema StorageGRID. Los valores de los atributos están disponibles para cada nodo de la cuadrícula, cada sitio y toda la cuadrícula.

Los atributos de StorageGRID se utilizan en varios lugares de Grid Manager:

- **Página nodos**: Muchos de los valores mostrados en la página nodos son atributos StorageGRID. (Las métricas de Prometheus también se muestran en las páginas de nodos.)
- **Alarmas**: Cuando los atributos alcanzan valores de umbral definidos, las alarmas StorageGRID (sistema heredado) se activan a niveles de gravedad específicos.
- **Árbol de topología de cuadrícula**: Los valores de atributo se muestran en el árbol de topología de cuadrícula (**SUPPORT** > **Tools** > **topología de cuadrícula**).
- **Eventos**: Los eventos del sistema se producen cuando ciertos atributos registran un error o condición de fallo para un nodo, incluidos errores como errores de red.

Valores de atributo

Los atributos se notifican con el mejor esfuerzo y son aproximadamente correctos. Las actualizaciones de atributos se pueden perder en determinadas circunstancias, como el bloqueo de un servicio o el fallo y la reconstrucción de un nodo de cuadrícula.

Además, los retrasos de propagación pueden ralentizar la generación de informes de atributos. Los valores actualizados de la mayoría de los atributos se envían al sistema StorageGRID a intervalos fijos. Puede tardar varios minutos en que una actualización sea visible en el sistema, y se pueden notificar dos atributos que cambian más o menos simultáneamente en momentos ligeramente diferentes.

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 un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".

Acerca de esta tarea

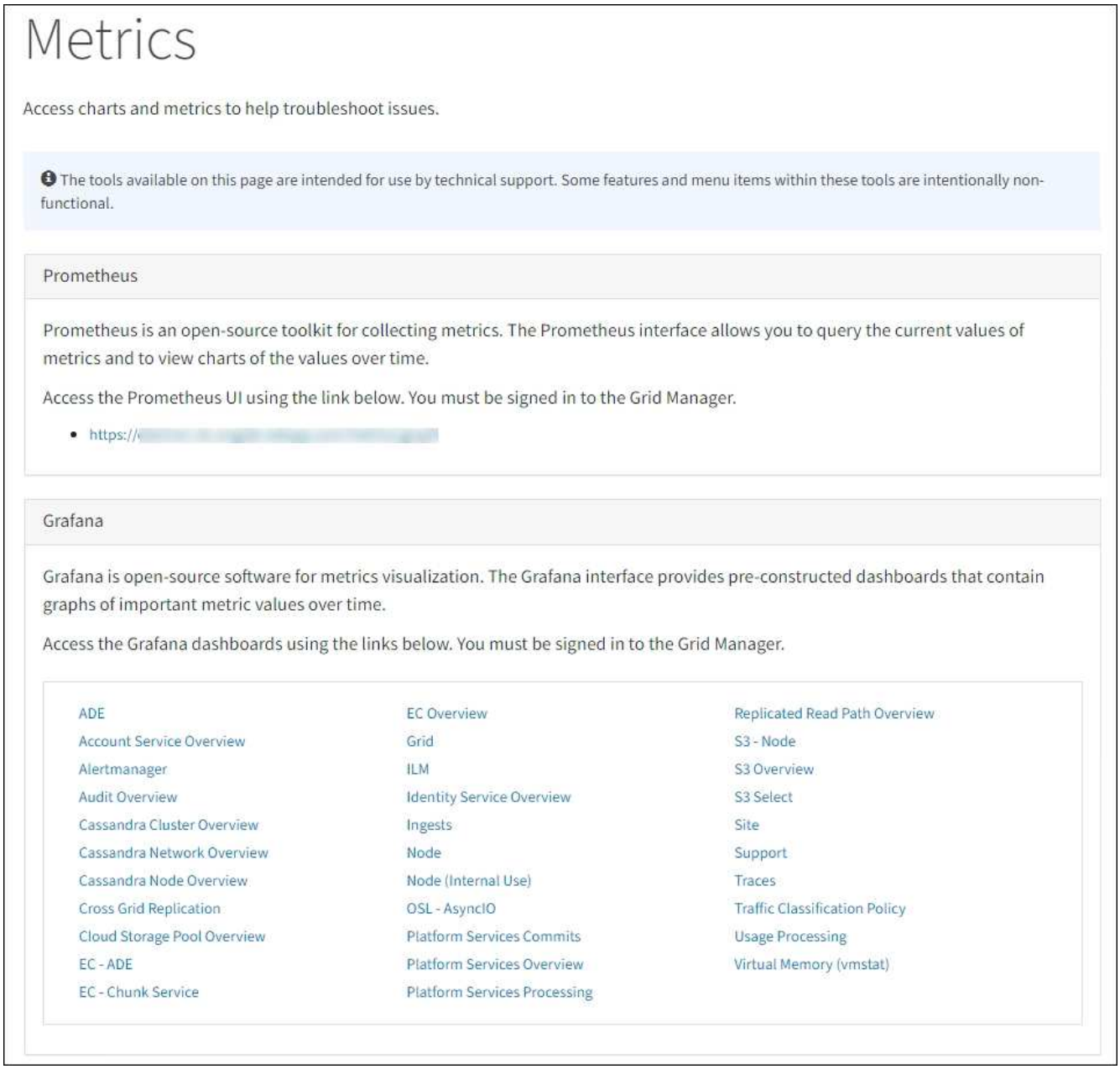
La página Metrics le permite acceder a las interfaces de usuario Prometheus y Grafana. Prometheus es un software de código abierto para recopilar métricas. Grafana es un software de código abierto para la visualización de métricas.

> 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 lo indicado por el soporte técnico, seleccione **ASISTENCIA** > **Herramientas** > **métricas**.

   A continuación se muestra un ejemplo de la página Metrics:



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.

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 un "navegador web compatible".
- Ya 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.

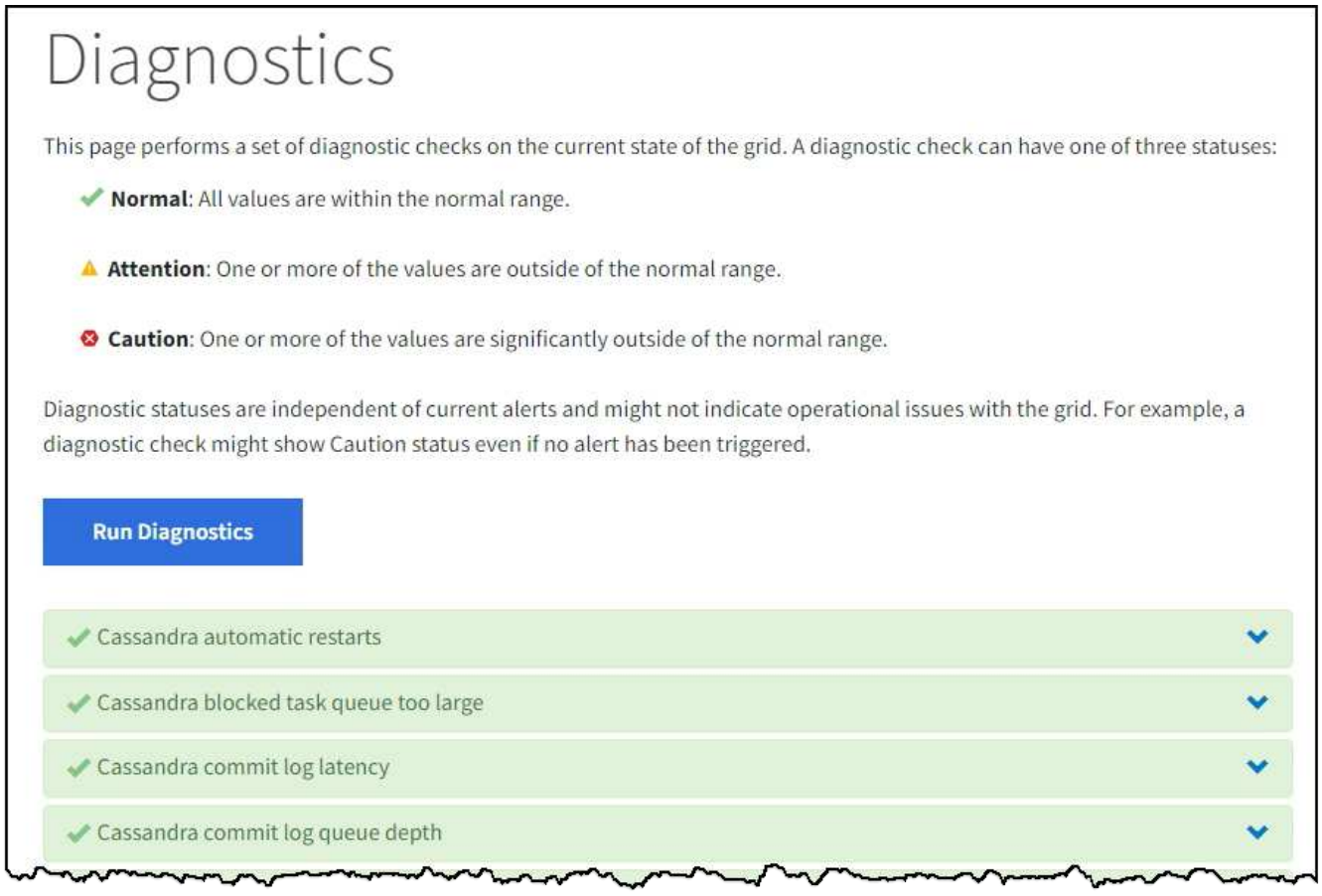
Los Estados de diagnóstico son independientes de las alertas actuales y podrían no indicar problemas operativos con la cuadrícula. Por ejemplo, una comprobación de diagnóstico puede mostrar el estado Precaución aunque no se haya activado ninguna alerta.

Pasos

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

   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, todos los diagnósticos tienen un estado normal.



2. Para obtener más información acerca de un diagnóstico específico, haga clic en cualquier lugar de la fila.

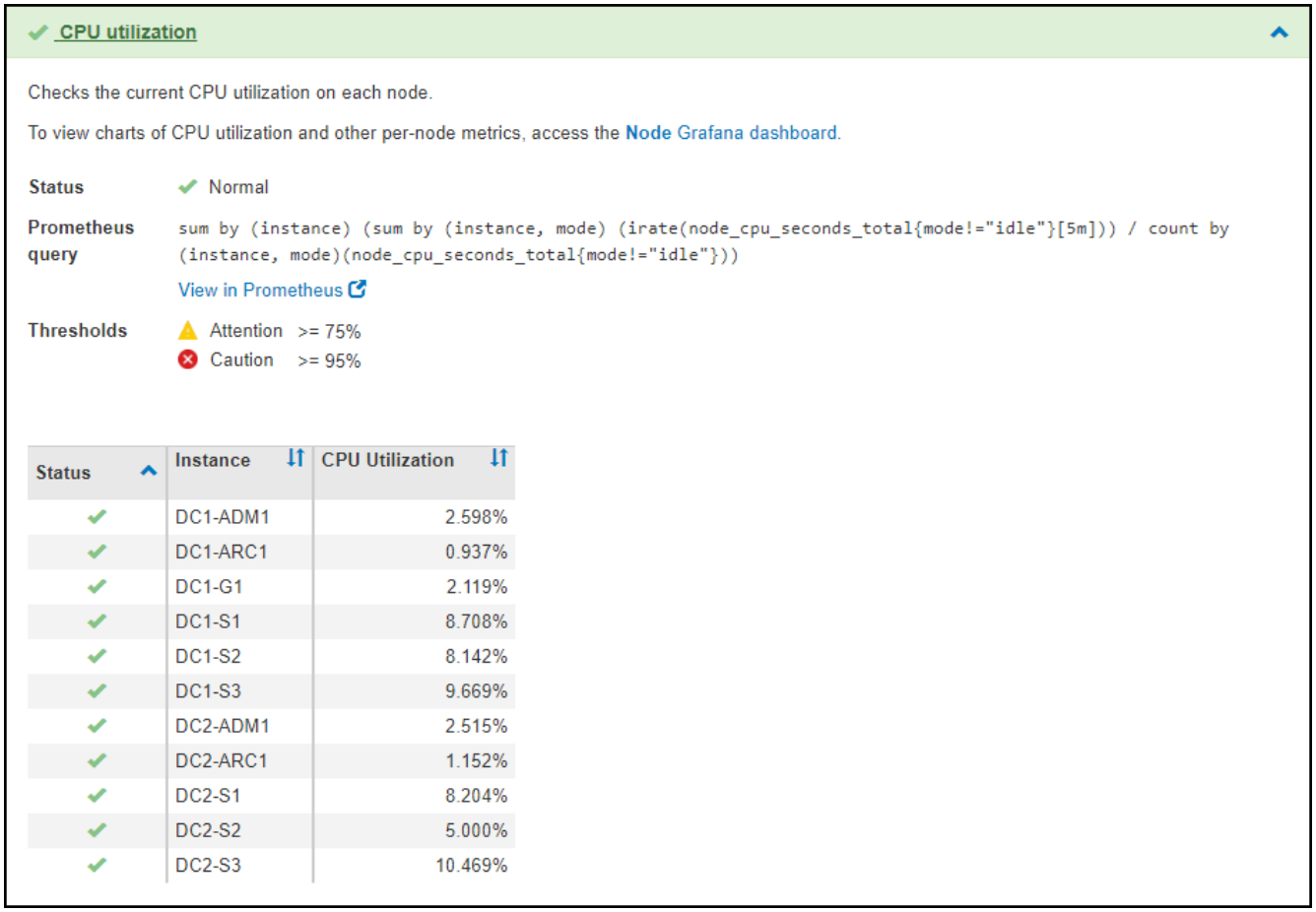
   Aparecen detalles sobre el diagnóstico y sus resultados actuales. Se enumeran los siguientes detalles:

   - **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**: Tabla que muestra el estado y el valor del diagnóstico en todo el sistema StorageGRID.
  En este ejemplo, se muestra el uso actual de la CPU para cada nodo de un sistema StorageGRID. Todos los valores de nodo 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 Grafana relacionados con este diagnóstico, haga clic en el enlace **Grafana Dashboard**.

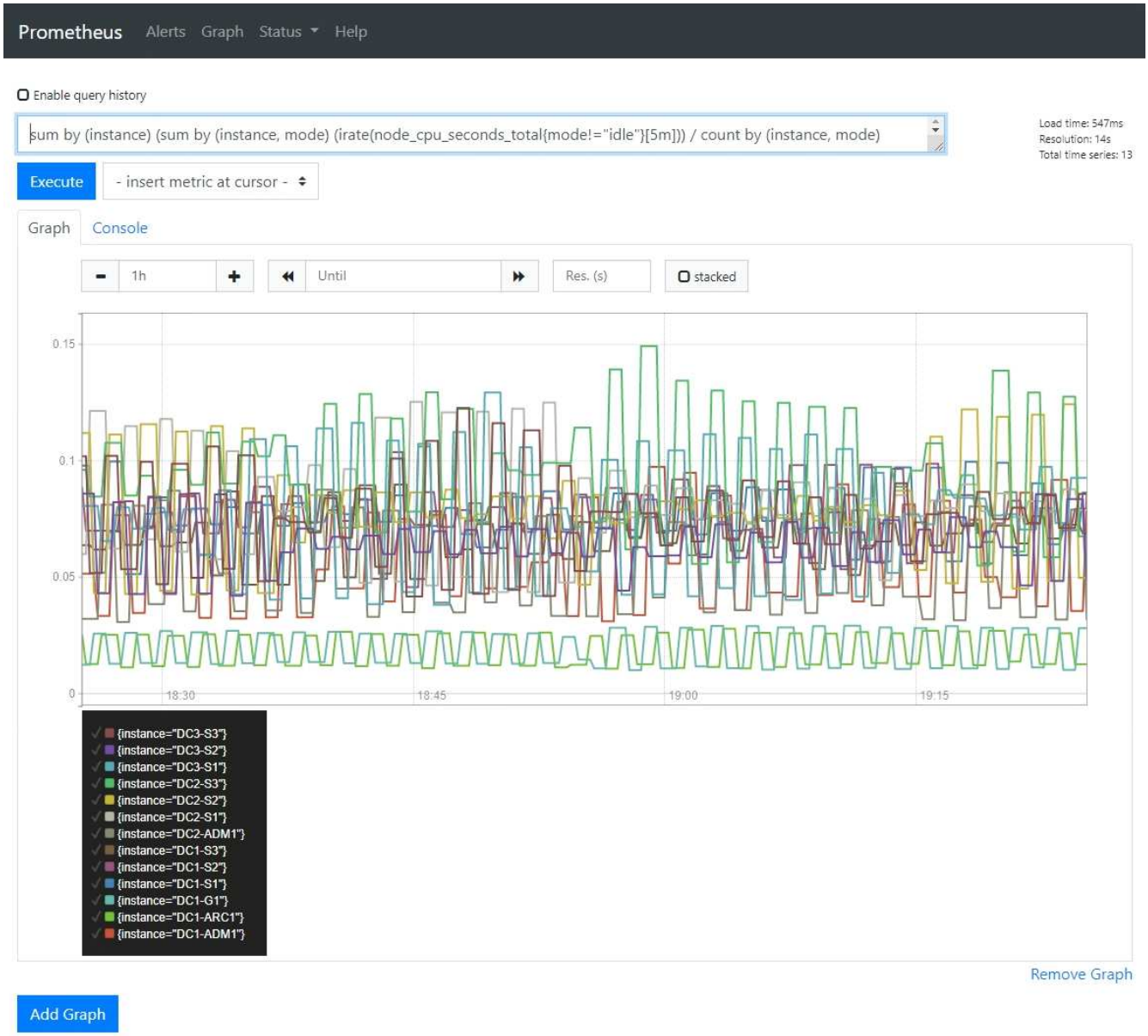
   Este enlace no se muestra para todos los diagnósticos.

   Aparece el panel Grafana relacionado. En este ejemplo, aparece el panel nodo que muestra la utilización de la CPU a lo largo del tiempo de este nodo, así como otros gráficos Grafana del nodo.

   > También puede acceder a los paneles Grafana preconstruidos desde la sección Grafana de la página **SUPPORT** > **Tools** > **Metrics**.

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.



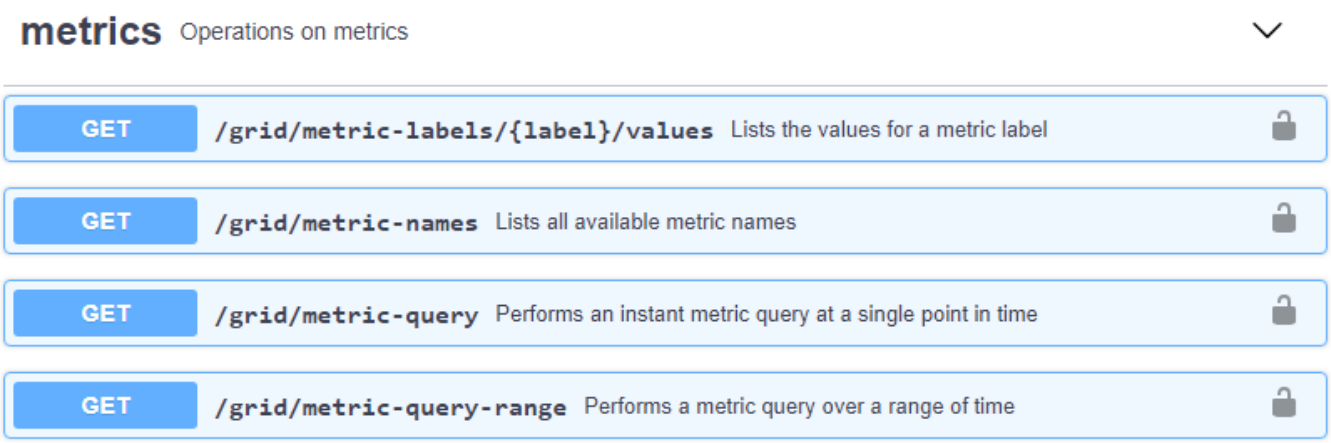
Crear aplicaciones de supervisión personalizadas

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 "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 icono de ayuda y selecciona **Documentación de la API** > **Métricas**.



Los detalles de cómo implementar una aplicación de supervisión personalizada están fuera del alcance de esta documentación.

Solucionar los problemas del sistema StorageGRID

Solucionar problemas en un sistema StorageGRID: Descripción general

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

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

Defina el problema

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

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

Pregunta	Ejemplo de respuesta
¿Qué está haciendo o no el sistema StorageGRID? ¿Cuáles son sus síntomas?	Las aplicaciones cliente informan de que los objetos no se pueden procesar en StorageGRID.
¿Cuándo comenzó el problema?	La ingesta de objetos fue denegada por primera vez a las 14:50 del 8 de enero de 2020.
¿Cómo notó el problema por primera vez?	Notificado por la aplicación cliente. También ha recibido notificaciones por correo electrónico de alerta.
¿El problema ocurre de manera consistente, o sólo a veces?	El problema está en curso.

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.

Evalúe el riesgo y el impacto sobre el sistema

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

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

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

Recopilación de datos

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

Tipo de datos que se van a recoger	Por qué recoger estos datos	Instrucciones
Crear una línea de tiempo de los cambios recientes	Los cambios realizados en el sistema StorageGRID, su configuración o su entorno pueden provocar nuevos comportamientos.	• Crear una línea de tiempo de cambios recientes

Tipo de datos que se van a recoger	Por qué recoger estos datos	Instrucciones
Revise las alertas y alarmas	Las alertas y alarmas pueden ayudarle a determinar rápidamente la causa raíz de un problema, proporcionando pistas importantes sobre los problemas subyacentes que podrían estar causando. Revise la lista de alertas y alarmas actuales para ver si StorageGRID ha identificado la causa raíz de un problema. Revise las alertas y alarmas activadas en el pasado para obtener información adicional.	• "Ver las alertas actuales y resueltas" • "Gestionar alarmas (sistema heredado)"
Supervisar eventos	Entre los eventos se incluye cualquier evento de error del sistema o fallo de un nodo, incluidos errores como errores de red. Supervisar eventos para obtener más información acerca de problemas o para ayudar en la solución de problemas.	• "Supervisar eventos"
Identificar tendencias mediante gráficos e informes de texto	Las tendencias pueden proporcionar pistas valiosas acerca de cuándo aparecieron los problemas por primera vez, y pueden ayudarle a entender la rapidez con la que las cosas están cambiando.	• "Utilice gráficos y gráficos" • "Usar informes de texto"
Establecer líneas base	Recopilar información acerca de los niveles normales de varios valores operativos. Estos valores de referencia y las desviaciones de estas líneas de base pueden proporcionar pistas valiosas.	• Establecer líneas base
Realice pruebas de procesamiento y recuperación	Para solucionar problemas de rendimiento con la ingesta y la recuperación, utilice una estación de trabajo para almacenar y recuperar objetos. Compare los resultados con los que se ven al usar la aplicación cliente.	• "SUPERVISE EL RENDIMIENTO DE PUT y GET"
Revisar los mensajes de auditoría	Revise los mensajes de auditoría para seguir las operaciones de StorageGRID con detalle. Los detalles de los mensajes de auditoría pueden ser útiles para solucionar muchos tipos de problemas, incluidos problemas de rendimiento.	• "Revisar los mensajes de auditoría"

Tipo de datos que se van a recoger	Por qué recoger estos datos	Instrucciones
Comprobar la ubicación de objetos y la integridad del almacenamiento	Si tiene problemas de almacenamiento, compruebe que los objetos se encuentren en la ubicación que espera. Compruebe la integridad de los datos de objetos en un nodo de almacenamiento.	• "Supervise las operaciones de verificación de objetos" • "Confirme las ubicaciones de los datos del objeto" • "Verifique la integridad del objeto"
Recopile datos para el soporte técnico	Es posible que el soporte técnico le solicite recopilar datos o revisar información específica para ayudar a resolver problemas.	• "Recopilar archivos de registro y datos del sistema" • "Active manualmente un paquete AutoSupport" • "Revisar las métricas de soporte"

cree una línea de tiempo de los cambios recientes

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

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

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

Momento del cambio	Tipo de cambio	Detalles
Por ejemplo: • ¿Cuándo inició la recuperación del nodo? • ¿Cuándo se completó la actualización de software? • ¿Interrumpió el proceso?	¿Qué ha sucedido? ¿Qué has hecho?	Documente los detalles relevantes sobre el cambio. Por ejemplo: • Detalles de los cambios de red. • Qué revisión se instaló. • Cambio de las cargas de trabajo de los clientes. Asegúrese de anotar si se estaba produciendo más de un cambio al mismo tiempo. Por ejemplo, ¿se ha realizado este cambio mientras se estaba realizando una actualización?

Ejemplos de cambios recientes significativos

A continuación se muestran algunos ejemplos de cambios potencialmente importantes:

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

Establecer líneas base

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

Propiedad	Valor	Cómo obtener
Consumo medio de almacenamiento	GB consumidos/día Porcentaje consumido/día	Vaya a Grid Manager. En la página Nodes, seleccione la cuadrícula completa o un sitio y vaya a la pestaña Storage. En el gráfico almacenamiento usado - datos de objeto, busque un punto en el que la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar cuánto almacenamiento se consume cada día Puede recopilar esta información para todo el sistema o para un centro de datos específico.
Consumo medio de metadatos	GB consumidos/día Porcentaje consumido/día	Vaya a Grid Manager. En la página Nodes, seleccione la cuadrícula completa o un sitio y vaya a la pestaña Storage. En el gráfico almacenamiento usado - metadatos de objeto, busque un punto en el que la línea sea bastante estable. Sitúe el cursor sobre el gráfico para estimar la cantidad de almacenamiento de metadatos que se consume cada día Puede recopilar esta información para todo el sistema o para un centro de datos específico.
Tasa de operaciones de S3/Swift	Operaciones por segundo	En el panel de Grid Manager, seleccione **Rendimiento** > **S3 operaciones** o **Rendimiento** > **Operaciones Swift**. Para ver las tasas y recuentos de procesamiento y recuperación de un sitio o nodo específico, seleccione **NODES** > ***site o Storage Node*** > **objetos**. Coloque el cursor sobre el gráfico de ingesta y recuperación para S3 o Swift.
Han fallado las operaciones de S3/Swift	Operaciones	Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. En la pestaña Overview de la sección API Operations, vea el valor de las operaciones de S3 - Failed o Swift - Failed.
Tasa de evaluación de ILM	Objetos por segundo	En la página Nodes, seleccione ***grid*** > **ILM**. En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar un valor de línea base para **Tasa de evaluación** para su sistema.

Propiedad	Valor	Cómo obtener
Tasa de análisis de ILM	Objetos por segundo	Seleccione **NODES** > ***grid*** > **ILM**. En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar un valor de línea base para **Tasa de exploración** para su sistema.
Objetos en cola de operaciones del cliente	Objetos por segundo	Seleccione **NODES** > ***grid*** > **ILM**. En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar un valor de línea base para **Objetos en cola (de operaciones del cliente)** para su sistema.
Latencia media de consultas	Milisegundos	Seleccione **NODES** > ***Storage Node*** > **Objects**. En la tabla consultas, vea el valor de latencia media.

Análisis de datos

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

El análisis depende-problema, pero en general:

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

Lista de comprobación de información de escalado

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

✓	Elemento	Notas
	Declaración de problema	¿Cuáles son los síntomas del problema? ¿Cuándo comenzó el problema? ¿Ocurre de manera sistemática o intermitente? Si es intermitente, ¿qué veces ha ocurrido? Defina el problema
	Evaluación del impacto	¿Cuál es la gravedad del problema? ¿Cómo afecta a la aplicación cliente? • ¿Se ha conectado el cliente correctamente anteriormente? • ¿El cliente puede procesar, recuperar y eliminar datos?

✔	Elemento	Notas
	ID del sistema StorageGRID	Seleccione **MANTENIMIENTO** > **sistema** > **Licencia**. El ID del sistema de StorageGRID se muestra como parte de la licencia actual.
	Versión de software	En la parte superior de Grid Manager, seleccione el icono de ayuda y seleccione **Acerca de** para ver la versión de StorageGRID.
	Personalización	Resuma cómo se configura el sistema StorageGRID. Por ejemplo, enumere lo siguiente: • ¿El grid utiliza compresión de almacenamiento, cifrado de almacenamiento o cumplimiento de normativas? • ¿Hace ILM objetos replicados o con código de borrado? ¿Garantiza ILM la redundancia de sitios? ¿Las reglas de ILM usan los comportamientos de ingesta de registro equilibrado, estricto o doble?
	Registrar archivos y datos del sistema	Recopile archivos de registro y datos del sistema para su sistema. Seleccione **SUPPORT** > **Tools** > **Logs**. Es posible recopilar registros de toda la cuadrícula o de los nodos seleccionados. Si va a recopilar registros solo para los nodos seleccionados, asegúrese de incluir al menos un nodo de almacenamiento que tenga el servicio ADC. (Los tres primeros nodos de almacenamiento de un sitio incluyen el servicio ADC). "Recopilar archivos de registro y datos del sistema"
	Información de línea de base	Recopile información de la línea de base sobre las operaciones de ingesta, las operaciones de recuperación y el consumo de almacenamiento. Establecer líneas base
	Cronología de los cambios recientes	Crear una línea de tiempo que resume los cambios recientes realizados en el sistema o en su entorno. Crear una línea de tiempo de cambios recientes
	Historia de los esfuerzos para diagnosticar el problema	Si ha tomado medidas para diagnosticar o solucionar el problema por su cuenta, asegúrese de registrar los pasos que ha realizado y el resultado.

Solucione problemas de almacenamiento y objetos

Confirme las ubicaciones de los datos del objeto

Dependiendo del problema, es posible que desee hacerlo "confirme dónde se almacenan los datos de objetos". Por ejemplo, puede que desee verificar que la política de ILM esté funcionando como se espera y que los datos de objetos se almacenen donde estaba previsto.

Antes de empezar

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

Pasos

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

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

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

4. Seleccione **Buscar**.

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

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

- Para los objetos S3, cualquier par de etiqueta de objeto clave-valor asociado al objeto.
- Para las copias de objetos replicadas, la ubicación de almacenamiento actual de cada copia.
- Para las copias de objetos codificados de borrado, la ubicación actual de almacenamiento de cada fragmento.
- Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluido el nombre del bloque externo y el identificador único del objeto.
- Para objetos segmentados y objetos multipartes, una lista de segmentos de objetos que incluyen identificadores de segmentos y tamaños de datos. Para objetos con más de 100 segmentos, sólo se muestran los primeros 100 segmentos.
- Todos los metadatos del objeto en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen los metadatos internos del sistema que no se garantiza que continúen del lanzamiento al lanzamiento.

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

System Metadata

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

Replicated Copies

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

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```

Errores del almacén de objetos (volumen de almacenamiento)

El almacenamiento subyacente en un nodo de almacenamiento se divide en almacenes de objetos. Los almacenes de objetos también se conocen como volúmenes de almacenamiento.

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

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

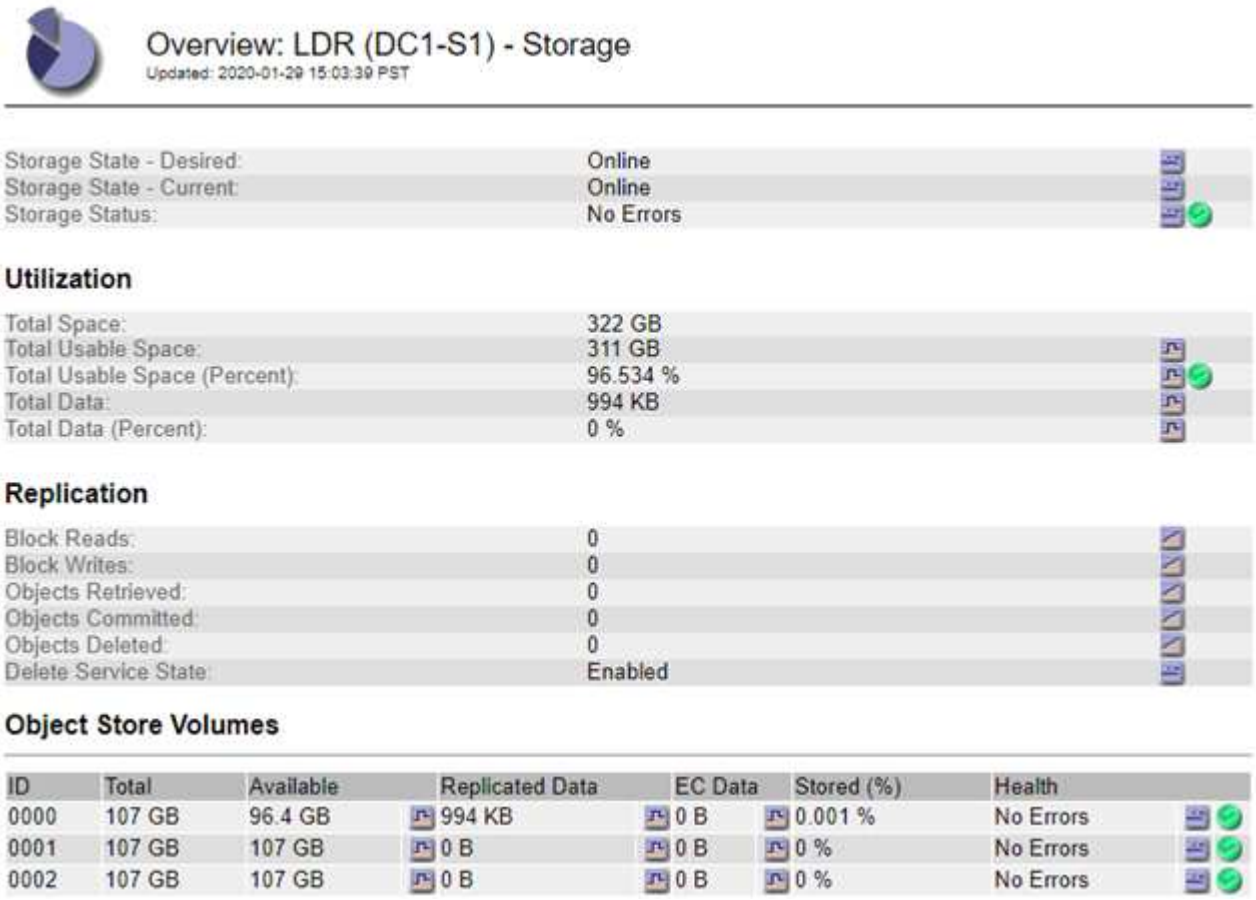
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online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

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

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

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



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

Verifique la integridad del objeto

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

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

¿Qué es la verificación en segundo plano?

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

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

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

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

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

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

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

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

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

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

Cambie la tasa de verificación en segundo plano

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

Antes de empezar

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

Acerca de esta tarea

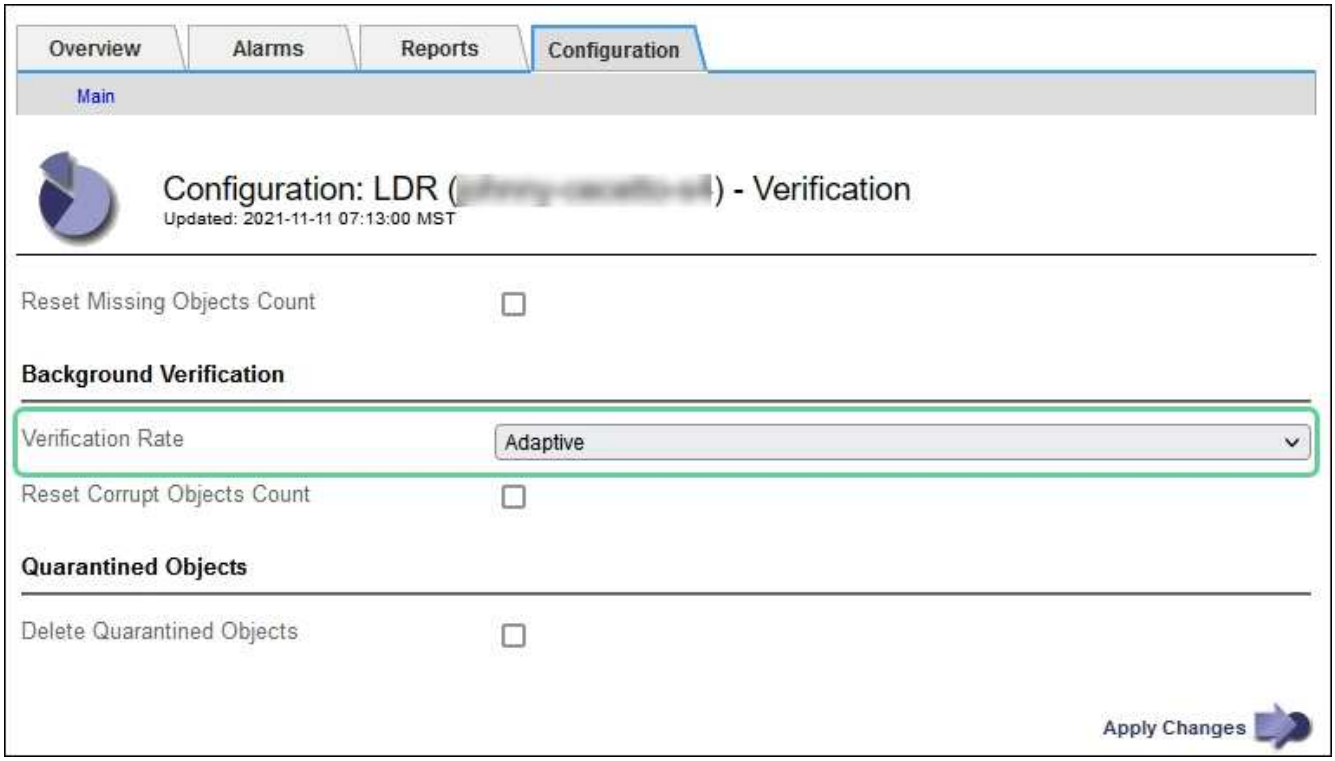
Es posible cambiar la tasa de verificación para la verificación en segundo plano en un nodo de almacenamiento:

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

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

Pasos

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



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

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

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

- Si se puede extraer el identificador del objeto, StorageGRID crea automáticamente una nueva copia de los datos del objeto. La nueva copia se puede realizar en cualquier parte del sistema de StorageGRID que cumpla las políticas de gestión de la vida útil de la información activas.
- Si el identificador de objeto no se puede extraer (porque se ha dañado), la métrica **Objetos corruptos no identificados** aumenta y se activa la alerta **Objeto corrupto no identificado detectado**.

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

8. Supervise los resultados de la verificación en segundo plano para objetos codificados mediante borrado.

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

   a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
   b. Seleccione ***Storage Node*** > **LDR** > **código de borrado**.
   c. En la tabla resultados de verificación, supervise el atributo fragmentos dañados detectados (ECCD).

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

10. Si está seguro de que los objetos en cuarentena no son necesarios, puede eliminarlos.

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

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

¿Qué es la comprobación de la existencia de objetos?

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

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

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

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

Ejecute la comprobación de existencia de objetos

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

Antes de empezar

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

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

Acerca de esta tarea

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

Pasos

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

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

   Puede buscar por nombre de nodo o sitio.

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

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

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

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

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

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

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

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

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

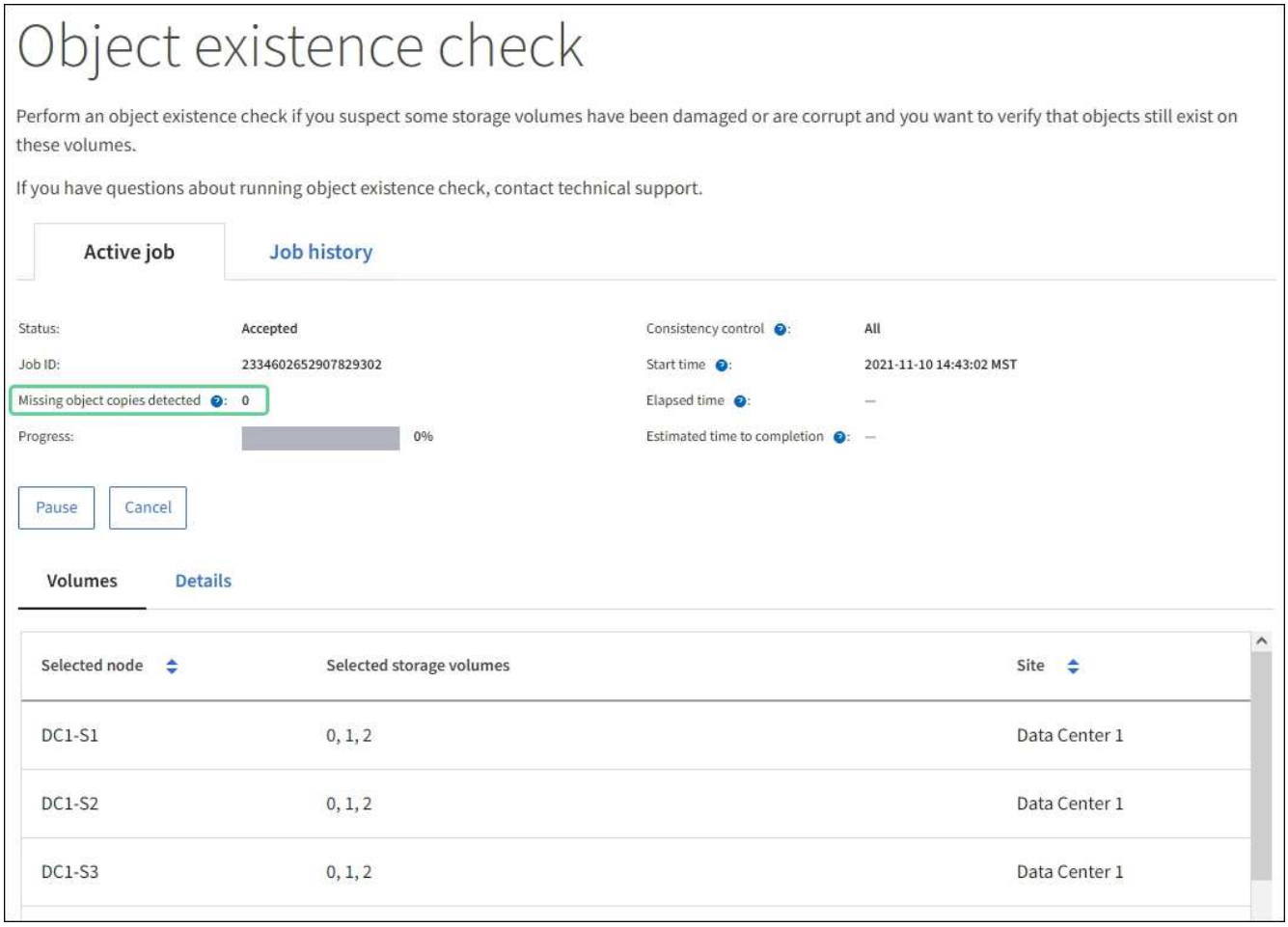
   - El trabajo finaliza.
   - El trabajo se pone en pausa o se cancela. Puede reanudar un trabajo que haya pausado, pero no puede reanudar un trabajo que haya cancelado.
   - El trabajo se cala. Se activa la alerta **comprobación de existencia de objeto ha calado**. Siga las acciones correctivas especificadas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

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

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

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

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



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

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

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

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

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

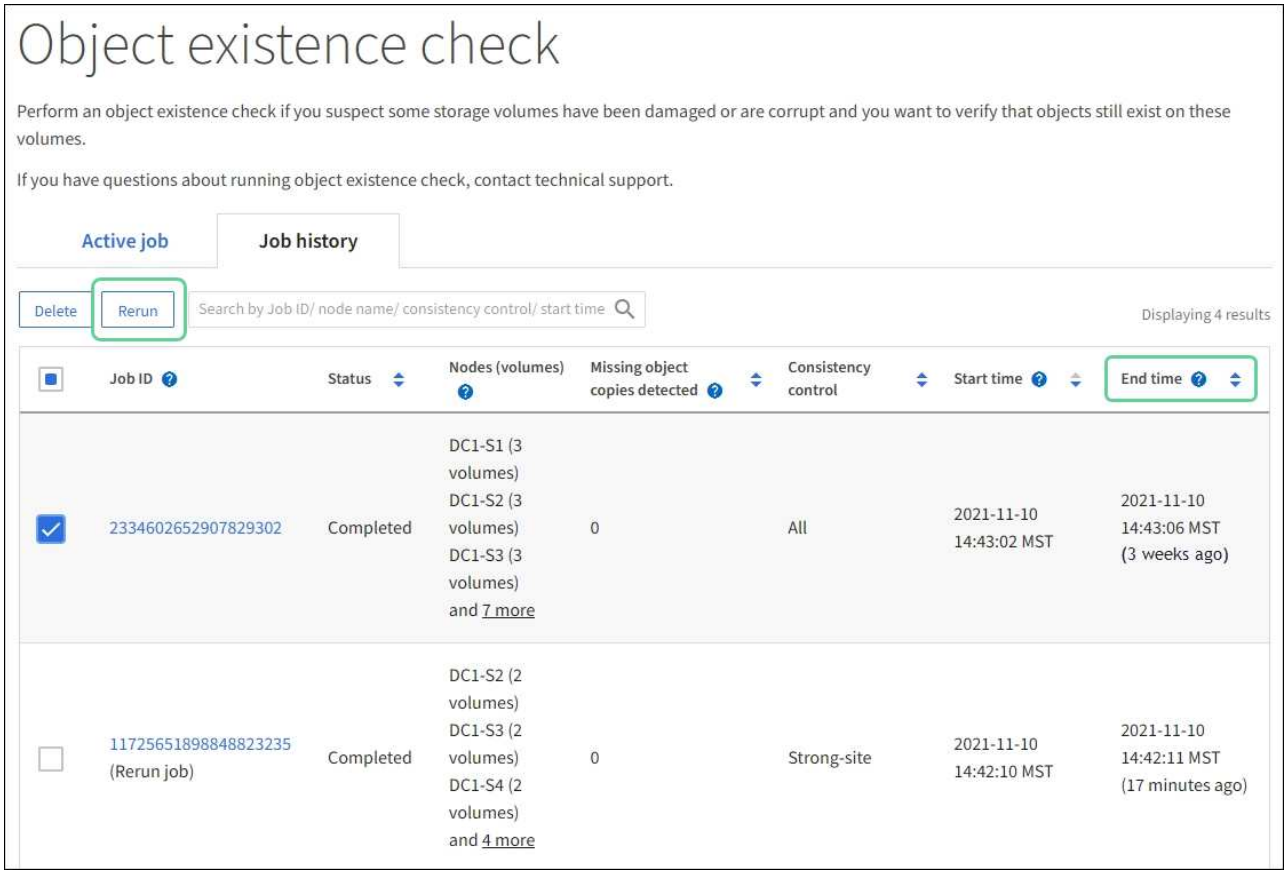
a. Seleccione **MANTENIMIENTO** > **verificación de existencia de objetos** > **Historial de trabajos**.

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

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

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

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



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

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

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

Después de terminar

Si aún tiene dudas sobre la integridad de los datos, vaya a **SUPPORT** > **Tools** > **Grid topolog** > ***site*** > ***Storage Node*** > **LDR** > **Verification** > **Configuration** > **Main** y aumente la velocidad de verificación de fondo. La verificación en segundo plano comprueba la corrección de todos los datos de objeto almacenados y repara cualquier problema que encuentre. Encontrar y reparar posibles problemas lo más rápidamente posible reduce el riesgo de pérdida de datos.

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

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

Antes de empezar

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

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

Pasos

1. Vaya a **CONFIGURACIÓN** > **Monitoreo** > **Servidor de auditoría y syslog**.
2. Si las escrituras de cliente son Normal, acceda al registro de auditoría:
   a. Introduzca `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

   e. Introduzca `cd /var/local/log`
   f. Identifique qué inquilinos están usando objetos mayores de 5 GiB.
      i. Introduzca `zgrep SPUT * | egrep "CSIZ\(UI64\):[0-9]*[5-9][0-9]{9}"`
      ii. Para cada mensaje de auditoría de los resultados, consulte `S3AI` Para determinar el ID de cuenta de inquilino. Utilice los otros campos del mensaje para determinar la dirección IP utilizada por el cliente, el depósito y el objeto:

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

Ejemplo de resultados de registro de auditoría

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

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

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

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

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

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

      Ejemplo bycast.log

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

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

Solucionar problemas de datos de objetos perdidos o faltantes

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

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

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

Si esta recuperación se realiza correctamente, el sistema StorageGRID sustituye a la copia del objeto que falta. De lo contrario, la alerta **objetos perdidos** se activa de la siguiente manera:

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

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

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

Investigar los objetos perdidos

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

Antes de empezar

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

Acerca de esta tarea

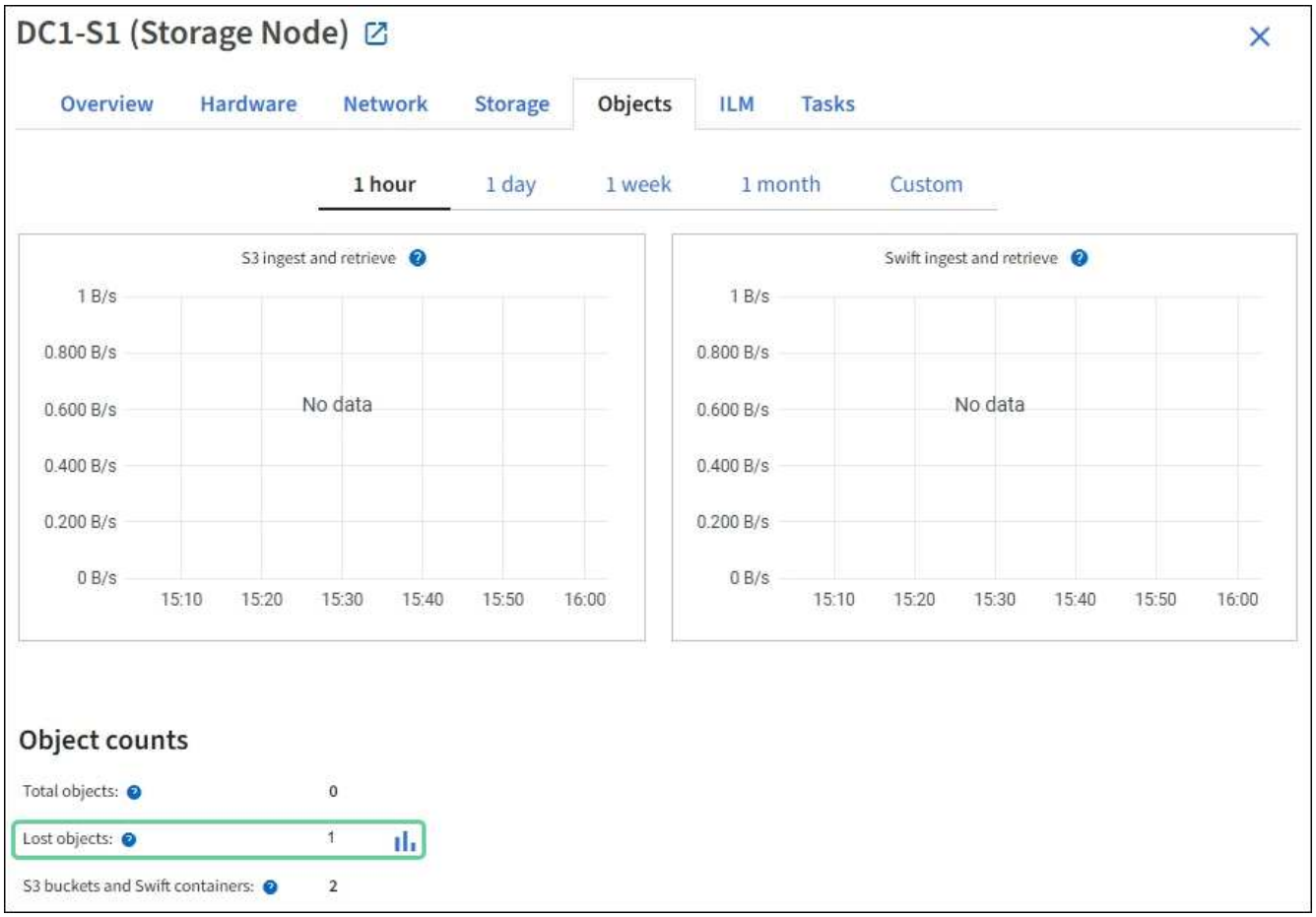
La alerta * objetos perdidos* indica que StorageGRID cree que no hay copias de un objeto en la cuadrícula. Es posible que los datos se hayan perdido de forma permanente.

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

Pasos

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

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



4. Desde un nodo de administración, "acceda al registro de auditoría" Para determinar el identificador único (UUID) del objeto que activó la alerta **Objetos perdidos**:
   a. Inicie sesión en el nodo de grid:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.
   b. Cambie al directorio donde se encuentran los registros de auditoría. Introduzca: `cd /var/local/log/`
   c. Utilice grep para extraer los mensajes de auditoría de objetos perdidos (OLST). Introduzca: `grep OLST audit_file_name`
   d. Observe el valor de UUID incluido en el mensaje.

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

5. Utilice la `ObjectByUUID` Comando para encontrar el objeto mediante su identificador (UUID) y, a continuación, determinar si los datos están en riesgo.

   a. Telnet a localhost 1402 para acceder a la consola LDR.

   b. Introduzca: `/proc/OBRP/ObjectByUUID UUID_value`

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

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

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

```
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```

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

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

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

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

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

Busque y restaure objetos que se han perdido potencialmente

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

Antes de empezar

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

Acerca de esta tarea

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

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

Pasos

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

   a. Inicie sesión en el nodo de grid:

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

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

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

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

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

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

      Por ejemplo:

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

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

      Por ejemplo:

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

      Un mensaje de auditoría LLST tiene el aspecto de este mensaje de ejemplo.

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

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

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

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

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

Node > **LDR**.

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

2. Determine si el objeto existe en el nodo de almacenamiento que se indica en el mensaje de auditoría:
   a. Inicie sesión en el nodo de grid:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

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

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

      Por ejemplo, introduzca:

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

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

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

3. Si se encontró la ruta del objeto, intente restaurar el objeto a StorageGRID:
   a. Desde el mismo nodo de almacenamiento, cambie la propiedad del archivo de objetos para que StorageGRID lo pueda gestionar. Introduzca: `chown ldr-user:bycast 'file_path_of_object'`
   b. Telnet a localhost 1402 para acceder a la consola LDR. Introduzca: `telnet 0 1402`
   c. Introduzca: `cd /proc/STOR`
   d. Introduzca: `Object_Found 'file_path_of_object'`

      Por ejemplo, introduzca:

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

      Emitir el `Object\_Found` command notifica a la cuadrícula la ubicación del objeto. También activa las políticas de ILM activas, que realizan copias adicionales según se especifica en cada política.

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

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

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

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

Continúe con el próximo paso.

4. Si el objeto se restauró correctamente en StorageGRID, compruebe que se crearon nuevas ubicaciones.
   a. Introduzca: `cd /proc/OBRP`
   b. Introduzca: `ObjectByUUID UUID_value`

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

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

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
```

```
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```

a. Cierre la sesión en la consola LDR. Introduzca: `exit`

5. En un nodo de administración, busque en los registros de auditoría del mensaje de auditoría ORLM de este objeto para confirmar que la gestión del ciclo de vida de la información (ILM) ha colocado las copias según sea necesario.

   a. Inicie sesión en el nodo de grid:

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

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

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

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

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

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

Por ejemplo:

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

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

Por ejemplo:

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

Un mensaje de auditoría ORLM tiene el aspecto de este mensaje de ejemplo.

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

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

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

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

Restablecer el número de objetos perdidos y faltantes

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

Antes de empezar

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

Acerca de esta tarea

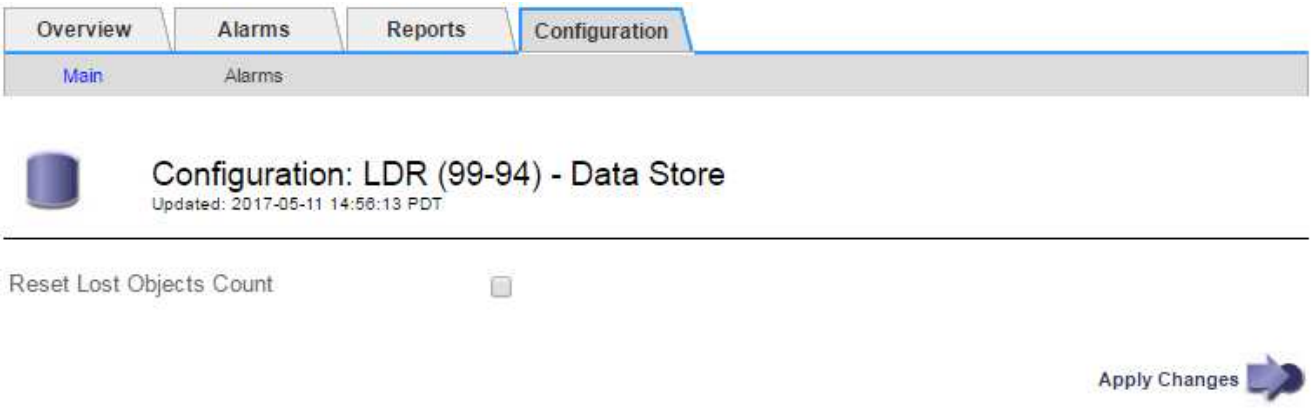
Puede restablecer el contador objetos perdidos desde cualquiera de las siguientes páginas:

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

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

Pasos

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



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

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

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

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

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

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

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

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

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

Antes de empezar

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

Acerca de esta tarea

La alerta **Low object data storage** se activa cuando la cantidad total de datos de objetos replicados y borrados en un nodo de almacenamiento cumple con una de las condiciones configuradas en la regla de alerta.

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

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

En esta condición:

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

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

Pasos

1. Seleccione **ALERTS** > **Current**.

   Aparece la página Alertas.

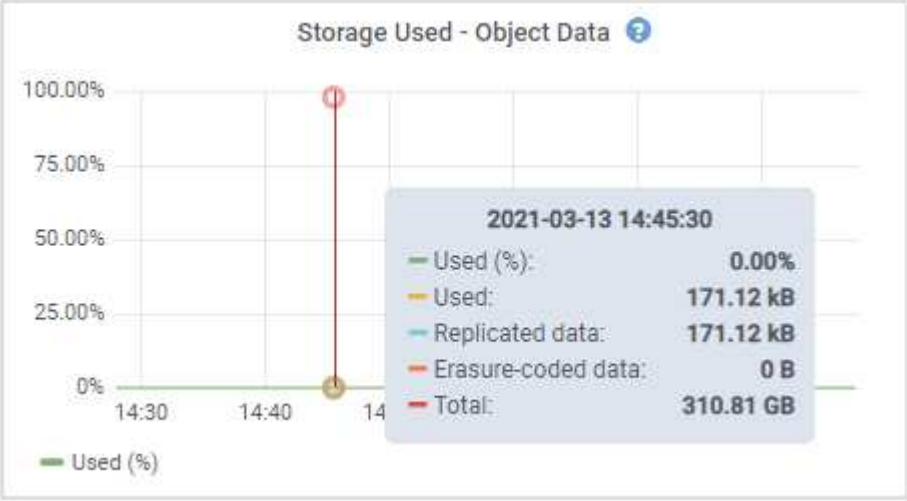
2. En la tabla de alertas, expanda el grupo de alertas **almacenamiento de datos de objeto bajo**, si es necesario, y seleccione la alerta que desea ver.

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

3. Revise los detalles en el cuadro de diálogo y tenga en cuenta lo siguiente:
   - Tiempo activado
   - El nombre del sitio y del nodo
   - Los valores actuales de las métricas de esta alerta
4. Seleccione **NODES** > ***Storage Node o Site*** > **Storage**.
5. Coloque el cursor sobre el gráfico Almacenamiento Utilizado - Datos de Objeto.

   Se muestran los siguientes valores:

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



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

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

7. Lo antes posible, "añadir capacidad de almacenamiento" en la cuadrícula.

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

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

Información relacionada

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

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

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

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

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

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

Comprenda la alerta

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

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

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

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

La alerta **Baja de sólo lectura de anulación de Marca de agua** se activa para el nodo De almacenamiento A porque su Marca de agua personalizada (5 GB) es menor que el valor mínimo optimizado para todos los

volúmenes de ese nodo (11 GB). Si continúa usando la configuración personalizada, el nodo podría ejecutarse con un nivel mínimo de espacio antes de que pueda realizar la transición de forma segura al estado de solo lectura.

Resolver la alerta

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

Antes de empezar

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

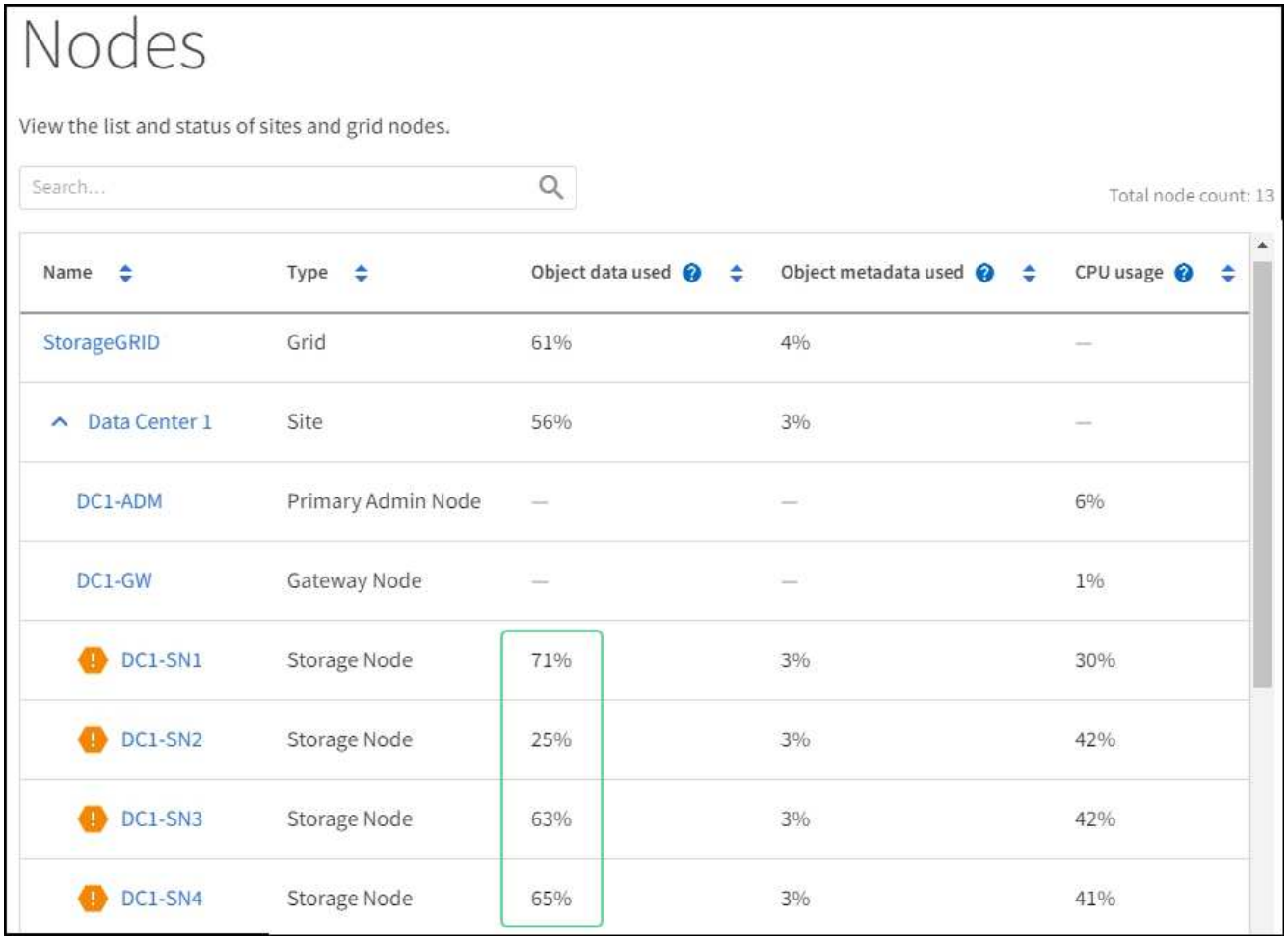
Acerca de esta tarea

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

Evalúe el uso de datos de objetos en todo el grid

Pasos

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



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

Ver marcas de agua de almacenamiento optimizadas

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

Pasos

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

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

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

todos los volúmenes de almacenamiento de cada nodo de almacenamiento. Si este valor es mayor que el valor personalizado para **Marca de agua blanda de sólo lectura de volumen de almacenamiento**, se activa la alerta **anulación de Marca de agua de sólo lectura baja** para el nodo de almacenamiento.

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

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

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

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

Determine si puede utilizar marcas de agua optimizadas

Pasos

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

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

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

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

Utilice marcas de agua optimizadas

Pasos

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

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

Solucione los problemas de la alarma de estado de almacenamiento (SST)

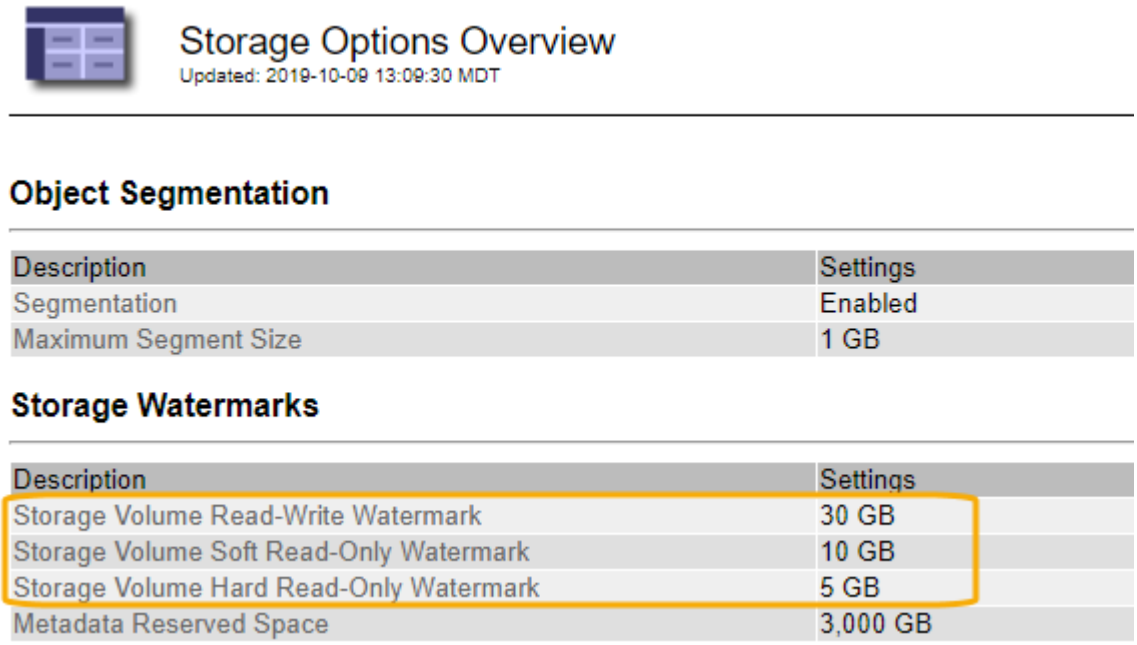
La alarma de estado del almacenamiento (SST) se activa si un nodo de almacenamiento no tiene suficiente espacio libre restante para el almacenamiento de objetos.

Antes de empezar

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

Acerca de esta tarea

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



Storage Options Overview

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

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

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

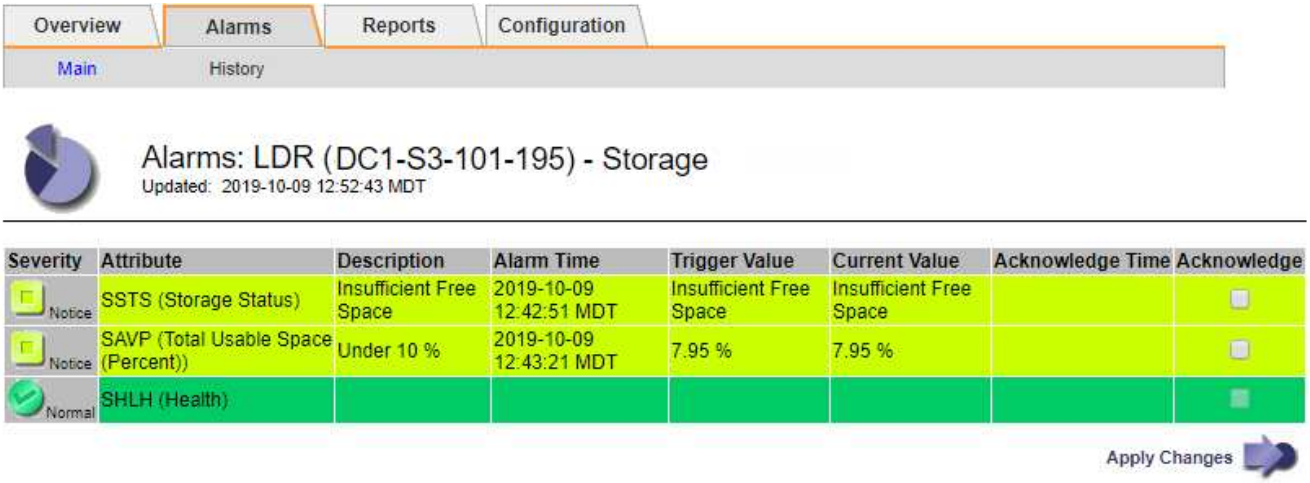
Por ejemplo, supongamos que la Marca de agua de sólo lectura suave del volumen de almacenamiento se establece en 10 GB, que es su valor predeterminado. La alarma SSTS se activa si queda menos de 10 GB de espacio utilizable en cada volumen de almacenamiento del nodo de almacenamiento. Si alguno de los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

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

Pasos

1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Current Alarms**.
2. En la columna Servicio, seleccione el centro de datos, el nodo y el servicio asociados a la alarma SSTS.

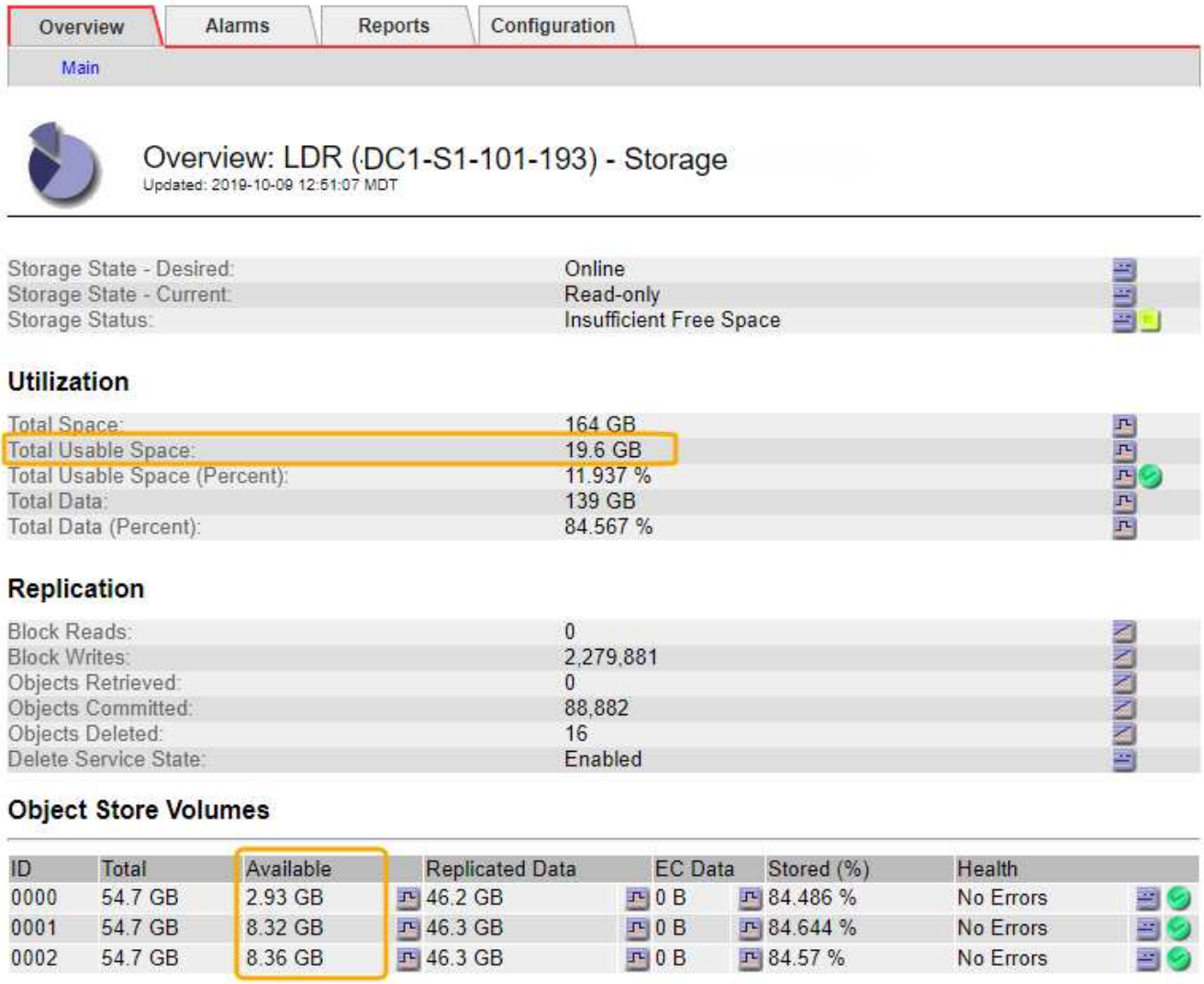
   Aparece la página Topología de cuadrícula. La ficha Alarmas muestra las alarmas activas del nodo y el servicio que ha seleccionado.



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

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

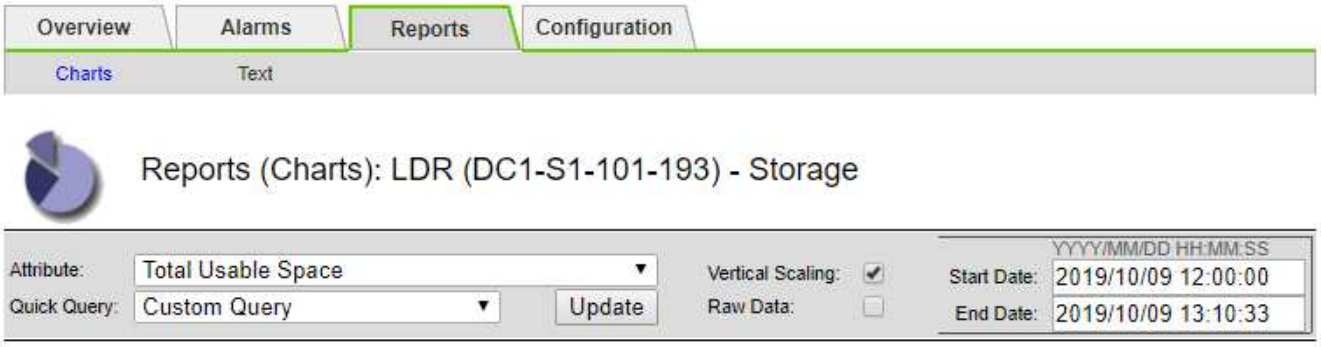
3. Para determinar cuánto espacio útil está realmente disponible, seleccione **LDR** > **almacenamiento** > **Descripción general** y busque el atributo espacio útil total (STS).

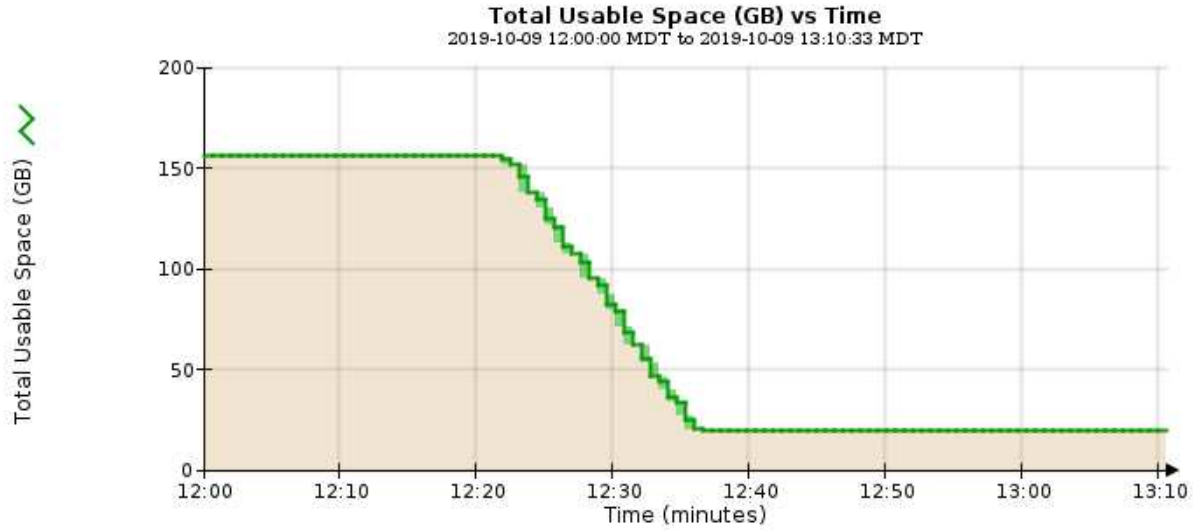


En este ejemplo, solo quedan disponibles 19.6 GB del espacio de 164 GB en este nodo de almacenamiento. Tenga en cuenta que el valor total es la suma de los valores **disponible** para los tres volúmenes de almacén de objetos. Se activó la alarma DE SSTS porque cada uno de los tres volúmenes de almacenamiento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

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

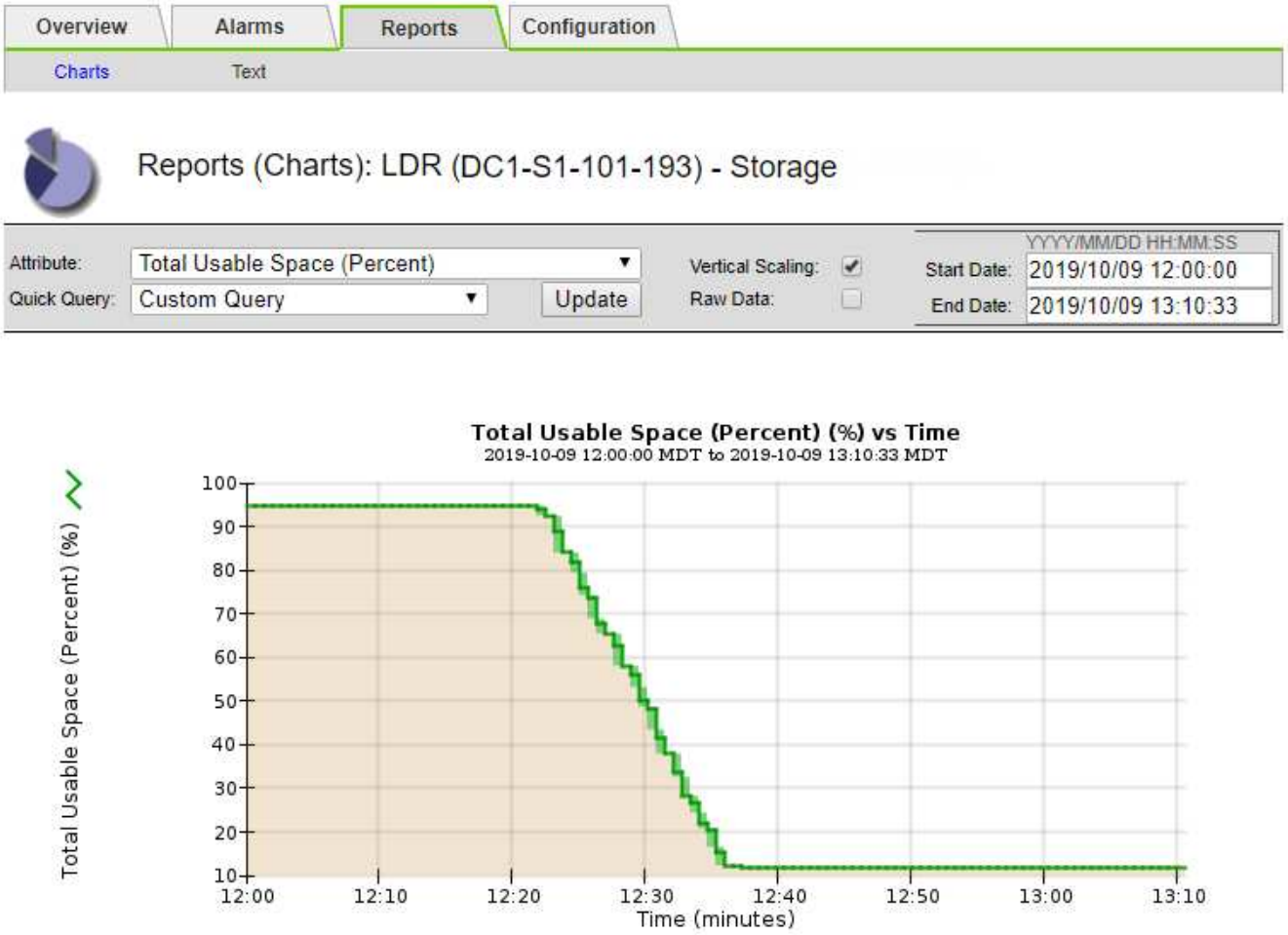
   En este ejemplo, el espacio útil total cayó de aproximadamente 155 GB a 12:00 a 20 GB a 12:35, lo que corresponde al tiempo en que se activó la alarma DE SST.





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

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



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

   Consulte también "Gestione nodos de almacenamiento completos".

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

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

Acerca de esta tarea

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

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

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

Para obtener más información, consulte "Solucione problemas de servicios de plataforma". Puede que necesite hacerlo "Acceda al inquilino del Administrador de inquilinos" para depurar un error de servicio de plataforma.

Pasos

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

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

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

Solucionar problemas de metadatos

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

Alerta de almacenamiento de metadatos baja

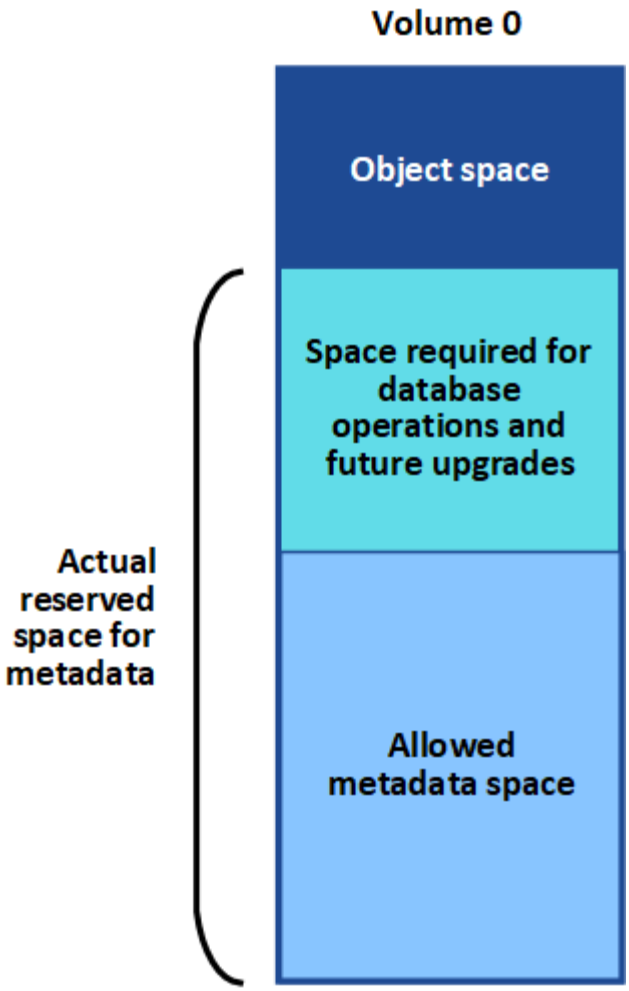
Si se activa la alerta **almacenamiento de metadatos bajo**, debe agregar nuevos nodos de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".

Acerca de esta tarea

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



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

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

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

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

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

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

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

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

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

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

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

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

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

Pasos

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

   Dado que StorageGRID mantiene copias completas de todos los metadatos de objetos en cada sitio, la capacidad de metadatos del grid completo está limitada por la capacidad de metadatos del sitio más pequeño. Si necesita agregar capacidad de metadatos a un sitio, también debe hacerlo "expanda cualquier otro sitio" Con la misma cantidad de nodos de almacenamiento.

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

Servicios: Estado - Alarma Cassandra (SVST)

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

Antes de empezar

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

Acerca de esta tarea

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

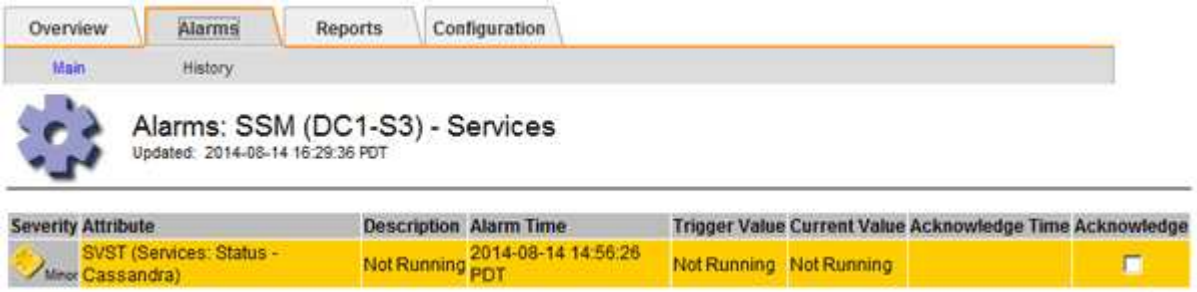
Puede hacerlo "ejecutar diagnóstico" para obtener información adicional sobre el estado actual de la cuadrícula.

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

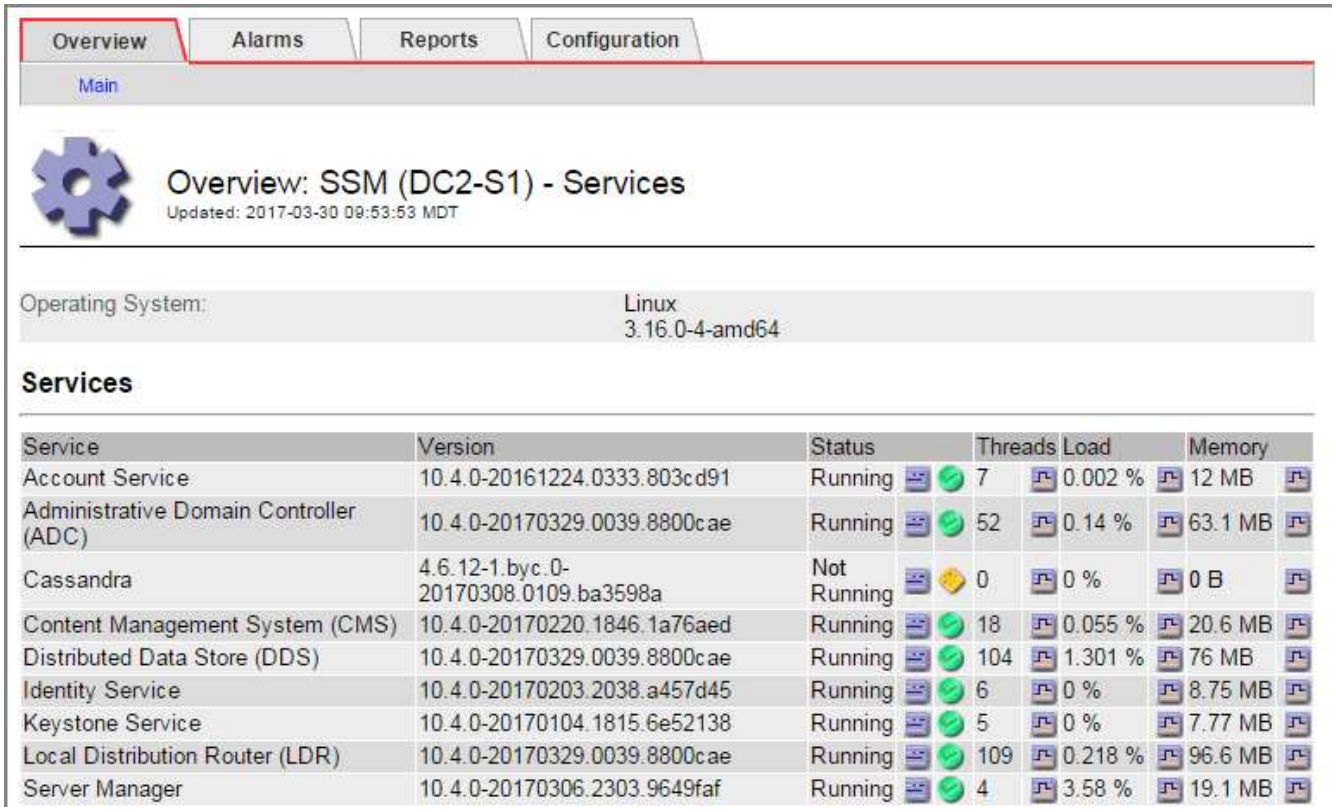
Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***Site*** > ***Storage Node*** > **SSM** > **Servicios** > **Alarmas** > **Principal** para mostrar alarmas.

   Este ejemplo muestra que se ha activado la alarma SVST.



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



3. Intente reiniciar Cassandra desde el nodo de almacenamiento:
   a. Inicie sesión en el nodo de grid:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.
   b. Introduzca: `/etc/init.d/cassandra status`
   c. Si Cassandra no se está ejecutando, reinicie: `/etc/init.d/cassandra restart`
4. Si Cassandra no se reinicia, determine cuánto tiempo ha estado inactivo Cassandra. Si Cassandra ha estado inactiva durante más de 15 días, debe reconstruir la base de datos de Cassandra.

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

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

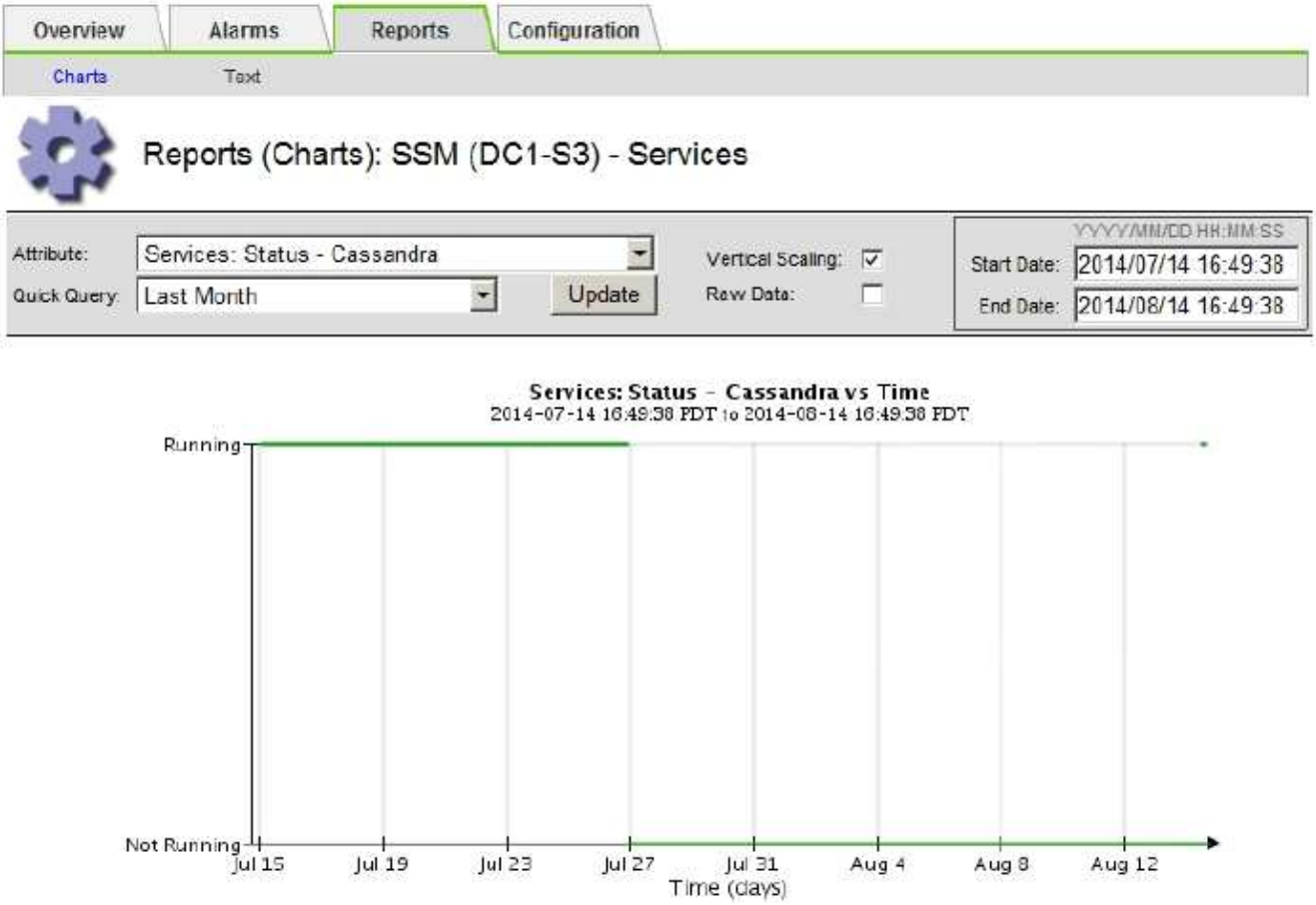
5. Para crear un gráfico en Cassandra:
   a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***Site*** > ***Storage Node*** > **SSM** > **Servicios** > **Informes** > **Cartas**.
   b. Seleccione **atributo** > **Servicio: Estado - Cassandra**.
   c. Para **Fecha de inicio**, introduzca una fecha que tenga al menos 16 días antes de la fecha actual. Para

Fecha de finalización, introduzca la fecha actual.

d. Haga clic en **Actualizar**.

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

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



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

a. Inicie sesión en el nodo de grid:

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

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

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

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

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

Se muestra el contenido del archivo servermanager.log.

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

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

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

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

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

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

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

Errores de memoria agotada de Cassandra (alarma SMTT)

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

Acerca de esta tarea

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

Pasos

1. Para ver el evento, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula** > **Configuración**.
2. Compruebe que el número de errores de memoria de salida de Cassandra sea 1 o superior.

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

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

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

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

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

Solucionar errores de certificado

Si ve un problema de seguridad o un certificado cuando intenta conectarse a StorageGRID mediante un explorador web, un cliente S3 o Swift o una herramienta de

supervisión externa, debe comprobar el certificado.

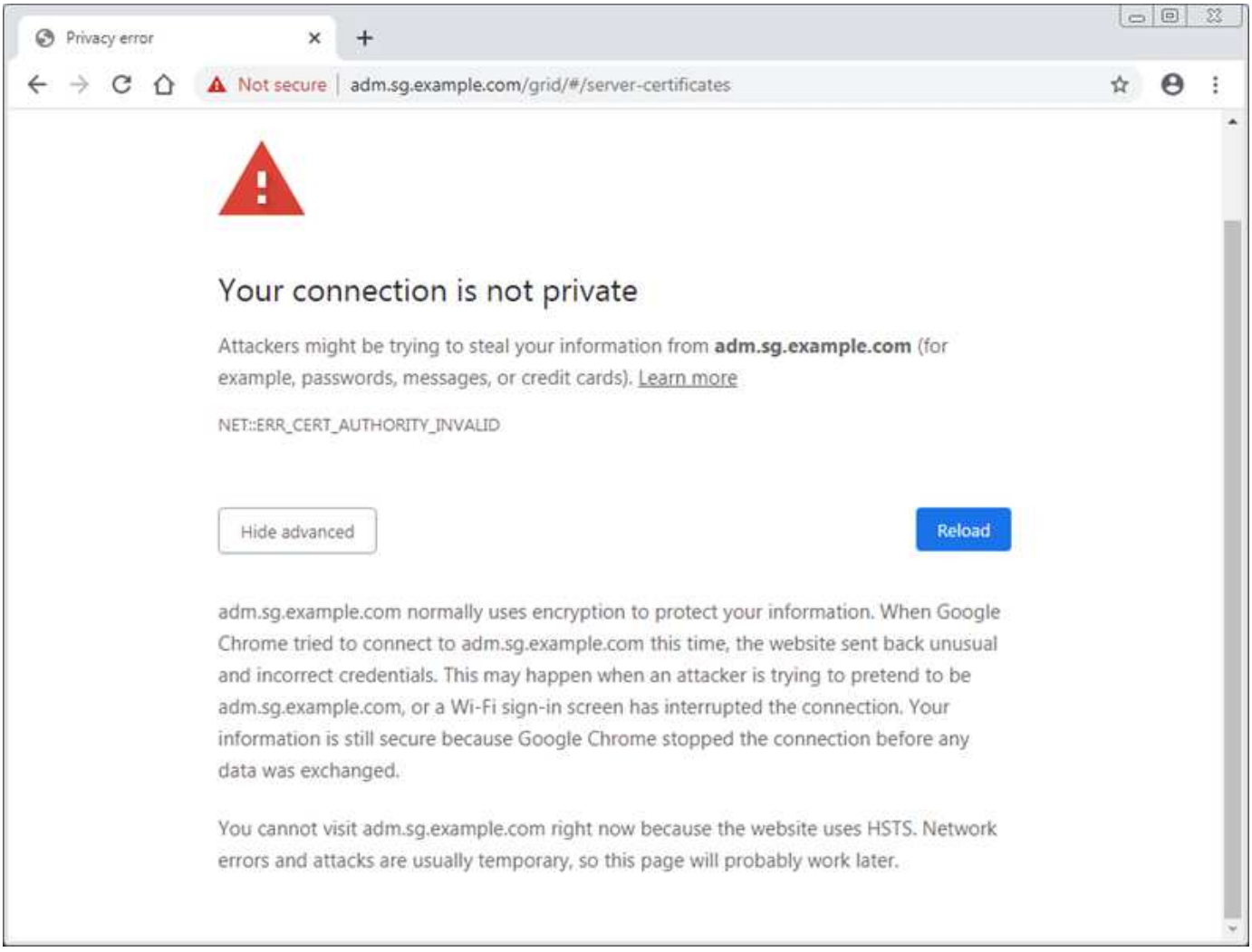
Acerca de esta tarea

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

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

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

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



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

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

Pasos

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

1. Compruebe el período de validez del certificado.
   Algunos navegadores web y clientes S3 o Swift no aceptan certificados con un período de validez superior a 398 días.
2. Si el certificado ha caducado o lo hará pronto, cargue o genere uno nuevo.
   - Para un certificado de servidor, consulte los pasos de "Configuración de un certificado de servidor personalizado para el administrador de grid y el administrador de inquilinos".
   - Para obtener un certificado de cliente, consulte los pasos de "configurar un certificado de cliente".
3. En el caso de errores de certificado de servidor, intente con una de las siguientes opciones o ambas:
   - Asegúrese de que se rellena el asunto Nombre alternativo (SAN) del certificado y que LA SAN coincida con la dirección IP o el nombre de host del nodo al que se conecta.
   - Si está intentando conectarse a StorageGRID con un nombre de dominio:
     i. Introduzca la dirección IP del nodo de administración en lugar del nombre de dominio para omitir el error de conexión y acceder a Grid Manager.
     ii. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, "seleccione la ficha de certificado adecuada" para instalar un nuevo certificado personalizado o continuar con el certificado predeterminado.
     iii. En las instrucciones para administrar StorageGRID, consulte los pasos para "Configuración de un certificado de servidor personalizado para el administrador de grid y el administrador de inquilinos".

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

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

Errores de inicio de sesión

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

Antes de empezar

- Usted tiene la `Passwords.txt` archivo.
- Ya tienes "permisos de acceso específicos".

Acerca de esta tarea

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

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

Pasos

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

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

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

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

   > Si SSO está activado, no puede iniciar sesión con un puerto restringido. Se debe usar el puerto 443.

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

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

   - Si el usuario local puede iniciar sesión:
     i. Revise las alarmas mostradas.
     ii. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **federación de identidades**.
     iii. Haga clic en **probar conexión** para validar la configuración de conexión para el servidor LDAP.
     iv. Si la prueba falla, resuelva cualquier error de configuración.
   - Si el usuario local no puede iniciar sesión y está seguro de que las credenciales son correctas, vaya al siguiente paso.
6. Utilice Secure Shell (ssh) para iniciar sesión en el nodo de administración:
   a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

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

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

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

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

8. Confirme que el servicio nginx-gw se está ejecutando `# service nginx-gw status`
9. use Lumberjack para recopilar registros: `# /usr/local/sbin/lumberjack.rb`

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

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

10. Revise los siguientes registros:
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`
    - `**/*commands.txt`
11. Si no pudo identificar ningún problema con el nodo de administración, ejecute cualquiera de los siguientes comandos para determinar las direcciones IP de los tres nodos de almacenamiento que ejecutan el servicio ADC en el sitio. Normalmente, estos son los primeros tres nodos de almacenamiento que se instalaron en el sitio.

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

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

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

12. Desde el nodo de administración, inicie sesión en cada uno de los nodos de almacenamiento de ADC usando las direcciones IP identificadas.
    a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
    b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
    c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
    d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

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

    Asegúrese de que los servicios idnt, acct, nginx y cassandra están en ejecución.

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

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

Problemas de la interfaz de usuario

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

Pasos

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

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

2. Borre la caché del navegador web.

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

Nodo de administración no disponible

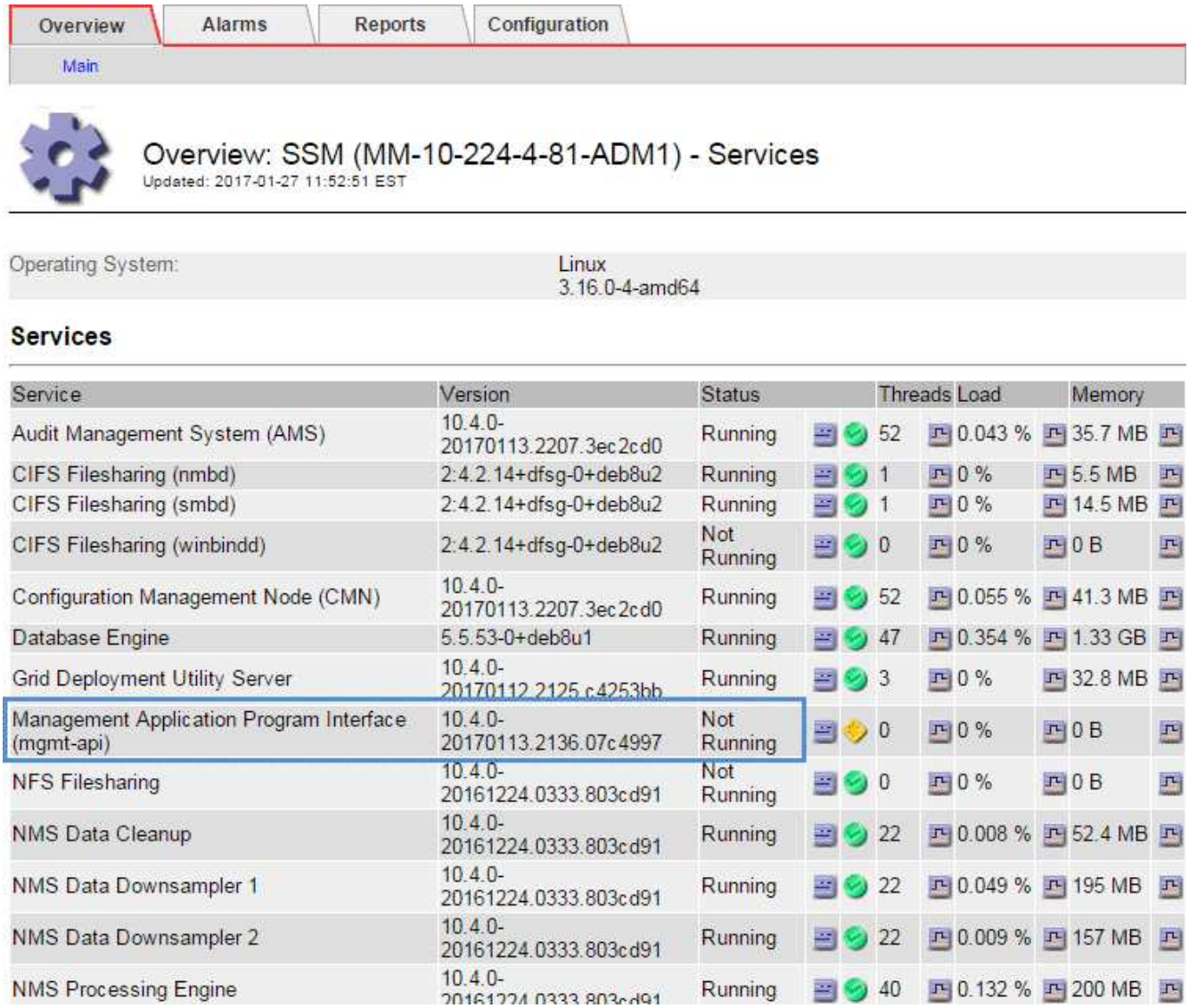
Si el sistema StorageGRID incluye varios nodos de administrador, puede usar otro nodo de administración para comprobar el estado de un nodo de administración no disponible.

Antes de empezar

Ya tienes "permisos de acceso específicos".

Pasos

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



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

Solucionar problemas de red, hardware y plataforma

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

Errores de «422: Entidad no procesable»

El error 422: Entidad no procesable puede ocurrir por diferentes razones. Compruebe el mensaje de error para determinar la causa del problema.

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

Mensaje de error	Causa raíz y acción correctiva

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

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	Este mensaje aparece si intenta utilizar un cifrado no compatible para establecer una conexión TLS (Seguridad de la capa de transporte) desde StorageGRID a un sistema externo utilizado para identificar los grupos de almacenamiento de la federación o de la nube.
	
	Compruebe los códigos que ofrece el sistema externo. El sistema debe utilizar uno de los "Cifrados compatibles con StorageGRID" Para conexiones TLS salientes, como se muestra en las instrucciones para administrar StorageGRID.

Alerta de discrepancia de MTU de red de cuadrícula

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

Acerca de esta tarea

Las diferencias en la configuración de MTU podrían indicar que algunas redes eth0, pero no todas, están configuradas para tramas gigantes. Un error de coincidencia del tamaño de MTU de más de 1000 puede provocar problemas de rendimiento de la red.

Pasos

1. Enumere la configuración de MTU para eth0 en todos los nodos.
   - Utilice la consulta proporcionada en Grid Manager.
   - Vaya a. *primary Admin Node IP address*`/metrics/graph` e introduzca la siguiente consulta: `node_network_mtu_bytes{device="eth0"}`
2. "Modifique la configuración de MTU" Según sea necesario para garantizar que son iguales para la interfaz de red de grid (eth0) en todos los nodos.
   - Para los nodos basados en Linux y VMware, use el siguiente comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

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

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

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

Argumentos posicionales	Descripción
`mtu`	La MTU que se va a establecer. Debe estar entre 1280 y 9216.
`network`	Las redes a las que se va a aplicar la MTU. Incluya uno o varios de los siguientes tipos de red: • cuadrícula • admin • cliente

+

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

Alarma de error de recepción de red (NRER)

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

Acerca de esta tarea

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

StorageGRID:

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

Pasos

1. Siga los pasos de solución de problemas para todas las posibles causas de la alarma NRER dada la configuración de la red.
2. Realice los siguientes pasos en función de la causa del error:

FEC no coincide

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

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

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

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

Discrepancia entre el puerto del switch y la MTU de NIC

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

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

Para obtener el mejor rendimiento de red, todos los nodos deben configurarse con valores MTU similares en sus interfaces de Grid Network. La alerta **Red de cuadrícula MTU** se activa si hay una diferencia significativa en la configuración de MTU para la Red de cuadrícula en nodos individuales. No es necesario que los valores de MTU sean los mismos para todos los tipos de red. Consulte Solucione problemas de la alerta de discrepancia de MTU de red de cuadrícula si quiere más información.

Consulte también "Cambie la configuración de MTU".

Índices altos de errores de enlace

a. Active FEC, si aún no está activado.

b. Compruebe que el cableado de red es de buena calidad y que no está dañado o conectado incorrectamente.

c. Si parece que los cables no son el problema, póngase en contacto con el soporte técnico.

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

Desbordamiento del búfer de anillo NIC

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

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

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

Información relacionada

"Referencia de alarmas (sistema heredado)"

Errores de sincronización de hora

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

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

> Cuando "Especificación del origen NTP externo" Para una instalación de StorageGRID en el nivel de producción, no use el servicio Windows Time (W32Time) en una versión de Windows anterior a Windows Server 2016. El servicio de tiempo en versiones anteriores de Windows no es lo suficientemente preciso y no es compatible con Microsoft para su uso en entornos de gran precisión como StorageGRID.

Linux: Problemas de conectividad de red

Puede ver problemas con la conectividad de red de los nodos de StorageGRID alojados en hosts Linux.

Clonación de direcciones MAC

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

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

Para obtener más información sobre la activación de la clonación MAC, consulte las instrucciones de "Red Hat Enterprise Linux" o. "Ubuntu o Debian".

Modo promiscuo

Si no desea utilizar la clonación de direcciones MAC y prefiere permitir que todas las interfaces reciban y transmitan datos para direcciones MAC distintas de las asignadas por el hipervisor, Asegúrese de que las propiedades de seguridad en los niveles de conmutador virtual y grupo de puertos estén establecidas en **Aceptar** para el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas. Los valores establecidos en el conmutador virtual pueden ser anulados por los valores en el nivel de grupo de puertos, por lo que asegúrese de que la configuración sea la misma en ambos lugares.

Para obtener más información sobre el uso del modo Promiscuous, consulte las instrucciones de "Red Hat Enterprise Linux" o. "Ubuntu o Debian".

Linux: El estado del nodo es «huérfano»

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

Acerca de esta tarea

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

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

Pasos

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

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

   Si el nodo está huérfano, la respuesta es

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

4. Desde Linux, detenga el motor de contenedor y todos los procesos que controlan el nodo storagegrid. Por ejemplo:`sudo docker stop --time secondscontainer-name`

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

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

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

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

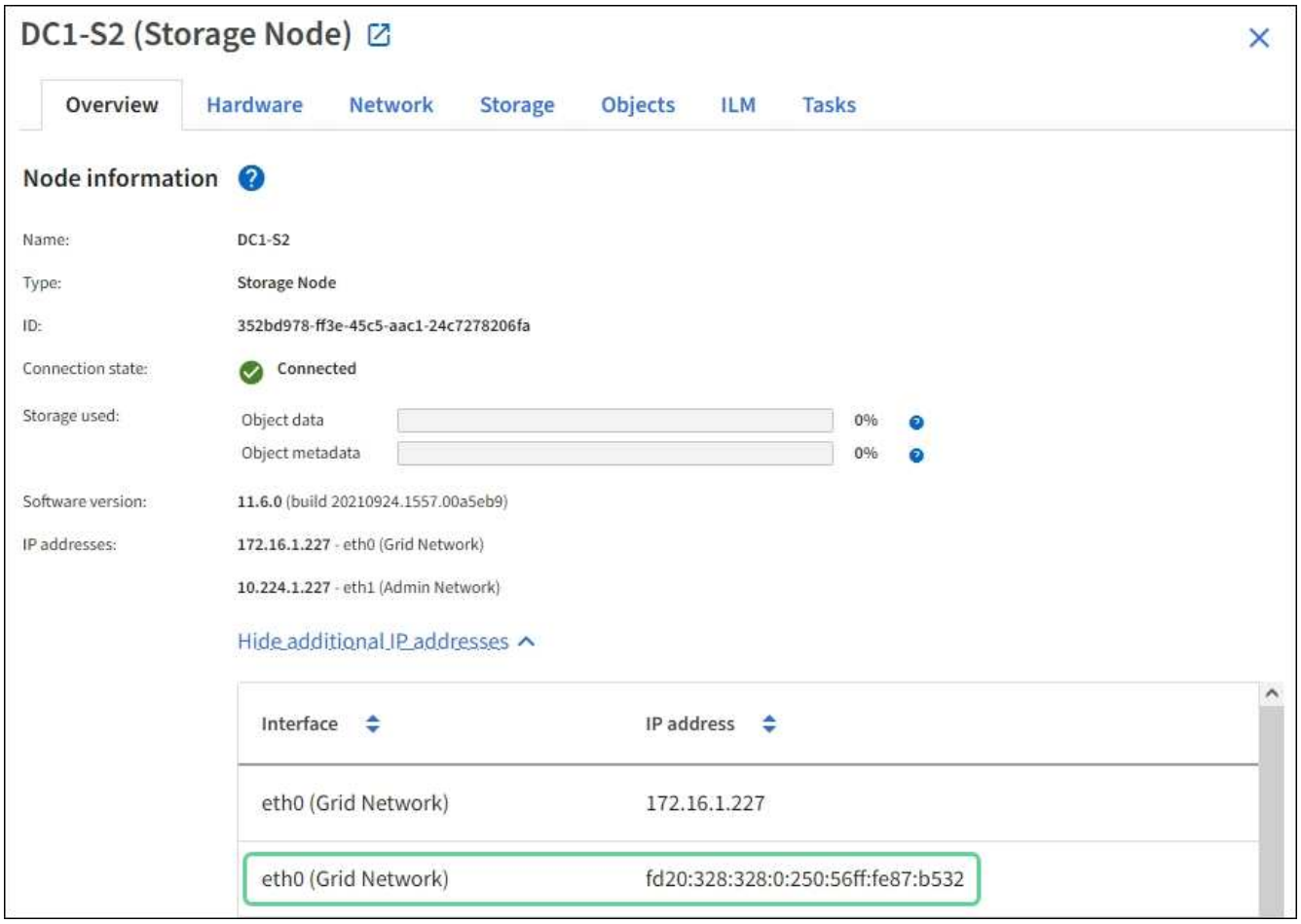
Linux: Solucione problemas de compatibilidad con IPv6

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

Acerca de esta tarea

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

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



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

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

Pasos

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

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

El resultado debe ser 0.

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

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

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

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

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

El resultado debería ser 1.

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

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

5. Salga del contenedor: `exit`

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

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

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

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

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

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

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

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

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

Solucione problemas de un servidor de syslog externo

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

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

consulte:

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

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

Mensaje de error	Descripción y acciones recomendadas
Tiempo de espera de conexión agotado	Se ha realizado un intento de conexión TCP/TLS, pero no se ha recibido respuesta del servidor de syslog durante mucho tiempo. Es posible que haya una configuración incorrecta de enrutamiento o que un firewall esté borrando el tráfico sin enviar ninguna respuesta (una configuración común). 1. Compruebe que haya introducido el FQDN o la dirección IP correctos para el servidor de syslog. 2. Para cada nodo de la lista, compruebe la lista de subredes de redes de cuadrícula, las listas de subredes de redes de administración y las puertas de enlace de red de cliente. Confirme que están configurados para enrutar el tráfico hacia el servidor de syslog mediante la interfaz de red y la puerta de enlace (Grid, Admin o Client) mediante las que espera acceder al servidor de syslog. 3. Confirme que un firewall no bloquea el acceso a las conexiones TCP/TLS desde los nodos indicados a la IP y al puerto del servidor de syslog.
Conexión cerrada por el partner	Se estableció correctamente una conexión TCP con el servidor de syslog, pero se cerró posteriormente. Algunos motivos pueden ser: • Es posible que se haya reiniciado o reiniciado el servidor de syslog. • Es posible que el nodo y el servidor de syslog tengan diferentes ajustes de TCP/TLS. • Un firewall intermedio podría estar cerrando conexiones TCP inactivas. • Es posible que un servidor que no esté escuchando en el puerto del servidor de syslog haya cerrado la conexión. Para resolver este problema: 1. Compruebe que haya introducido el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor de syslog. 2. Si utiliza TLS, confirme que el servidor de syslog también está usando TLS. Si utiliza TCP, confirme que el servidor de syslog también utiliza TCP. 3. Compruebe que un firewall intermedio no está configurado para cerrar las conexiones TCP inactivas.
Error del certificado de TLS	El certificado de servidor recibido del servidor de syslog no era compatible con el paquete de certificado de CA y el certificado de cliente proporcionados. 1. Confirme que el paquete de certificado de CA y el certificado de cliente (si los hubiera) son compatibles con el certificado de servidor en el servidor de syslog. 2. Confirme que las identidades en el certificado de servidor del servidor de syslog incluyen los valores esperados de IP o FQDN.

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

Revisar los registros de auditoría

Revisar registros de auditoría: Información general

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 la configuración de niveles de mensajes de auditoría y el uso de un servidor de syslog externo, consulte "Configurar los mensajes de auditoría y los destinos de registro".

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 la forma en que estos mensajes de auditoría pasan por el sistema StorageGRID al `audit.log` archivo.

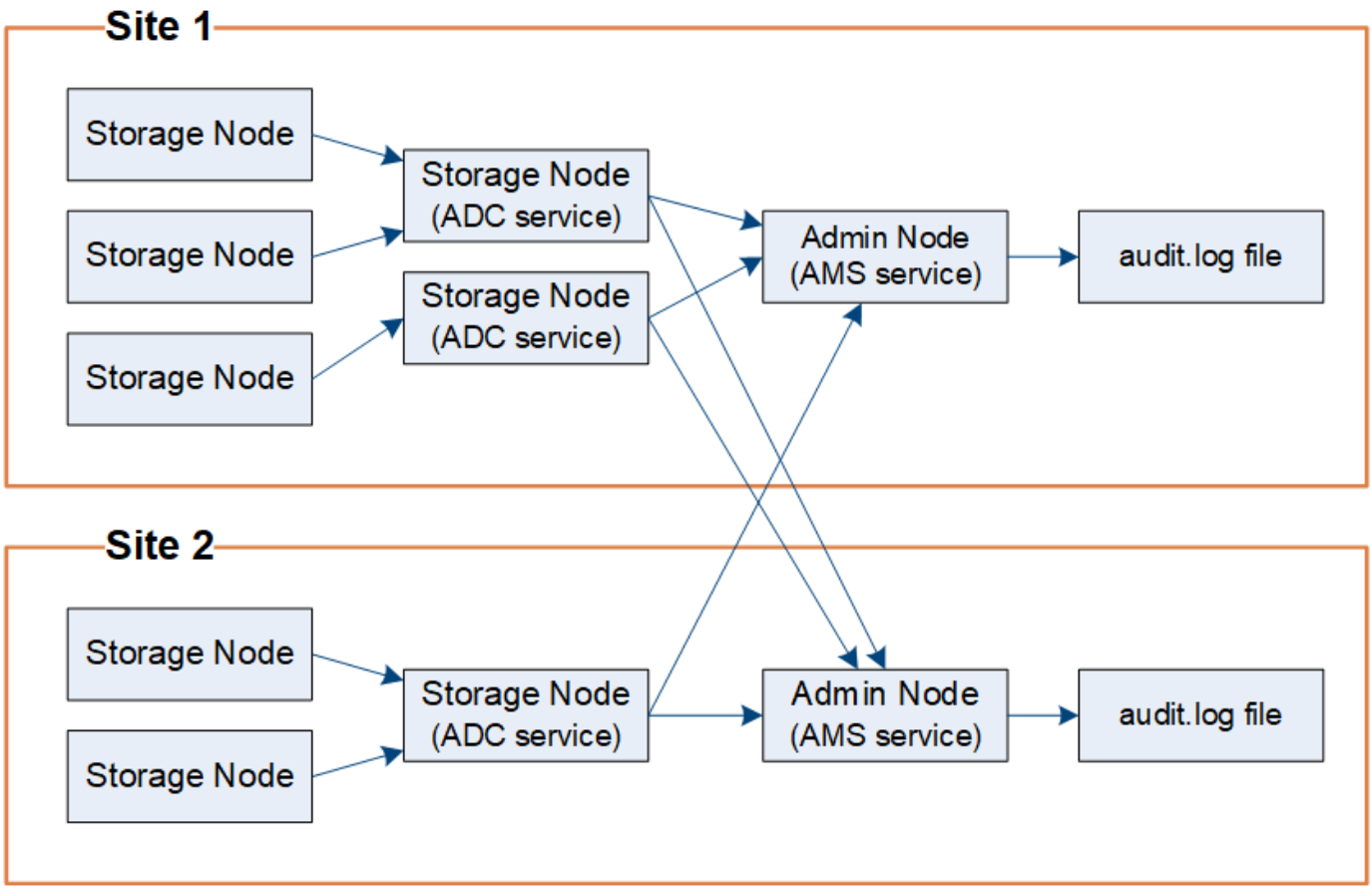
Flujo de mensajes de auditoría

Los mensajes de auditoría los procesan los nodos de administrador y los 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.

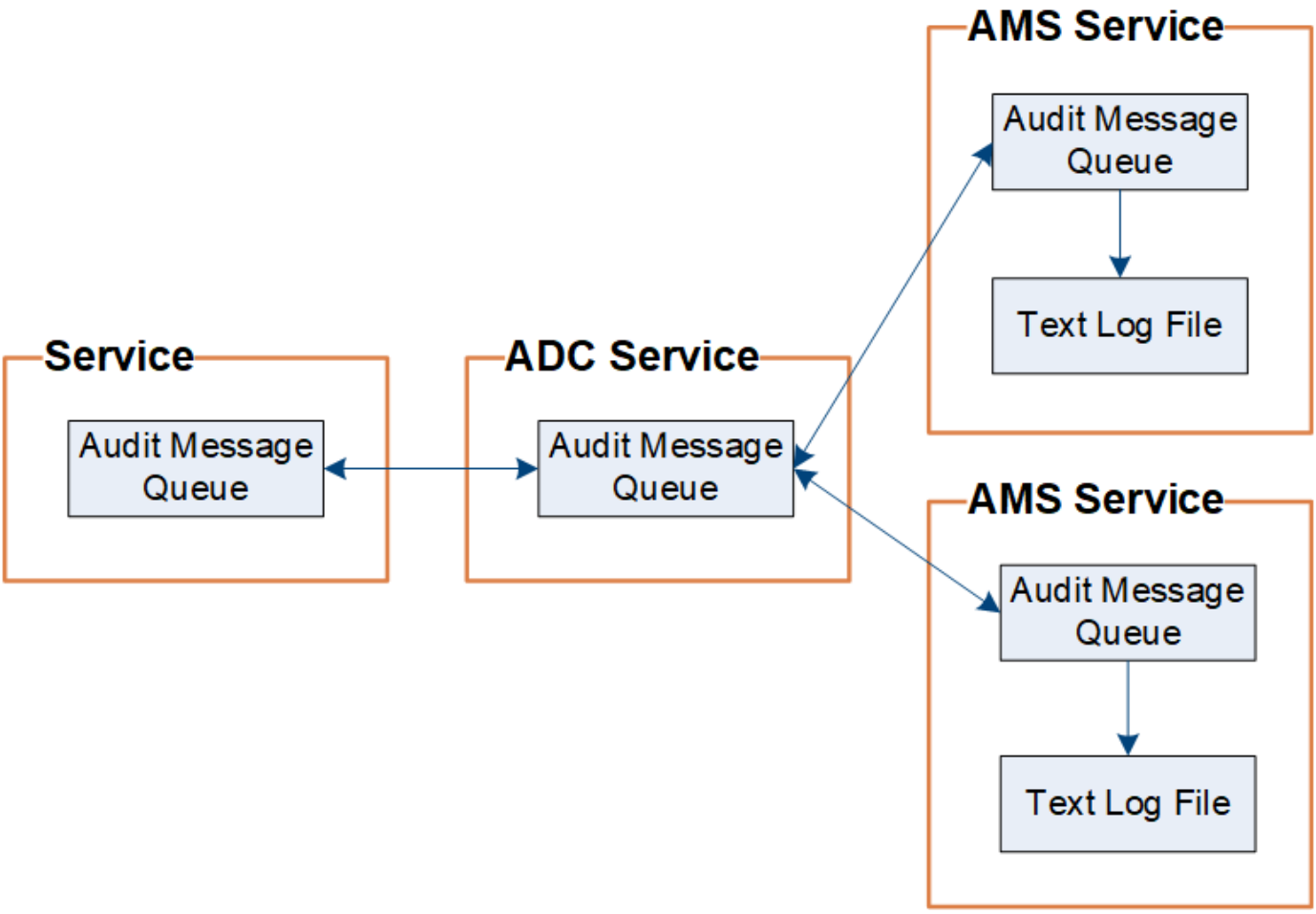
Cada nodo de administración almacena mensajes de auditoría en archivos de registro de texto; se asigna el nombre al archivo de registro activo `audit.log`.



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 transmite un mensaje de auditoría, el mensaje se almacena en una cola de mensajes de auditoría en el disco del sistema del nodo de cuadrícula. Siempre se mantiene una copia del mensaje en la cola de mensajes de auditoría hasta que el mensaje se escribe en el archivo de registro de auditoría del nodo de administración `/var/local/log` 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 está demasiado lleno, los nodos individuales priorizarán el procesamiento de su acumulación y no estarán disponibles temporalmente para los mensajes nuevos.

Específicamente, puede ver los siguientes comportamientos:

- Si la `/var/local/log` el directorio utilizado por un nodo de administración se llena, el nodo de administración se marcará como no disponible para los nuevos mensajes de auditoría hasta que el directorio ya no esté lleno. Las solicitudes de clientes S3 y Swift no se ven afectadas. La alarma XAMS (repositorios de auditoría no accesibles) se activa cuando no se puede acceder a un repositorio de auditoría.
- Si la `/var/local/` el directorio utilizado por un nodo de almacenamiento con el servicio ADC se llena al 92%, el nodo se marcará como no disponible para auditar mensajes hasta que el directorio sólo esté lleno al 87%. Las solicitudes de clientes de S3 y Swift a otros nodos no se ven afectadas. La alarma NRLY (Relés de auditoría disponibles) se activa cuando no se pueden acceder a los relés de auditoría.

Si no hay nodos de almacenamiento disponibles con el servicio ADC, los nodos de almacenamiento almacenan los mensajes de auditoría localmente en la `/var/local/log/localaudit.log` archivo.

- Si la `/var/local/` El directorio que utiliza un nodo de almacenamiento se llena al 85%, el nodo empezará a rechazar las solicitudes de cliente S3 y Swift `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.
- La `/var/local/` El espacio de un nodo de almacenamiento ADC se llena por motivos que no están relacionados 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 su gravedad, vea un gráfico del tamaño de la cola. Si el número aumenta constantemente durante horas o días, es probable que la carga de auditoría haya superado la capacidad de auditoría del sistema. Reduzca la tasa de operaciones del cliente o disminuya el número de mensajes de auditoría registrados cambiando el nivel de auditoría de las escrituras del cliente y las lecturas del cliente a error o Desactivado. Consulte "Configurar los mensajes de auditoría y los destinos de registro".

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 activo `audit.log` archivo y todos 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.

Antes de empezar

- Ya tienes "permisos de acceso específicos".
- Debe tener la `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 `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Vaya al directorio que contiene los archivos del registro de auditoría:

```
cd /var/local/log
```

3. Ver el archivo de registro de auditoría actual o guardado, según sea necesario.

Rotación del archivo de registro de auditoría

Los archivos de registros de auditoría se guardan en un nodo administrador `/var/local/log` directorio. Se denomina los archivos de registro de auditoría activos `audit.log`.

> 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. Consulte "Configurar los mensajes de auditoría y los destinos de registro".

Una vez al día, el activo `audit.log` el archivo se guardará y se guardará un nuevo `audit.log` se ha iniciado el 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 utilizan la fecha en la que se guardó el archivo, añadido por un número, en 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 cambia su nombre, en el formato *`yyyy-mm-dd.txt.gz`*, que conserva la fecha original. Con el tiempo, esto genera el consumo de almacenamiento asignado a los registros de auditoría en el nodo de administración. Una secuencia de comandos supervisa el consumo de espacio del registro de auditoría y elimina los archivos de registro según sea necesario para liberar espacio en la `/var/local/log` directorio. Los registros de auditoría se eliminan según la fecha en la que se crearon, y la más antigua se eliminó primero. Puede supervisar las acciones del script en el siguiente archivo: `/var/local/log/manage-audit.log`.

En este ejemplo se muestra el activo `audit.log` archivo, 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 de archivo de registro de auditoría: Información general

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* son microsegundos.

- El mensaje de auditoría mismo, 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):SUCS][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):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][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):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][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):SPUT][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 el "herramienta audit-explain" para obtener resúmenes simplificados de los mensajes de auditoría en el log de auditoría. Puede utilizar el "herramienta audit-sum" para resumir cuántas operaciones de escritura, lectura y eliminación se han registrado y cuánto tiempo demoraron estas operaciones.

Utilice la herramienta de explicación de auditoría

Puede utilizar el `audit-explain` herramienta para traducir los mensajes de auditoría

del registro de auditoría a un formato de fácil lectura.

Antes de empezar

- Ya tienes "permisos de acceso específicos".
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la dirección IP del nodo de administrador principal.

Acerca de esta tarea

La `audit-explain` La herramienta, disponible en el nodo de administración principal, proporciona resúmenes simplificados de los mensajes de auditoría en un registro de auditoría.

> La `audit-explain` la herramienta está diseñada principalmente para su uso por parte del soporte técnico durante operaciones de solución de problemas. Procesamiento `audit-explain` Las consultas pueden consumir una gran cantidad de energía de CPU, lo que puede afectar a las operaciones de StorageGRID.

Este ejemplo muestra el resultado típico de `audit-explain` herramienta. Estos cuatro "SPUT" Los mensajes de auditoría se generaron cuando el inquilino de S3 con ID de cuenta 92484777680322627870 utilizó solicitudes PUT S3 para crear un bloque llamado «bucket1» y añadir tres objetos a ese bloque.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

La `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/log/*
  ```

- 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 partes, en lugar del archivo completo.

> La `audit-explain` la herramienta no acepta archivos comprimidos como entrada con hilo. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comandos o utilice `zcat` herramienta para descomprimir primero los archivos. 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:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Introduzca el comando siguiente, donde `/var/local/log/audit.log` representa el nombre y la ubicación del archivo o archivos que desea analizar:

   ```
   $ audit-explain /var/local/log/audit.log
   ```

   La `audit-explain` la herramienta imprime interpretaciones legibles por el usuario de todos los mensajes en el archivo o los 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, use la Marca de hora (`-t`) opción.

Utilice la herramienta de suma de auditoría

Puede utilizar el `audit-sum` herramienta para contar los mensajes de auditoría de escritura, lectura, cabecera y eliminación y para ver el tiempo mínimo, máximo y promedio (o tamaño) para cada tipo de operación.

Antes de empezar

- Ya tienes "permisos de acceso específicos".
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la dirección IP del nodo de administrador principal.

Acerca de esta tarea

La `audit-sum` Herramienta, disponible en el nodo de administración principal, resume cuántas operaciones de escritura, lectura y eliminación se han registrado y cuánto tiempo han tardado estas operaciones.

> La `audit-sum` la herramienta está diseñada principalmente para su uso por parte del soporte técnico durante operaciones de solución de problemas. Procesamiento `audit-sum` Las consultas pueden consumir una gran cantidad de energía de CPU, lo que puede afectar a las operaciones de StorageGRID.

Este ejemplo muestra el resultado típico de `audit-sum` herramienta. Este ejemplo muestra el tiempo que tardaban las operaciones de protocolo.

```
  message group           count     min(sec)        max(sec)
average(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
```

La `audit-sum` La herramienta proporciona recuentos y horas para los siguientes mensajes de auditoría de S3, Swift y ILM en un registro de auditoría:

Codificación	Descripción	Consulte
ARCT	Archive recupere desde Cloud-Tier	"ARCT: Recuperación de archivos a partir de nivel de cloud"
ASCT	Almacenamiento de datos para el nivel cloud	"ASCT: Archive Store Cloud-Tier"
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"

Codificación	Descripción	Consulte
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"
¡WDEL	Swift DELETE: Registra una transacción realizada correctamente para eliminar un objeto o un contenedor.	"WDEL: ELIMINACIÓN de Swift"
CONSIGA	Swift GET: Registra una transacción realizada correctamente para recuperar un objeto o enumerar los objetos de un contenedor.	"WGET: Swift GET"
WHEA	Swift HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o contenedor.	"WHEA: CABEZA de Swift"
WPUT	Swift PUT: Registra una transacción correcta para crear un nuevo objeto o contenedor.	"WPUT: SWIFT PUT"

La `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/log/*
```

- 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 con hilo. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comandos o utilice `zcat` herramienta para descomprimir primero los archivos. 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 promedio de funcionamiento, pero puede utilizar `size (-s)` opción para mirar 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:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Si desea analizar todos los mensajes relacionados con las operaciones de escritura, lectura, cabeza y eliminación, siga estos pasos:
   a. Introduzca el comando siguiente, donde `/var/local/log/audit.log` representa el nombre y la ubicación del archivo o archivos que desea analizar:

      ```
      $ audit-sum /var/local/log/audit.log
      ```

      Este ejemplo muestra el resultado típico de `audit-sum` herramienta. Este ejemplo muestra el tiempo que tardaban las operaciones de protocolo.

```
  message group           count     min(sec)        max(sec)
average(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 Long OUTPUT (`-l`) para incluir rutas de 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/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-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 lentos tiempos de recuperación en el peor de los casos.

3. Si desea determinar qué tamaños de objetos se están ingiriendo y recuperando de la cuadrícula, utilice la opción size (`-s`):

   ```
   audit-sum -s audit.log
   ```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                   213371        0.000          10.504
1.695
  SGET                   201906        0.000        5000.000
14.920
  SHEA                    22716        0.001          10.504
2.967
  SPUT                 1771398        0.000        5000.000
2.495
```

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. Emita el comando en el registro de auditoría correspondiente y use 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           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Estos resultados muestran que S3 CONSIGUE tráfico pico entre 06:00 y 07:00. Los tiempos máximo y promedio son considerablemente más altos en estos tiempos también, y no subieron gradualmente a medida que el recuento aumentó. Esto sugiere que se ha superado la capacidad en algún lugar, quizás en la red o en la capacidad del grid para procesar solicitudes.

b. Para determinar el tamaño de los objetos recuperados ayer cada hora, agregue la opción size (`-s`) para el mando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

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 de muchas líneas, agregue `less` comando para mostrar el contenido del archivo de registro 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 utilizar el `-go` opción, que agrupa mensajes para 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 cucharones tienen las operaciones de SPUT más lentas, utilice `-gb` opción, que agrupa 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 cucharones tienen el tamaño de objeto SPUT más grande, utilice ambos `-gb` y la `-s` opciones:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Formato de mensaje de auditoría

Formato del mensaje de auditoría: Información general

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 resumida proporcionada por el "auditoría-explicar" y.. "suma de auditoría" las herramientas son insuficientes; 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 se encuentra entre paréntesis (`[ ]`), y cada elemento de atributo de la cadena tiene las siguientes características:

- 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 avance 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 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: • 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.

Siguiendo la abertura `[AUDT:` contenedor que identifica el mensaje en sí, el siguiente conjunto de atributos proporciona información acerca del evento o la acción descrita por el mensaje de auditoría. Estos atributos se resaltan en el siguiente ejemplo:

2018-12-05T08:24:45,921845 [AUDT:*\[RSLT\(FC32\):SUCS\]*
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\): «10.224.0.100»\]\[S3AI\(CSTR\): «60025621595611246499»\]
\[SACC\(CSTR\): "Cuenta"\]\[S3AK\(CSTR\):
"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJA="\]
\[SUSR\(CSTR\): "Urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\): "60025621595611246499"\]\[SBAC\(CSTR\): "CUENTA"\]\[S3BK\(CSTR\): "CUBO"\]
\[S3KY\(CSTR\): "Objeto"\]\[CBID\(UI64\):0xCC128B9B9E428347\]
\[UUID\(CSTR\): «B975D2CE-E4DA-4D14-8A23-
1CB4B83F2CD8»\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][AMID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]

La `ATYP` elemento (subrayado en el ejemplo) identifica qué evento generó el mensaje. Este mensaje de ejemplo incluye el "SHEA" Código de mensaje ([ATYP(FC32):SHEA]), que indica que fue generado por una solicitud correcta de S3 CABEZA.

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.

Codificación	Tipo	Descripción
AID	UI64	ID de seguimiento: Identificador que comparte el conjunto de mensajes activados por un solo evento.
ATIM	UI64	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. 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 `audit.log` File es el atributo ATIM en formato ISO 8601. La fecha y la hora se representan como *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, donde `T` es un carácter literal de cadena que indica el comienzo del segmento de tiempo de la fecha. *`UUUUUU`* son microsegundos.
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 la `audit.log` archivo:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][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):"s3small1"][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 ingesta 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\(CSTR\):"s3small1"][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):157922414
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):"s3small1"][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 al jueves 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 localizando mensajes de auditoría específicos de la API (S3 o Swift).

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 operaciones de Swift	WCON (contenedor), WOBJ (objeto) 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.

Nodos de archivado

La serie de mensajes de auditoría generados cuando un nodo de archivado envía datos de objeto a un sistema de almacenamiento de archivado externo es similar a la de los nodos de almacenamiento, excepto que no hay ningún mensaje SCMT (confirmación de objeto de almacén), Y los mensajes ATCE (Archive Object Store Begin) y ASCE (Archive Object Store End) se generan para cada copia archivada de datos de objeto.

La serie de mensajes de auditoría generados cuando un nodo de archivado recupera datos de objeto de un sistema de almacenamiento de archivado externo es similar a la de los nodos de almacenamiento, excepto que los mensajes ARCB (Archive Object Retrieve Begin) y ARCE (Archive Object Retrieve End) se generan para cada copia recuperada de los datos de objeto.

La serie de mensajes de auditoría generados cuando un nodo de archivado elimina los datos de objeto de un sistema de almacenamiento de archivado externo es similar a la de los nodos de almacenamiento, excepto que no hay ningún mensaje SREM (Object Store Remove) y hay un mensaje AREM (Archive Object Remove) para cada solicitud de eliminación.

Transacciones de procesamiento de objetos

Puede identificar las transacciones de procesamiento del cliente en el registro de auditoría ubicando mensajes de auditoría específicos de la API (S3 o Swift).

No todos los mensajes de auditoría generados durante una transacción de procesamiento se muestran en las tablas siguientes. Sólo se incluyen los mensajes necesarios para rastrear la transacción de procesamiento.

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"

Mensajes de auditoría de procesamiento rápido

Codificación	Nombre	Descripción	Traza	Consulte
WPUT	Transacción DE SWIFT PUT	Se ha completado correctamente una transacción de procesamiento DE PUT de Swift.	CBID, WCON, WOBJ	"WPUT: SWIFT 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 (SPUT).

En este ejemplo se supone que se ha creado previamente un bloque de S3.

SPUT: 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(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][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 sobre el bloque de S3 y claves o información sobre el contenedor y el objeto de Swift, según qué API se haya utilizado.

```
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 eliminación de objetos en el registro de auditoría ubicando mensajes de auditoría específicos de la API (S3 y Swift).

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"

Elimine mensajes de auditoría de Swift

Codificación	Nombre	Descripción	Traza	Consulte
¡WDEL	Eliminación de Swift	Solicitud realizada para eliminar el objeto de un contenedor o del contenedor.	CBID, WOBJ	"WDEL: ELIMINACIÓN de Swift"

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_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][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 transacciones de recuperación de objetos en el registro de auditoría ubicando mensajes de auditoría específicos de la API (S3 y Swift).

En las tablas siguientes no se enumeran todos los mensajes de auditoría generados durante una transacción de recuperación. Sólo se incluyen los mensajes necesarios para rastrear la transacción de recuperación.

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"

Mensajes de auditoría de recuperación rápida

Codificación	Nombre	Descripción	Traza	Consulte
CONSIGA	OBTENGA Swift	Solicitud realizada para recuperar un objeto de un contenedor.	CBID, WCON, WOBJ	"WGET: Swift 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):SUCS][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][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][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):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):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 estándar 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 las solicitudes se incluyen en el campo HTRH porque se ha configurado como encabezado de protocolo de auditoría (**CONFIGURACIÓN** > **Supervisión** > **servidor de auditoría y syslog**). Consulte "Configurar los mensajes de auditoría y los destinos de registro".

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][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

Mensajes de auditoría: Información general

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 la configuración de niveles de mensajes de auditoría, el cambio de destinos de registro y el uso de un servidor syslog externo para la información de auditoría, consulte "Configurar los mensajes de auditoría y los destinos de registro"

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.	"GNUR: 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.

Codificación	Descripción	Consulte
APCT	Análisis de archivo desde Cloud-Tier: Los datos de objetos archivados se eliminan de un sistema de almacenamiento de archivado externo, que se conecta a StorageGRID a través de la API S3.	"APCT: Purga de archivos desde la capa de cloud"

Codificación	Descripción	Consulte
ARCB	Inicio de recuperación de objetos de archivo: El servicio ARC inicia la recuperación de datos de objetos desde el sistema de almacenamiento de archivos externo.	"ARCB: Inicio de recuperación de objetos de archivo"
ARCE	Fin de recuperación de objeto de archivo: Los datos de objeto se han recuperado de un sistema de almacenamiento de archivos externo y el servicio ARC informa del estado de la operación de recuperación.	"ARCE: Fin de recuperación de objetos archivados"
ARCT	Recuperación de archivo desde Cloud-Tier: Los datos de objetos archivados se recuperan de un sistema de almacenamiento de archivado externo, que se conecta a StorageGRID a través de la API S3.	"ARCT: Recuperación de archivos a partir de nivel de cloud"
AREM	Eliminación de objetos de archivo: Un bloque de contenido se ha eliminado correctamente o sin éxito del sistema de almacenamiento de archivos externo.	"AREM: Eliminación de objeto de archivado"
ASCE	Fin del almacén de objetos archivados: Se ha escrito un bloque de contenido en el sistema de almacenamiento de archivos externo y el servicio ARC informa del estado de la operación de escritura.	"ASCE: Fin del almacén de objetos de archivo"
ASCT	Almacenamiento de archivos Cloud-Tier: Los datos de objetos se almacenan en un sistema de almacenamiento de archivado externo, que se conecta a la StorageGRID a través de la API de S3.	"ASCT: Archive Store Cloud-Tier"
ATCE	Inicio del almacén de objetos de archivado: Se ha iniciado la escritura de un bloque de contenido en un almacenamiento de archivado externo.	"ATCE: Inicio del almacén de objetos de archivado"
AVCC	Validación de archivo Configuración de nivel de cloud: La configuración de la cuenta y el bloque proporcionados se validó correctamente o sin éxito.	"AVCC: Validación de archivo de la configuración de Cloud-Tier"
BROR	Solicitud de solo lectura de bloque: Un bloque entró o salió del modo de solo lectura.	"BROR: Solicitud de solo lectura de bucket"
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"

Codificación	Descripción	Consulte
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 vacía).	"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 de cliente se registran cuando una aplicación cliente S3 o Swift hace 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"
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"

Codificación	Descripción	Utilizado por	Consulte
SHEA	S3 HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o bloque.	Cliente S3	"SHEA: CABEZA S3"
CONSIGA	Swift GET: Registra una transacción realizada correctamente para recuperar un objeto o enumerar los objetos de un contenedor.	Cliente Swift	"WGET: Swift GET"
WHEA	Swift HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o contenedor.	Cliente Swift	"WHEA: CABEZA de Swift"

El cliente escribe mensajes de auditoría

Los mensajes de auditoría de escritura de cliente se registran cuando una aplicación cliente S3 o Swift hace 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.	Clientes S3 y Swift	"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"
¡WDEL	Swift DELETE: Registra una transacción realizada correctamente para eliminar un objeto o un contenedor.	Cliente Swift	"WDEL: ELIMINACIÓN de Swift"

Codificación	Descripción	Utilizado por	Consulte
WPUT	Swift PUT: Registra una transacción correcta para crear un nuevo objeto o contenedor.	Cliente Swift	"WPUT: SWIFT PUT"

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 sobrescrito. Este mensaje de auditoría se genera cuando se elimina automáticamente un objeto sobrescrito para liberar espacio de almacenamiento.	"LKCU: Limpieza de objetos sobrescritos"
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

APCT: Purga de archivos desde la capa de cloud

Este mensaje se genera cuando los datos de objetos archivados se eliminan de un sistema de almacenamiento de archivado externo, que se conecta a la StorageGRID a través de la API S3.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido eliminado.
CSIZ	Tamaño de contenido	El tamaño del objeto en bytes. Siempre devuelve 0.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Código de resultado	Devuelve correcto (SUCS) o el error notificado por el backend.
SUID	Identificador único de almacenamiento	Identificador único (UUID) del nivel de cloud desde el que se eliminó el objeto.

ARCB: Inicio de recuperación de objetos de archivo

Este mensaje se genera cuando se realiza una solicitud para recuperar datos de objeto archivados y comienza el proceso de recuperación. Las solicitudes de recuperación se procesan de forma inmediata, pero se pueden reordenar para mejorar la eficacia de la recuperación de medios lineales como, por ejemplo, la cinta.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido que se va a recuperar del sistema de almacenamiento de archivos externo.
TRANSFORMACIÓN DIGITAL	Resultado	Indica el resultado de iniciar el proceso de recuperación de archivos. El valor definido actualmente es:SUCS: Se recibió la solicitud de contenido y se puso en cola para su recuperación.

Este mensaje de auditoría Marca el tiempo de una recuperación de archivo. Permite hacer coincidir el mensaje con un mensaje ARCE End correspondiente para determinar la duración de la recuperación del archivo y si la operación se ha realizado correctamente.

ARCE: Fin de recuperación de objetos archivados

Este mensaje se genera cuando finaliza un intento del nodo de archivado de recuperar datos de objeto de un sistema de almacenamiento de archivado externo. Si se realiza correctamente, el mensaje indica que los datos del objeto solicitado se han leído completamente desde la ubicación de archivado y se han verificado correctamente. Una vez que se recuperan y verifican los datos del objeto, se envían al servicio que lo solicita.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido que se va a recuperar del sistema de almacenamiento de archivos externo.
VLID	Identificador del volumen	El identificador del volumen en el cual se archivaron los datos. Si no se encuentra una ubicación de archivado para el contenido, se devuelve un ID de volumen 0.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Resultado de la recuperación	El estado de finalización del proceso de recuperación de archivos: • SUCS: Exitoso • VRFL: Error (fallo de verificación del objeto) • ARUN: Error (sistema de almacenamiento de archivado externo no disponible) • CANC: Fallo (operación de recuperación cancelada) • ERROR GENERAL (ERROR general)

La coincidencia de este mensaje con el correspondiente mensaje ARCB puede indicar el tiempo que se tarda en realizar la recuperación del archivo. Este mensaje indica si la recuperación se ha realizado correctamente y, en caso de fallo, la causa del fallo al recuperar el bloque de contenido.

ARCT: Recuperación de archivos a partir de nivel de cloud

Este mensaje se genera cuando se recuperan datos de objetos archivados de un sistema de almacenamiento de archivado externo, que se conecta a la StorageGRID a través de la API de S3.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido recuperado.
CSIZ	Tamaño de contenido	El tamaño del objeto en bytes. El valor sólo es preciso para las recuperar correctamente.
TRANSFORMACIÓN DIGITAL	Código de resultado	Devuelve correcto (SUCS) o el error notificado por el backend.
SUID	Identificador único de almacenamiento	Identificador único (UUID) del sistema de almacenamiento de archivado externo.
TIEMPO	Tiempo	Tiempo de procesamiento total de la solicitud en microsegundos.

AREM: Eliminación de objeto de archivado

El mensaje de auditoría Eliminar objeto de archivado indica que un bloque de contenido se eliminó correctamente o de forma incorrecta de un nodo de archivado. Si el resultado es correcto, el nodo de archivado ha informado correctamente al sistema de almacenamiento de archivado externo que StorageGRID ha lanzado una ubicación de objeto. Si el objeto se elimina del sistema de almacenamiento de archivos externo depende del tipo de sistema y de su configuración.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido que se va a recuperar del sistema de archivos multimedia externo.
VLID	Identificador del volumen	El identificador del volumen en el que se han archivado los datos de objeto.
TRANSFORMACIÓN DIGITAL	Resultado	El estado de finalización del proceso de eliminación de archivos: • SUCS: Exitoso • ARUN: Error (sistema de almacenamiento de archivado externo no disponible) • ERROR GENERAL (ERROR general)

ASCE: Fin del almacén de objetos de archivo

Este mensaje indica que ha finalizado la escritura de un bloque de contenido en un sistema de almacenamiento de archivado externo.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador del bloque de contenido almacenado en el sistema de almacenamiento de archivos externo.
VLID	Identificador del volumen	El identificador único del volumen de archivado en el que se escriben los datos de objetos.
REN	Verificación habilitada	Indica si se realiza la verificación para bloques de contenido. Los valores definidos actualmente son: • VENA: La verificación está activada • VDSA: La verificación está desactivada
MCLS	Clase de Gestión	Cadena que identifica la clase de gestión de TSM a la que se asigna el bloque de contenido si procede.
TRANSFORMACIÓN DIGITAL	Resultado	Indica el resultado del proceso de archivado. Los valores definidos actualmente son: • ÉXITO: Correcto (proceso de archivado realizado correctamente) • OFL: Error (el archivado está sin conexión) • VRFL: Error (fallo de verificación del objeto) • ARUN: Error (sistema de almacenamiento de archivado externo no disponible) • ERROR GENERAL (ERROR general)

Este mensaje de auditoría significa que el bloque de contenido especificado se ha escrito en el sistema de almacenamiento de archivado externo. Si la escritura falla, el resultado ofrece información básica de solución de problemas sobre dónde se produjo el error. Puede encontrar información más detallada acerca de los errores de archivado examinando los atributos del nodo de archivado en el sistema StorageGRID.

ASCT: Archive Store Cloud-Tier

Este mensaje se genera cuando los datos de objetos archivados se almacenan en un sistema de almacenamiento de archivado externo, que se conecta a StorageGRID a través de la API S3.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido recuperado.
CSIZ	Tamaño de contenido	El tamaño del objeto en bytes.
TRANSFORMACIÓN DIGITAL	Código de resultado	Devuelve correcto (SUCS) o el error notificado por el backend.
SUID	Identificador único de almacenamiento	Identificador único (UUID) del nivel de cloud al que se almacenó el contenido.
TIEMPO	Tiempo	Tiempo de procesamiento total de la solicitud en microsegundos.

ATCE: Inicio del almacén de objetos de archivado

Este mensaje indica que se ha iniciado la escritura de un bloque de contenido en un almacenamiento de archivado externo.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido que se va a archivar.
VLID	Identificador del volumen	Identificador único del volumen en el que se escribe el bloque de contenido. Si se produce un error en la operación, se devuelve un ID de volumen 0.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Resultado	Indica el resultado de la transferencia del bloque de contenido. Los valores definidos actualmente son: • ÉXITO (bloque de contenido almacenado correctamente) • EXIS: Ignorado (el bloque de contenido ya estaba almacenado) • ISFD: Error (espacio en disco insuficiente) • STER: Error (error al almacenar el CBID) • OFL: Error (el archivado está sin conexión) • ERROR GENERAL (ERROR general)

AVCC: Validación de archivo de la configuración de Cloud-Tier

Este mensaje se genera cuando se validan las opciones de configuración para un tipo de destino Cloud Tiering: Simple Storage Service (S3).

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Código de resultado	Devuelve correcto (SUCS) o el error notificado por el backend.
SUID	Identificador único de almacenamiento	UUID asociado con la validación del sistema de almacenamiento de archivado externo.

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.

Codificación	Campo	Descripción
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.

Codificación	Campo	Descripción
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.

Codificación	Campo	Descripción
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.

Codificación	Campo	Descripción
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.

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	El tamaño del objeto en bytes. 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.

Codificación	Campo	Descripción
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.
OPERATIVO	Funcionamiento de CGR	Tipo de operación de replicación entre grid que se intentó: • 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 (SUCS) 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 de contenedor	UUID del contenedor para el 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 SUCS 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.

Codificación	Campo	Descripción
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	El motivo del fallo: SCNI: Error en el establecimiento de conexión segura. CERM: Falta el certificado. CERTIFICADO: El certificado no es válido. CERE: El certificado ha caducado. CERR: Se revocó el certificado. CSGN: La firma del certificado no era válida. CSGU: El firmante del certificado era desconocido. UCRM: Faltan credenciales de usuario. UCRI: Las credenciales de usuario no son válidas. UCRU: No se han permitido las credenciales de usuario. TOUT: Tiempo de espera de autenticación agotado.

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: • 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: • 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	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. **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.
TRANSFORMACIÓN DIGITAL	Resultado	El resultado final del estado de la tarea de la cuadrícula: • 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	Este campo 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.
TRANSFORMACIÓN DIGITAL	Resultado	El resultado. Este campo solo tiene un valor: • 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.

Codificación	Campo	Descripción
TSRC	Origen	El origen de la tarea: • 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: • 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: • 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 o contenedores Swift** que no cumplen las normativas. 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.

Codificación	Campo	Descripción
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.
BLOQUEOS	Ubicaciones	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). 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. CLDI: Para los objetos replicados, el ID de nodo LDR y el ID de volumen de la ubicación del objeto. CLNL: ID de nodo DE ARCO de la ubicación del objeto si se archivan los datos del objeto.
RUTA	S3 Bucket/Key o Swift Container/Object ID	El nombre de bloque de S3 y el nombre de clave S3, o el nombre del contenedor de Swift y el identificador de objetos de Swift.
TRANSFORMACIÓN DIGITAL	Resultado	Resultado de la operación de ILM. SUCS: La operación de ILM fue exitosa.
REGLA	Etiqueta de reglas	• 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.

Codificación	Campo	Descripción
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 sobrescritos

Este mensaje se genera cuando StorageGRID elimina un objeto sobrescrito que anteriormente requería una limpieza para liberar espacio de almacenamiento. Un objeto se sobrescribe cuando un cliente S3 o Swift 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	*Uso interno solamente.*
LUID	UUID de objeto eliminado	Identificador del objeto que se ha eliminado.
RUTA	S3 Bucket/Key o Swift Container/Object ID	El nombre de bloque de S3 y el nombre de clave S3, o el nombre del contenedor de Swift y el identificador de objetos de Swift.
SEGC	UUID de contenedor	UUID del contenedor para el 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.

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.
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 `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
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 que no sea UNA solicitud GET o HEAD a la API registra una respuesta con el nombre de usuario, la IP y el tipo de solicitud a la API.

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.

Codificación	Campo	Descripción
MPAT	RUTA de la solicitud	La ruta de la solicitud.
MPQP	Solicitar parámetros de consulta	Los parámetros de consulta para la solicitud.
MRBD	Solicitar el cuerpo	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: • 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** **Nota:** la información confidencial se elimina (por ejemplo, una clave de acceso S3) o se oculta con asteriscos (por ejemplo, una contraseña).
MRMD	Método de solicitud	El método de solicitud HTTP: • PUBLICAR • PUESTO • ELIMINAR • PARCHE
MRSC	Código de respuesta	El código de respuesta.
MRSP	Cuerpo de respuesta	El contenido de la respuesta (el cuerpo de la respuesta) se registra de forma predeterminada. **Nota:** la información confidencial se elimina (por ejemplo, una clave de acceso S3) o se oculta con asteriscos (por ejemplo, una contraseña).
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 Bucket/Key o Swift Container/Object ID	Si está disponible, el nombre del bloque de S3 y el nombre de la clave S3, o el nombre del contenedor de Swift y el identificador de objetos de Swift.
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 o del nodo de archivado de 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.

Codificación	Campo	Descripción
CSIZ	Tamaño de contenido	El tamaño del objeto en bytes.
BLOQUEOS	Ubicaciones	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). 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. CLDI: Para los objetos replicados, el ID de nodo LDR y el ID de volumen de la ubicación del objeto. CLNL: ID de nodo DE ARCO de la ubicación del objeto si se archivan los datos del objeto.
RUTA	S3 Bucket/Key o Swift Container/Object ID	El nombre de bloque de S3 y el nombre de clave S3, o el nombre del contenedor de Swift y el identificador de objetos de Swift.
TRANSFORMACIÓN DIGITAL	Resultado	Resultado de la operación de ILM. SUCS: La operación de ILM fue exitosa.
REGLA	Etiqueta de reglas	La etiqueta legible para seres humanos proporcionada a la regla ILM aplicada a este objeto.
SEGC	UUID de contenedor	UUID del contenedor para el 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	El estado de la operación de ILM. DONE: Se completaron las operaciones de ILM contra el objeto. DFER: El objeto se ha marcado para una futura reevaluación de ILM. PRGD: El objeto se ha eliminado del sistema StorageGRID. 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.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.

Codificación	Campo	Descripción
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.

Codificación	Campo	Descripción
RUTA	La ruta de objetos S3 o Swift	La ruta de objetos S3 o Swift utilizada para el objeto nuevo y el anterior
TRANSFORMACIÓN DIGITAL	Código de resultado	Resultado de la transacción de sobrescritura de objetos. El resultado es siempre: SUCS: Exitoso
SGRP	Planta (grupo)	Si está presente, el objeto sobrescrito se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto sobrescrito.

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.

Codificación	Campo	Descripción
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.
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.
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 ingesta 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.
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	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. `` `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP). `` `x-amz-bypass-governance-retention` se incluye automáticamente si está presente en la solicitud.
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

Codificación	Campo	Descripción
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.
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.

Codificación	Campo	Descripción
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.
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.

Codificación	Campo	Descripción
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	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
MENIDAD	ListObjectsV2	Se solicitó una respuesta *v2 format*. 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 transacción HEAD, se realiza una solicitud para comprobar la existencia de un objeto o bloque y recuperar los metadatos sobre un 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.
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	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
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	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP). (No se espera para SPOS).
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: `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.

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	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP). `x-amz-bypass-governance-retention` se incluye automáticamente si está presente en la solicitud.
LKEN	Bloqueo de objeto activado	Valor de la cabecera de la solicitud `x-amz-bucket-object-lock-enabled`, si está presente en la solicitud.
LKLH	Bloqueo de objeto retención legal	Valor de la cabecera de la 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 la 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 la solicitud `x-amz-object-lock-retain-until-date`, Si está presente en la solicitud PutObject.
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: 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.

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: `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.

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	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
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.
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	Tipo de fallo de verificación: CRCF: Error en la comprobación de redundancia cíclica (CRC). HMAC: Error en la comprobación del código de autenticación de mensajes basados en hash (HMAC). EHSH: Hash de contenido cifrado inesperado. PHSH: Hash de contenido original inesperado. SEQC: Secuencia de datos incorrecta en el disco. PERR: Estructura no válida del archivo de disco. DERR: Error de disco. FNAM: Nombre de archivo incorrecto.

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	La naturaleza del cierre: SUCS: El sistema se cerró limpiamente. DSDN: El sistema no se ha apagado correctamente. VRGN: El sistema se inició por primera vez tras la instalación del servidor (o la reinstalación).

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.

WDEL: ELIMINACIÓN de Swift

Cuando un cliente de Swift emite una transacción DE ELIMINACIÓN, se realiza una solicitud para quitar el objeto o contenedor especificado. 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 contenedores no incluyen este campo.
CSIZ	Tamaño de contenido	El tamaño del objeto eliminado en bytes. Las operaciones en contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
MTME	Hora de la última modificación	La Marca de hora de Unix, en microsegundos, indica cuándo se modificó por última vez el objeto.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Código de resultado	Resultado de la transacción DE ELIMINACIÓN. El resultado es siempre: SUCS: Exitoso
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
SGRP	Planta (grupo)	Si está presente, el objeto se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto.
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.
WACC	ID de cuenta de Swift	El ID de cuenta único especificado por el sistema StorageGRID.
WCON	Contenedor Swift	El nombre del contenedor Swift.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones en contenedores no incluyen este campo.
WUSR	Usuario de la cuenta de Swift	El nombre de usuario de la cuenta de Swift que identifica de manera exclusiva al cliente que realiza la transacción.

WGET: Swift GET

Cuando un cliente de Swift emite una transacción GET, se realiza una solicitud para recuperar un objeto, enumerar los objetos de un contenedor o enumerar los contenedores en una cuenta. 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 cuentas y contenedores no incluyen este campo.

Codificación	Campo	Descripción
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes. Las operaciones en cuentas y contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
TRANSFORMACIÓN DIGITAL	Código de resultado	Resultado DE LA transacción GET. El resultado es siempre SUCS: Exitoso
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
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.
WACC	ID de cuenta de Swift	El ID de cuenta único especificado por el sistema StorageGRID.
WCON	Contenedor Swift	El nombre del contenedor Swift. Las operaciones en las cuentas no incluyen este campo.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones en cuentas y contenedores no incluyen este campo.
WUSR	Usuario de la cuenta de Swift	El nombre de usuario de la cuenta de Swift que identifica de manera exclusiva al cliente que realiza la transacción.

WHEA: CABEZA de Swift

Cuando un cliente de Swift emite una transacción HEAD, se realiza una solicitud para comprobar la existencia de una cuenta, un contenedor o un objeto, y recuperar los

metadatos relevantes. 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 cuentas y contenedores no incluyen este campo.
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes. Las operaciones en cuentas y contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
TRANSFORMACIÓN DIGITAL	Código de resultado	Resultado de la transacción PRINCIPAL. El resultado es siempre: SUCS: Exitoso
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
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.
WACC	ID de cuenta de Swift	El ID de cuenta único especificado por el sistema StorageGRID.
WCON	Contenedor Swift	El nombre del contenedor Swift. Las operaciones en las cuentas no incluyen este campo.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones en cuentas y contenedores no incluyen este campo.

Codificación	Campo	Descripción
WUSR	Usuario de la cuenta de Swift	El nombre de usuario de la cuenta de Swift que identifica de manera exclusiva al cliente que realiza la transacción.

WPUT: SWIFT PUT

Cuando un cliente Swift emite una transacción PUT, se realiza una solicitud para crear un nuevo objeto o contenedor. 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 contenedores no incluyen este campo.
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes. Las operaciones en contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. `` `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP). ``
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: SUCS: Exitoso
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
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
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
WACC	ID de cuenta de Swift	El ID de cuenta único especificado por el sistema StorageGRID.
WCON	Contenedor Swift	El nombre del contenedor Swift.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones en contenedores no incluyen este campo.
WUSR	Usuario de la cuenta de Swift	El nombre de usuario de la cuenta de Swift que identifica de manera exclusiva al cliente que realiza la transacción.

Expanda una cuadrícula

Expandir una cuadrícula: Visión general

Puede expandir la capacidad o las funcionalidades de su sistema StorageGRID sin interrumpir las operaciones del sistema.

La ampliación StorageGRID le permite añadir:

- Volúmenes de almacenamiento a los nodos de almacenamiento
- Nuevos nodos de cuadrícula en un sitio existente
- Un sitio completamente nuevo

El motivo por el que se realiza la expansión determina cuántos nodos nuevos de cada tipo se deben añadir y la ubicación de esos nuevos nodos. Por ejemplo, existen requisitos de nodos diferentes si realiza una ampliación para aumentar la capacidad de almacenamiento, añadir capacidad de metadatos o añadir redundancia o funcionalidades nuevas.

Siga los pasos para el tipo de expansión que está realizando:

Añadir volúmenes de almacenamiento

Siga los pasos de "Añadir volúmenes de almacenamiento a los nodos de almacenamiento".

Agregar nodos de cuadrícula

1. Siga los pasos de "adición de nodos de cuadrícula a un sitio existente".
2. "Actualice las subredes".
3. Desplegar nodos de grid:
   - "Dispositivos"
   - "VMware"
   - "Linux"

> «Linux» se refiere a una implementación de Red Hat Enterprise Linux, Ubuntu o Debian. Para obtener una lista de las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp (IMT)".

4. "Realice la expansión".
5. "Configure el sistema ampliado".

Agregar nuevo sitio

1. Siga los pasos de "Agregar un sitio nuevo".
2. "Actualice las subredes".
3. Desplegar nodos de grid:
   - "Dispositivos"
   - "VMware"
   - "Linux"

> «Linux» se refiere a una implementación de Red Hat Enterprise Linux, Ubuntu o Debian. Para obtener una lista de las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp (IMT)".

4. "Realice la expansión".
5. "Configure el sistema ampliado".

Planifique la ampliación de StorageGRID

Añadir capacidad de almacenamiento

Directrices para añadir capacidad de objeto

Puede expandir la capacidad de almacenamiento de objetos del sistema StorageGRID añadiendo volúmenes de almacenamiento a los nodos de almacenamiento existentes o añadiendo nodos de almacenamiento nuevos a los sitios existentes. Debe añadir capacidad de almacenamiento de modo que cumpla los requisitos de la política de

gestión del ciclo de vida de la información (ILM).

Directrices para añadir volúmenes de almacenamiento

Antes de añadir volúmenes de almacenamiento a los nodos de almacenamiento existentes, revise las siguientes directrices y limitaciones:

- Debe examinar las reglas de ILM actuales para determinar dónde y cuándo hacerlo "añadir volúmenes de almacenamiento" para aumentar el almacenamiento disponible para "objetos replicados" o. "los objetos codificados de borrado".
- No se puede aumentar la capacidad de metadatos del sistema añadiendo volúmenes de almacenamiento, ya que los metadatos de objetos se almacenan solo en el volumen 0.
- Cada nodo de almacenamiento basado en software puede admitir un máximo de 16 volúmenes de almacenamiento. Si necesita añadir capacidad más allá de eso, debe añadir nuevos nodos de almacenamiento.
- Se pueden añadir una o dos bandejas de expansión a cada dispositivo SG6060. Cada bandeja de expansión añade 16 volúmenes de almacenamiento. Con las dos bandejas de expansión instaladas, el SG6060 puede admitir un total de 48 volúmenes de almacenamiento.
- No es posible añadir volúmenes de almacenamiento a ningún otro dispositivo de almacenamiento.
- No es posible aumentar el tamaño de un volumen de almacenamiento existente.
- No es posible añadir volúmenes de almacenamiento a un nodo de almacenamiento al mismo tiempo que realiza una actualización del sistema, una operación de recuperación u otra expansión.

Después de haber decidido añadir volúmenes de almacenamiento y de determinar qué nodos de almacenamiento debe expandir para cumplir con la política de ILM, siga las instrucciones para su tipo de nodo de almacenamiento:

- Para añadir una o dos bandejas de expansión a un dispositivo de almacenamiento SG6060, vaya a. "Añada la bandeja de expansión al SG6060 implementado".
- Para un nodo basado en software, siga las instrucciones de "Añadir volúmenes de almacenamiento a los nodos de almacenamiento".

Directrices para añadir nodos de almacenamiento

Antes de añadir nodos de almacenamiento a sitios existentes, revise las siguientes directrices y limitaciones:

- Debe examinar las reglas de ILM actuales para determinar dónde y cuándo se deben añadir nodos de almacenamiento con el fin de aumentar el almacenamiento disponible para "objetos replicados" o. "los objetos codificados de borrado".
- No se deben añadir más de 10 nodos de almacenamiento en un único procedimiento de ampliación.
- Puede añadir nodos de almacenamiento a más de un sitio en un único procedimiento de ampliación.
- Puede añadir nodos de almacenamiento y otros tipos de nodos en un único procedimiento de ampliación.
- Antes de iniciar el procedimiento de ampliación, debe confirmar que se han completado todas las operaciones de reparación de datos realizadas como parte de una recuperación. Consulte "Compruebe los trabajos de reparación de datos".
- Si necesita quitar nodos de almacenamiento antes o después de realizar una ampliación, no debe retirar más de 10 nodos de almacenamiento en un único procedimiento de nodo de retirada.

Directrices para el servicio ADC en nodos de almacenamiento

Al configurar la expansión, debe elegir si desea incluir el servicio controlador de dominio administrativo (ADC) en cada nodo de almacenamiento nuevo. El servicio ADC realiza un seguimiento de la ubicación y disponibilidad de los servicios de red.

- El sistema StorageGRID requiere un "Quórum de servicios de ADC" estar disponible en todas las instalaciones y en todo momento.
- Al menos tres nodos de almacenamiento en cada sitio deben incluir el servicio ADC.
- No se recomienda agregar el servicio ADC a cada nodo de almacenamiento. La inclusión de demasiados servicios de ADC puede provocar ralentizaciones debido al aumento de la comunicación entre los nodos.
- Un único grid no debe tener más de 48 nodos de almacenamiento con el servicio ADC. Esto equivale a 16 sitios con tres servicios ADC en cada sitio.
- En general, al seleccionar el ajuste **Servicio ADC** para un nodo nuevo, debe seleccionar **automático**. Seleccione **Sí** sólo si el nuevo nodo reemplazará a otro nodo de almacenamiento que incluya el servicio ADC. Debido a que no puede retirar un nodo de almacenamiento si quedan muy pocos servicios ADC, esto garantiza que un nuevo servicio ADC esté disponible antes de eliminar el servicio antiguo.
- No puede agregar el servicio ADC a un nodo después de que se haya desplegado.

Agregar capacidad de almacenamiento para objetos replicados

Si la política de gestión de ciclo de vida de la información (ILM) para la implementación incluye una regla que crea copias replicadas de objetos, debe considerar cuánto almacenamiento añadir y dónde añadir los nuevos volúmenes de almacenamiento o nodos de almacenamiento.

Para obtener una guía sobre dónde añadir almacenamiento adicional, examine las reglas de ILM que crean copias replicadas. Si las reglas de ILM crean dos o más copias de objetos, planifique añadir almacenamiento en cada ubicación donde se realicen copias de objetos. Como ejemplo sencillo, si tiene un grid de dos sitios y una regla de ILM que crea una copia de objeto en cada sitio, debe hacerlo "añadir almacenamiento" a cada sitio para aumentar la capacidad total de objeto de la cuadrícula. Para obtener más información sobre la replicación de objetos, consulte "Qué es la replicación".

Por motivos de rendimiento, debe intentar mantener la capacidad de almacenamiento y la potencia de computación equilibrada en varios sitios. Así pues, para este ejemplo, debería añadir el mismo número de nodos de almacenamiento a cada sitio o volúmenes de almacenamiento adicionales en cada sitio.

Si tiene una política de ILM más compleja que incluye reglas para colocar objetos en distintas ubicaciones en función de criterios como el nombre del bloque o reglas que cambian las ubicaciones de objetos con el tiempo, su análisis de dónde se necesita almacenamiento para la expansión será similar, pero más complejo.

Un gráfico que muestra la rapidez con la que se consume la capacidad de almacenamiento general puede ayudarle a comprender cuánto almacenamiento debe añadir a la expansión y cuándo se necesitará el espacio de almacenamiento adicional. Puede utilizar Grid Manager para "supervise y cree un gráfico de la capacidad de almacenamiento".

Al planificar los plazos de una expansión, recuerde considerar cuánto tiempo puede tardar en obtener e instalar almacenamiento adicional.

Añada capacidad de almacenamiento para objetos codificados de borrado

Si la política de ILM incluye una regla que realiza copias con código de borrado, debe planificar dónde añadir más almacenamiento y cuándo añadir más almacenamiento. La cantidad de almacenamiento que debe añadir y el momento oportuno puede afectar a la capacidad de almacenamiento útil del grid.

El primer paso a la hora de planificar una expansión del almacenamiento es examinar las reglas de la política de ILM que crean objetos codificados de borrado. Como StorageGRID crea fragmentos *k+m* para cada objeto con código de borrado y almacena cada fragmento en un nodo de almacenamiento diferente, debe asegurarse de que al menos los nodos de almacenamiento *k+m* tengan espacio para los nuevos datos codificados con borrado después de la expansión. Si el perfil de código de borrado proporciona protección contra pérdida de sitio, debe añadir almacenamiento a cada sitio. Consulte "¿Qué son los esquemas de código de borrado" para obtener información sobre perfiles de codificación de borrado.

El número de nodos que debe añadir también depende de lo lleno que estén los nodos existentes cuando se realice la ampliación.

Recomendación general sobre la adición de capacidad de almacenamiento para objetos con código de borrado

Si desea evitar cálculos detallados, puede añadir dos nodos de almacenamiento por sitio cuando los nodos de almacenamiento existentes alcancen el 70 % de capacidad.

Esta recomendación general ofrece resultados razonables a través de una amplia gama de esquemas de codificación de borrado para grids individuales y para cuadrículas donde la codificación de borrado proporcione protección frente a pérdidas en las instalaciones.

Para comprender mejor los factores que llevaron a esta recomendación o para desarrollar un plan más preciso para su sitio, consulte "Consideraciones que tener en cuenta al reequilibrar los datos codificados a borrado". Para obtener una recomendación personalizada optimizada para su situación, póngase en contacto con su asesor de servicios profesionales de NetApp.

Consideraciones que tener en cuenta al reequilibrar los datos codificados a borrado

Si va a realizar una ampliación para añadir nodos de almacenamiento y utiliza reglas de ILM para borrar datos de código, es posible que deba realizar el procedimiento de reequilibrio de EC si no puede agregar nodos de almacenamiento suficientes para el esquema de código de borrado que está utilizando.

Después de revisar estas consideraciones, realice la expansión y vaya a. "Reequilibre los datos con código de borrado tras añadir nodos de almacenamiento" para ejecutar el procedimiento.

¿Qué es el reequilibrio de la CE?

El reequilibrado de EC es un procedimiento de StorageGRID que puede ser necesario después de una ampliación de nodo de almacenamiento. El procedimiento se ejecuta como un script de línea de comandos desde el nodo de administración principal. Cuando ejecuta el procedimiento de reequilibrio de EC, StorageGRID redistribuye los fragmentos con código de borrado entre los nodos de almacenamiento existentes y los recién añadidos en un sitio.

Procedimiento de reequilibrio de EC:

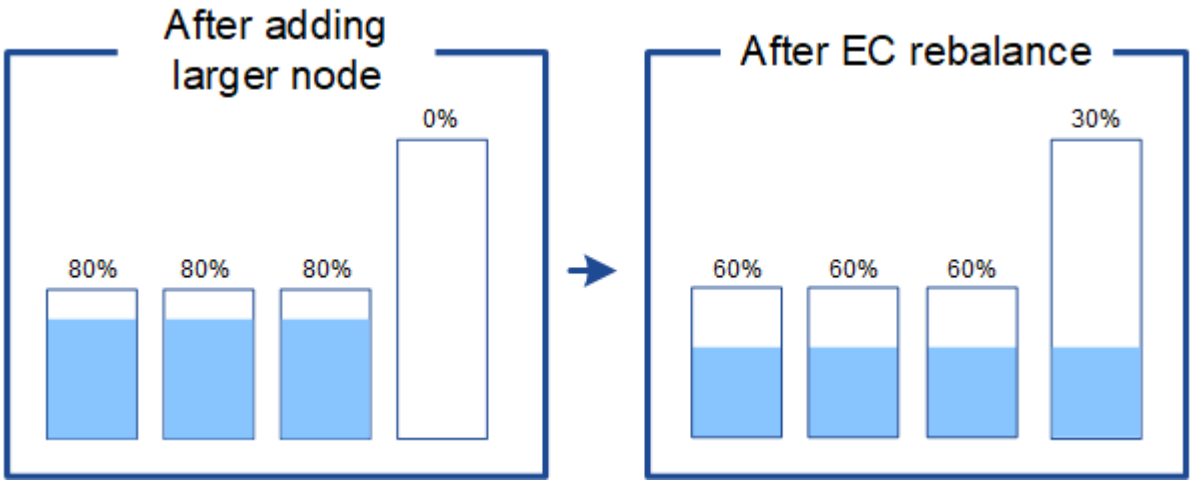
- Solo mueve datos de objetos codificados con borrado. No mueve los datos de objetos replicados.

- Redistribuye los datos dentro de un sitio. No mueve datos de un sitio a otro.
- Redistribuye los datos entre todos los nodos de almacenamiento de un sitio. No redistribuye datos dentro de los volúmenes de almacenamiento.
- No tiene en cuenta el uso de los datos replicados en cada nodo de almacenamiento cuando se determine dónde mover los datos con código de borrado.
- Redistribuye los datos con código de borrado de manera uniforme entre los nodos de almacenamiento sin tener en cuenta las capacidades relativas de cada nodo.
- No distribuirá datos codificados de borrado a los nodos de almacenamiento que tengan una capacidad superior al 80 %.
- Puede reducir el rendimiento de las operaciones de ILM y de las operaciones del cliente Swift y S3 cuando se ejecuta— se necesitan recursos adicionales para redistribuir los fragmentos de código de borrado.

Una vez finalizado el procedimiento de reequilibrio de EC:

- Los datos con código de borrado se habrán movido de los nodos de almacenamiento con menos espacio disponible hasta los nodos de almacenamiento que tienen más espacio disponible.
- La protección de datos de los objetos codificados de borrado no cambiará.
- Los valores usados (%) pueden ser diferentes entre los nodos de almacenamiento por dos motivos:
  - Las copias de objetos replicados seguirán consumiendo espacio en los nodos existentes—El procedimiento de reequilibrio de EC no mueve datos replicados.
  - Los nodos de mayor capacidad estarán relativamente menos completos que los de menor capacidad, a pesar de que todos los nodos acabarán con aproximadamente la misma cantidad de datos codificados de borrado.

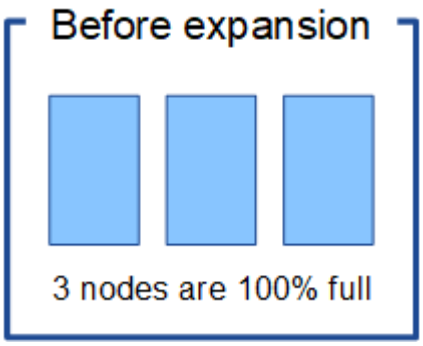
    Por ejemplo, suponga que tres nodos de 200 TB se llenan al 80 % cada uno (200 × 0,8 = 160 TB en cada nodo o 480 TB en el sitio). Si agrega un nodo de 400 TB y ejecuta el procedimiento de reequilibrio, ahora todos los nodos tendrán aproximadamente la misma cantidad de datos de código de borrado (480/4 TB = 120 TB). Sin embargo, el utilizado (%) para el nodo más grande será menor que el usado (%) para los nodos más pequeños.



Cuándo reequilibrar los datos con código de borrado

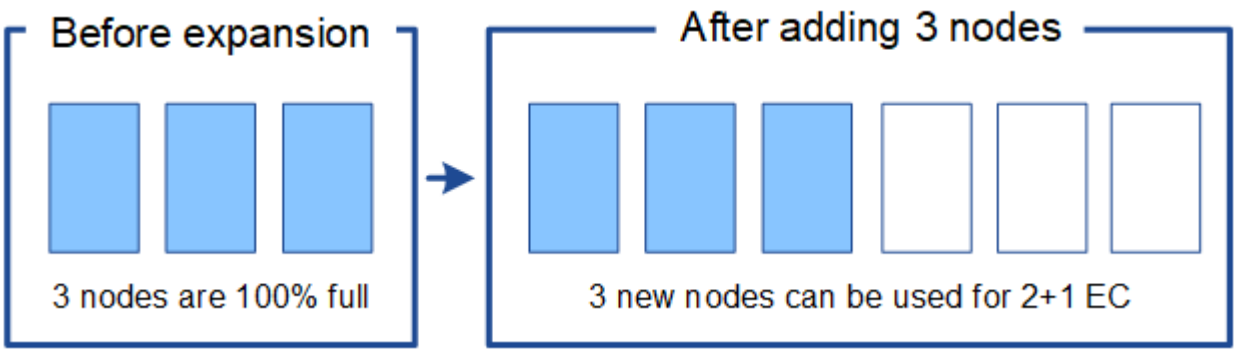
Considere el siguiente escenario:

- StorageGRID se ejecuta en un solo sitio, que contiene tres nodos de almacenamiento.
- La política de ILM usa una regla de codificación de borrado de 2+1 para todos los objetos de mayor tamaño que 1.0 MB y una regla de replicación de 2 copias para los objetos más pequeños.
- Todos los nodos de almacenamiento se han lleno por completo. La alerta **Low Object Storage** se ha disparado en el nivel de gravedad principal.



No es necesario reequilibrar si se agregan suficientes nodos

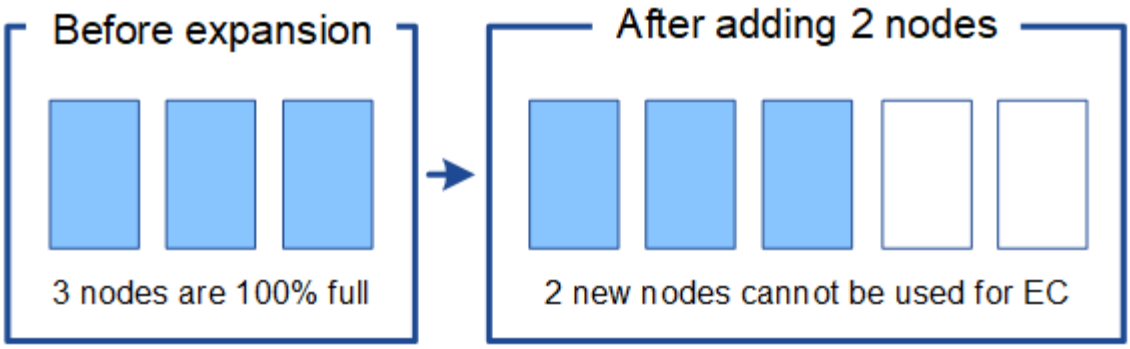
Para comprender cuándo no es necesario reequilibrar EC, suponga que se han añadido tres (o más) nuevos nodos de almacenamiento. En este caso, no es necesario realizar un reequilibrio de EC. Los nodos de almacenamiento originales se mantendrán llenos, pero los objetos nuevos ahora usarán los tres nodos nuevos para 2+1 código de borrado—Los dos fragmentos de datos y el fragmento de paridad único podrán almacenarse en un nodo diferente.



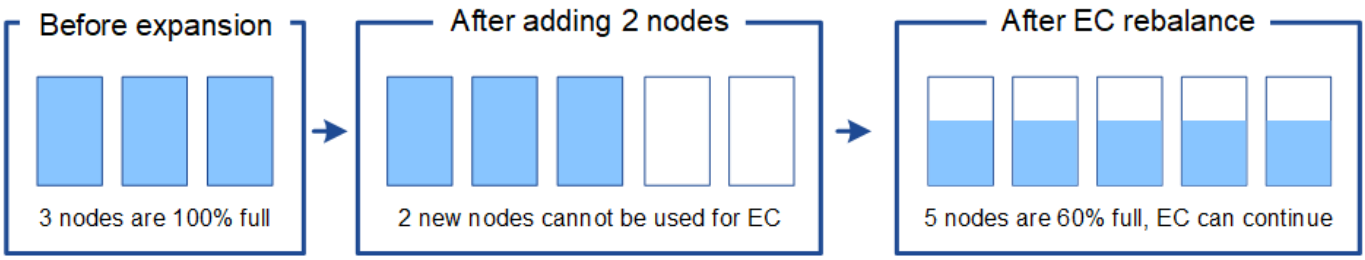
Aunque puede ejecutar el procedimiento de equilibrio de EC en este caso, mover los datos existentes con código de borrado reducirá temporalmente el rendimiento del grid, lo que puede afectar a las operaciones del cliente.

Si no puede agregar suficientes nodos, es necesario reequilibrar

Para comprender cuándo es necesario reequilibrar EC, suponga que solo puede añadir dos nodos de almacenamiento, en lugar de tres. Dado que el esquema de 2+1 requiere al menos tres nodos de almacenamiento para tener espacio disponible, los nodos vacíos no se pueden usar para nuevos datos codificados de borrado.



Para utilizar los nuevos nodos de almacenamiento, debe ejecutar el procedimiento de reequilibrio de EC. Cuando este procedimiento se ejecuta, StorageGRID redistribuye los datos existentes con código de borrado y los fragmentos de paridad entre todos los nodos de almacenamiento del sitio. En este ejemplo, cuando se haya completado el procedimiento de reequilibrio de EC, los cinco nodos ahora sólo estarán llenos al 60 % y los objetos pueden seguir ingiriendo en el esquema de código de borrado 2+1 en todos los nodos de almacenamiento.



Recomendaciones para el reequilibrio de EC

NetApp requiere el reequilibrio de EC si *all* de las siguientes afirmaciones son verdaderas:

- Se utiliza la codificación de borrado para los datos de objetos.
- La alerta **almacenamiento de objetos bajo** se ha activado para uno o más nodos de almacenamiento de un sitio, lo que indica que los nodos están al menos un 80% llenos.
- No puede añadir nodos de almacenamiento nuevos suficientes para el esquema de codificación de borrado en uso. Consulte "Añada capacidad de almacenamiento para objetos codificados de borrado".
- Sus clientes de S3 y Swift pueden tolerar un menor rendimiento de sus operaciones de escritura y lectura mientras se ejecuta el procedimiento de reequilibrio de EC.

Opcionalmente, puede ejecutar el procedimiento de reequilibrio de EC si prefiere que los nodos de almacenamiento se llenen a niveles similares y los clientes S3 y Swift pueden tolerar un menor rendimiento en sus operaciones de escritura y lectura mientras se ejecuta el procedimiento de reequilibrio de EC.

La forma en que el procedimiento de reequilibrio de EC interactúa con otras tareas de mantenimiento

No puede realizar determinados procedimientos de mantenimiento al mismo tiempo que ejecuta el procedimiento de reequilibrio de EC.

Procedimiento	Permitido durante el procedimiento de reequilibrio de EC?
Procedimientos adicionales de reequilibrio de EC	No Sólo puede ejecutar un procedimiento de reequilibrio de EC a la vez.
Procedimiento de retirada Trabajo de reparación de datos de EC	No • Se le impide iniciar un procedimiento de retirada de servicio o una reparación de datos de EC mientras se está ejecutando el procedimiento de reequilibrio de EC. • Se le impide iniciar el procedimiento de reequilibrio de EC mientras se ejecuta un procedimiento de retirada del nodo de almacenamiento o una reparación de datos de EC.
Procedimiento de expansión	No Si necesita añadir nodos de almacenamiento nuevos en una ampliación, ejecute el procedimiento de reequilibrio de EC después de agregar todos los nodos nuevos.
Procedimiento de actualización	No Si necesita actualizar el software StorageGRID, realice el procedimiento de actualización antes o después de ejecutar el procedimiento de reequilibrio de EC. Según sea necesario, puede finalizar el procedimiento de reequilibrio de EC para realizar una actualización de software.
Procedimiento de clonación del nodo de dispositivos	No Si necesita clonar un nodo de almacenamiento de dispositivo, ejecute el procedimiento de reequilibrio de EC después de agregar el nuevo nodo.
Procedimiento de revisión	Sí. Puede aplicar una revisión StorageGRID mientras se ejecuta el procedimiento de reequilibrio de EC.
Otros procedimientos de mantenimiento	No Debe finalizar el procedimiento de reequilibrio de EC antes de ejecutar otros procedimientos de mantenimiento.

La interacción del procedimiento de reequilibrio de EC con ILM

Mientras se ejecuta el procedimiento de reequilibrio de EC, evite realizar cambios en la gestión de la información durante el proceso que puedan cambiar la ubicación de los objetos ya codificados de borrado. Por ejemplo, no empiece a utilizar una regla de ILM que tenga un perfil de código de borrado diferente. Si necesita realizar estos cambios en ILM, debe finalizar el procedimiento de reequilibrio de EC.

Añada capacidad de metadatos

Para garantizar que haya espacio adecuado disponible para los metadatos de objetos, puede que deba realizar un procedimiento de ampliación para añadir nuevos nodos de almacenamiento en cada sitio.

StorageGRID reserva espacio para los metadatos del objeto en el volumen 0 de cada nodo de almacenamiento. En cada sitio se mantienen tres copias de todos los metadatos de objetos, distribuidas uniformemente por todos los nodos de almacenamiento.

Puede usar Grid Manager para supervisar la capacidad de metadatos de los nodos de almacenamiento y calcular la rapidez con la que se consume la capacidad de metadatos. Además, la alerta **almacenamiento de metadatos bajo** se activa para un nodo de almacenamiento cuando el espacio de metadatos utilizado alcanza determinados umbrales.

Tenga en cuenta que la capacidad de metadatos de objetos de un grid se puede consumir con mayor rapidez que la capacidad de almacenamiento de objetos, en función de cómo se utilice el grid. Por ejemplo, si normalmente procesa grandes cantidades de objetos pequeños o añade grandes cantidades de metadatos de usuario o etiquetas a objetos, es posible que deba añadir nodos de almacenamiento para aumentar la capacidad de metadatos aunque haya suficiente capacidad de almacenamiento de objetos.

Para obtener más información, consulte lo siguiente:

- "Gestione el almacenamiento de metadatos de objetos"
- "Supervise la capacidad de metadatos de los objetos para cada nodo de almacenamiento"

Directrices para aumentar la capacidad de metadatos

Antes de añadir nodos de almacenamiento para aumentar la capacidad de metadatos, revise las siguientes directrices y limitaciones:

- Suponiendo que haya suficiente capacidad de almacenamiento de objetos disponible, tener más espacio disponible para los metadatos de objetos aumenta el número de objetos que se pueden almacenar en su sistema StorageGRID.
- Es posible aumentar la capacidad de metadatos de un grid si se añaden uno o varios nodos de almacenamiento a cada sitio.
- El espacio real reservado para los metadatos del objeto en un nodo de almacenamiento determinado depende de la opción de almacenamiento de espacio reservado de metadatos (configuración para todo el sistema), la cantidad de RAM asignada al nodo y el tamaño del volumen del nodo 0.
- No se puede aumentar la capacidad de metadatos añadiendo volúmenes de almacenamiento a los nodos de almacenamiento existentes, ya que los metadatos se almacenan solo en el volumen 0.
- No se puede aumentar la capacidad de los metadatos añadiendo un sitio nuevo.
- StorageGRID conserva tres copias de todos los metadatos de objetos en cada sitio. Por esta razón, la capacidad de metadatos de su sistema está limitada por la capacidad de metadatos de su sitio más pequeño.
- Cuando se añade capacidad de metadatos, debe añadir el mismo número de nodos de almacenamiento a cada sitio.

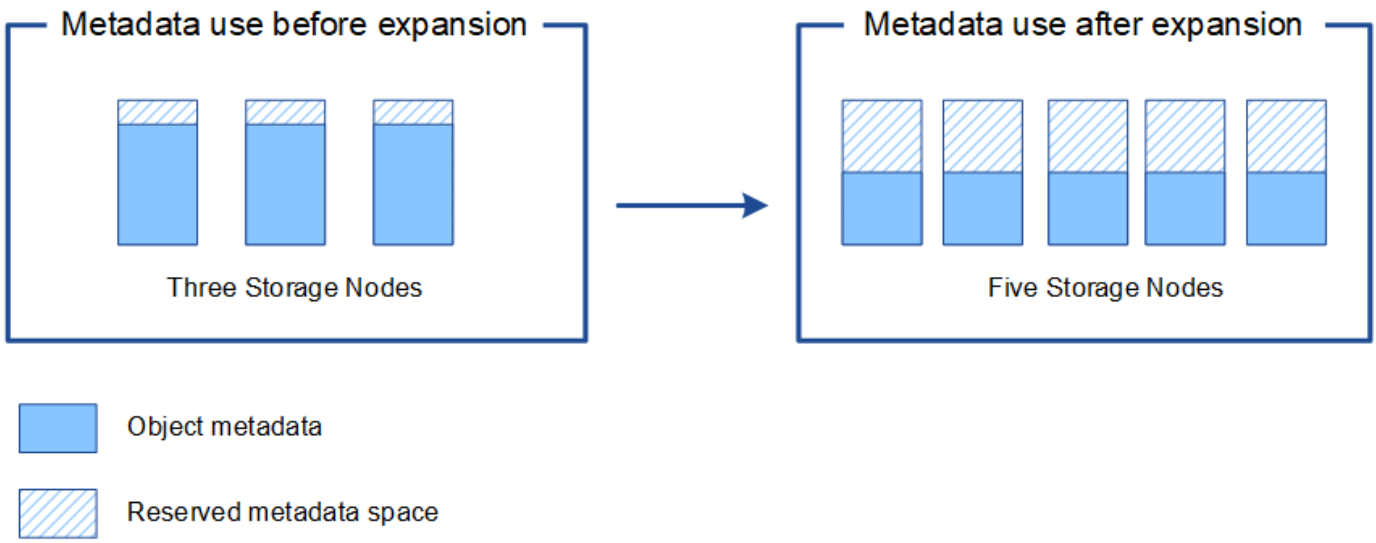
Consulte "Descripción del espacio reservado de metadatos".

La forma en que se redistribuyen los metadatos cuando se añaden nodos de almacenamiento

Cuando se añaden nodos de almacenamiento en una expansión, StorageGRID redistribuye los metadatos de objetos existentes a los nodos nuevos de cada sitio, lo que aumenta la capacidad general de metadatos del grid. No se requiere ninguna acción del usuario.

La figura siguiente muestra cómo StorageGRID redistribuye los metadatos de objetos cuando añade nodos de almacenamiento en una expansión. El lado izquierdo de la figura representa el volumen 0 de tres nodos de almacenamiento antes de la ampliación. Los metadatos consumen una parte relativamente grande del espacio de metadatos disponible de cada nodo y se ha activado la alerta **almacenamiento de metadatos bajo**.

El lado derecho de la figura muestra cómo se redistribuyen los metadatos existentes después de agregar dos nodos de almacenamiento al sitio. La cantidad de metadatos en cada nodo ha disminuido, la alerta **almacenamiento de metadatos bajo** ya no se activa y ha aumentado el espacio disponible para los metadatos.



Añada nodos de grid para añadir funcionalidades al sistema

Es posible añadir redundancia o funcionalidades adicionales a un sistema StorageGRID añadiendo nodos grid a las ubicaciones existentes.

Por ejemplo, puede optar por agregar nodos de puerta de enlace para utilizarlos en un grupo de alta disponibilidad (HA), o puede agregar un nodo de administración en un sitio remoto para permitir la supervisión mediante un nodo local.

Los siguientes tipos de nodos se pueden añadir uno o varios de ellos en uno o varios sitios existentes en una sola operación de ampliación:

- Nodos de administrador no primario
- Nodos de almacenamiento
- Nodos de puerta de enlace

Al preparar la adición de nodos de grid, tenga en cuenta las siguientes limitaciones:

- El nodo de administrador principal se pone en marcha durante la instalación inicial. No puede agregar un nodo de administración principal durante una expansión.

- En la misma expansión, puede añadir nodos de almacenamiento y otros tipos de nodos.
- Cuando añada nodos de almacenamiento, debe planificar con cuidado el número y la ubicación de los nodos nuevos. Consulte "Directrices para añadir capacidad de objeto".
- Si la opción **Establecer nuevo nodo predeterminado** es **Sin confianza** en la pestaña Redes de cliente sin confianza de la página de control del firewall, las aplicaciones cliente que se conecten a los nodos de expansión mediante la red cliente deben conectarse mediante un puerto de punto final del equilibrador de carga (**CONFIGURACIÓN** > **Seguridad** > **Control del firewall**). Consulte las instrucciones a. "cambie la configuración de seguridad del nuevo nodo" y a. "configurar puntos finales de equilibrio de carga".

Agregar un sitio nuevo

Puede ampliar su sistema StorageGRID añadiendo un sitio nuevo.

Directrices para agregar un sitio

Antes de agregar un sitio, revise los siguientes requisitos y limitaciones:

- Solo puede añadir un sitio por operación de ampliación.
- No puede agregar nodos de grid a un sitio existente como parte de la misma expansión.
- Todos los sitios deben incluir al menos tres nodos de almacenamiento.
- La adición de un sitio nuevo no aumenta automáticamente el número de objetos que se pueden almacenar. La capacidad total de objetos de un grid depende de la cantidad de almacenamiento disponible, la política de ILM y la capacidad de metadatos de cada sitio.
- Al ajustar el tamaño a un sitio nuevo, debe asegurarse de que incluya suficiente capacidad de metadatos.

  StorageGRID mantiene una copia de todos los metadatos de objetos en cada sitio. Al añadir un sitio nuevo, debe asegurarse de que incluya la capacidad de metadatos suficiente para los metadatos del objeto existente y la capacidad de metadatos suficiente para crecer.

  Para obtener más información, consulte lo siguiente:

  - "Gestione el almacenamiento de metadatos de objetos"
  - "Supervise la capacidad de metadatos de los objetos para cada nodo de almacenamiento"
- Debe tener en cuenta el ancho de banda de red disponible entre los sitios y el nivel de latencia de red. Las actualizaciones de los metadatos se replican continuamente entre los sitios aunque todos los objetos se almacenan solo en el sitio donde se ingieren.
- Dado que el sistema StorageGRID permanece operativo durante la ampliación, debe revisar las reglas de ILM antes de iniciar el procedimiento de ampliación. Debe asegurarse de que las copias de objetos no se almacenan en el nuevo sitio hasta que se complete el procedimiento de expansión.

  Por ejemplo, antes de iniciar la expansión, determine si existen reglas que utilizan el pool de almacenamiento predeterminado (todos los nodos de almacenamiento). Si lo hacen, debe crear un nuevo pool de almacenamiento que contenga los nodos de almacenamiento existentes y actualizar las reglas de ILM para usar el nuevo pool de almacenamiento. De lo contrario, los objetos se copiarán en el sitio nuevo tan pronto como el primer nodo de ese sitio se active.

  Para obtener más información sobre cómo cambiar ILM al agregar un sitio nuevo, consulte "Ejemplo de cambio de una política de ILM".

Reúna los materiales necesarios

Antes de realizar una operación de expansión, recopile los materiales e instale y configure cualquier hardware y redes nuevos.

Elemento	Notas
Archivo de instalación de StorageGRID	Si va a añadir nodos de grid o un sitio nuevo, debe descargar y extraer el archivo de instalación de StorageGRID. Debe utilizar la misma versión que se esté ejecutando actualmente en la cuadrícula. Para obtener más detalles, consulte las instrucciones de Descarga y extracción de los archivos de instalación de StorageGRID. **Nota:** No es necesario descargar archivos si está agregando nuevos volúmenes de almacenamiento a los nodos de almacenamiento existentes o instalando un nuevo dispositivo StorageGRID.
Portátil de servicio	El portátil de servicio tiene lo siguiente: • Puerto de red • Cliente SSH (por ejemplo, PuTTY) • "Navegador web compatible"
`Passwords.txt` archivo	Contiene las contraseñas que se necesitan para acceder a los nodos de grid en la línea de comandos. Incluido en el paquete de recuperación.
Clave de acceso de aprovisionamiento	La frase de contraseña se crea y documenta cuando se instala el sistema StorageGRID por primera vez. La clave de acceso de aprovisionamiento no está en la `Passwords.txt` archivo.
Documentación de StorageGRID	• "Administre StorageGRID" • "Notas de la versión" • Instrucciones de instalación para su plataforma ◦ "Instalar StorageGRID en Red Hat Enterprise Linux" ◦ "Instalar StorageGRID en Ubuntu o Debian" ◦ "Instale StorageGRID en VMware"
La documentación actual de su plataforma	Para conocer las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad (IMT)".

Descargue y extraiga los archivos de instalación de StorageGRID

Antes de poder añadir nuevos nodos de grid o un sitio nuevo, debe descargar el archivo de instalación de StorageGRID correspondiente y extraer los archivos.

Acerca de esta tarea

Es necesario realizar operaciones de ampliación con la versión de StorageGRID que se está ejecutando en el grid.

Pasos

1. Vaya a. "Descargas de NetApp: StorageGRID".
2. Seleccione la versión de StorageGRID que se está ejecutando actualmente en la cuadrícula.
3. Inicie sesión con el nombre de usuario y la contraseña de su cuenta de NetApp.
4. Lea el Contrato de licencia de usuario final, seleccione la casilla de verificación y, a continuación, seleccione * Aceptar y continuar *.
5. En la columna **instalar StorageGRID** de la página de descarga, seleccione `.tgz` o. `.zip` archivar para su plataforma.

   La versión que se muestra en el archivo de archivo de instalación debe coincidir con la versión del software que está instalado actualmente.

   Utilice la `.zip` Archivo si está ejecutando Windows en el portátil de servicio.

Plataforma	Archivo de instalación

Red Hat Enterprise Linux	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`

Ubuntu o Debian o dispositivos	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`

VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`

OpenStack/otro hipervisor	Para ampliar una puesta en marcha existente en OpenStack, debe implementar una máquina virtual que ejecute una de las distribuciones de Linux admitidas que se indican anteriormente y seguir las instrucciones correspondientes para Linux.

6. Descargue y extraiga el archivo de archivo.
7. Siga el paso adecuado para que su plataforma elija los archivos que necesite, en función de su plataforma, la topología de cuadrícula planificada y cómo ampliará su sistema StorageGRID.

   Las rutas enumeradas en el paso de cada plataforma son relativas al directorio de nivel superior instalado por el archivo de archivado.

8. Si va a ampliar un sistema Red Hat Enterprise Linux, seleccione los archivos adecuados.

Ruta y nombre de archivo	Descripción
	Archivo de texto que describe todos los archivos contenidos en el archivo de descarga de StorageGRID.
	Una licencia gratuita que no proporciona ningún derecho de soporte para el producto.
	Paquete DE RPM para instalar las imágenes de los nodos StorageGRID en los hosts RHEL.
	Paquete DE RPM para instalar el servicio de host StorageGRID en los hosts de RHEL.
Herramienta de secuencia de comandos de la implementación	Descripción
	Script Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Una secuencia de comandos Python que se utiliza para automatizar la configuración de los dispositivos StorageGRID.
	Ejemplo de archivo de configuración para utilizar con `configure-storagegrid.py` guión.
	Ejemplo de secuencia de comandos Python que puede utilizar para iniciar sesión en la API de gestión de grid cuando está activado el inicio de sesión único. También puede utilizar este script para ping federate.
	Un archivo de configuración en blanco para usar con el `configure-storagegrid.py` guión.
	Ejemplo de rol y libro de estrategia de Ansible para configurar hosts de RHEL para la puesta en marcha del contenedor StorageGRID. Puede personalizar el rol o el libro de estrategia según sea necesario.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de grid cuando se activa el inicio de sesión único (SSO) mediante Active Directory o ping federate.

Ruta y nombre de archivo	Descripción
	Un guion de ayuda llamado por el compañero `storagegrid-ssoauth-azure.py` Script de Python para realizar interacciones SSO con Azure.
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno StorageGRID que no sea de producción para probar la compatibilidad de la actualización.

1. Si va a ampliar un sistema Ubuntu o Debian, seleccione los archivos apropiados.

Ruta y nombre de archivo	Descripción
	Archivo de texto que describe todos los archivos contenidos en el archivo de descarga de StorageGRID.
	Un archivo de licencia de NetApp que no es de producción y que se puede usar para pruebas e implementaciones conceptuales.
	PAQUETE DEB para instalar las imágenes del nodo StorageGRID en hosts de Ubuntu o Debian.
	Suma de comprobación MD5 para el archivo `/debs/storagegrid-webscale-images-version-SHA.deb`.
	PAQUETE DEB para instalar el servicio de host de StorageGRID en hosts de Ubuntu o Debian.
Herramienta de secuencia de comandos de la implementación	Descripción
	Script Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Una secuencia de comandos Python que se utiliza para automatizar la configuración de los dispositivos StorageGRID.

Ruta y nombre de archivo	Descripción
	Ejemplo de secuencia de comandos Python que puede utilizar para iniciar sesión en la API de gestión de grid cuando está activado el inicio de sesión único. También puede utilizar este script para ping federate.
	Ejemplo de archivo de configuración para utilizar con `configure-storagegrid.py` guión.
	Un archivo de configuración en blanco para usar con el `configure-storagegrid.py` guión.
	Ejemplo de rol de Ansible y libro de aplicaciones para configurar hosts Ubuntu o Debian para la implementación del contenedor StorageGRID. Puede personalizar el rol o el libro de estrategia según sea necesario.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de grid cuando se activa el inicio de sesión único (SSO) mediante Active Directory o ping federate.
	Un guion de ayuda llamado por el compañero `storagegrid-ssoauth-azure.py` Script de Python para realizar interacciones SSO con Azure.
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno StorageGRID que no sea de producción para probar la compatibilidad de la actualización.

1. Si va a ampliar un sistema VMware, seleccione los archivos adecuados.

Ruta y nombre de archivo	Descripción
	Archivo de texto que describe todos los archivos contenidos en el archivo de descarga de StorageGRID.
	Una licencia gratuita que no proporciona ningún derecho de soporte para el producto.

Ruta y nombre de archivo	Descripción
	El archivo de disco de máquina virtual que se usa como plantilla para crear máquinas virtuales del nodo de grid.
	El archivo de plantilla Abrir formato de virtualización (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar el nodo de administración principal.
	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de administración no primarios.
	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de archivado.
	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de puerta de enlace.
	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de almacenamiento basados en máquinas virtuales.
Herramienta de secuencia de comandos de la implementación	Descripción
	Una secuencia de comandos de shell Bash que se utiliza para automatizar la implementación de nodos de cuadrícula virtual.
	Ejemplo de archivo de configuración para utilizar con `deploy-vsphere-ovftool.sh` guión.
	Script Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Una secuencia de comandos Python que se utiliza para automatizar la configuración de los dispositivos StorageGRID.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de grid cuando se activa el inicio de sesión único (SSO). También puede utilizar este script para ping federate.

Ruta y nombre de archivo	Descripción
	Ejemplo de archivo de configuración para utilizar con `configure-storagegrid.py` guión.
	Un archivo de configuración en blanco para usar con el `configure-storagegrid.py` guión.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de grid cuando se activa el inicio de sesión único (SSO) mediante Active Directory o ping federate.
	Un guion de ayuda llamado por el compañero `storagegrid-ssoauth-azure.py` Script de Python para realizar interacciones SSO con Azure.
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno StorageGRID que no sea de producción para probar la compatibilidad de la actualización.

1. Si va a ampliar un sistema basado en dispositivos StorageGRID, seleccione los archivos adecuados.

Ruta y nombre de archivo	Descripción
	DEB el paquete para instalar las imágenes de nodo StorageGRID en sus dispositivos.
	Suma de comprobación MD5 para el archivo `/debs/storagegridwebscale-images-version-SHA.deb`.

Para la instalación del dispositivo, estos archivos sólo son necesarios si necesita evitar el tráfico de red. El dispositivo puede descargar los archivos necesarios del nodo de administración principal.

Verifique el hardware y las redes

Antes de iniciar la ampliación del sistema StorageGRID, asegúrese de lo siguiente:

- Se ha instalado y configurado el hardware necesario para admitir los nuevos nodos de grid o un sitio nuevo.
- Todos los nodos nuevos tienen rutas de comunicación bidireccionales con todos los nodos nuevos y

existentes (un requisito para la red de grid). En particular, confirme que los siguientes puertos TCP están abiertos entre los nuevos nodos que está añadiendo en la ampliación y el nodo de administración principal:

  - 1055
  - 7443
  - 8011
  - 10342

  Consulte "Comunicaciones internas de los nodos de grid".

- El nodo de administración principal se puede comunicar con todos los servidores de expansión que tienen la intención de alojar el sistema StorageGRID.
- Si alguno de los nodos nuevos tiene una dirección IP de red de cuadrícula en una subred que no se ha utilizado anteriormente, ya lo ha hecho "se añadió la nueva subred" A la lista subred de red de cuadrícula. De lo contrario, tendrá que cancelar la expansión, agregar la nueva subred e iniciar el procedimiento de nuevo.
- No está utilizando la traducción de direcciones de red (NAT) en la red de grid entre nodos de grid o entre sitios de StorageGRID. Cuando utilice direcciones IPv4 privadas para la red de cuadrícula, esas direcciones deben poder enrudarse directamente desde cada nodo de cuadrícula de cada sitio. El uso de NAT para conectar la red de red a través de un segmento de red pública solo se admite si se utiliza una aplicación de túnel que es transparente para todos
  Nodos en la cuadrícula, lo que significa que los nodos de grid no necesitan conocimientos de las direcciones IP públicas.

  Esta restricción NAT es específica de los nodos de cuadrícula y de la red de cuadrícula. Según sea necesario, puede utilizar NAT entre clientes externos y nodos de cuadrícula, por ejemplo, para proporcionar una dirección IP pública para un nodo de puerta de enlace.

Añadir volúmenes de almacenamiento

Añada volúmenes de almacenamiento a los nodos de almacenamiento

Puede ampliar la capacidad de almacenamiento de los nodos de almacenamiento que tengan 16 o menos volúmenes de almacenamiento agregando volúmenes de almacenamiento adicionales. Es posible que deba añadir volúmenes de almacenamiento a más de un nodo de almacenamiento para satisfacer los requisitos de ILM para las copias replicadas o codificadas de borrado.

Antes de empezar

Antes de añadir volúmenes de almacenamiento, revise el "directrices para añadir capacidad de objeto" Para garantizar que sabe dónde añadir volúmenes para cumplir con los requisitos de la política de ILM.

> Estas instrucciones se aplican solamente a los nodos de almacenamiento basados en software. Consulte "Añada la bandeja de expansión al SG6060 implementado" Para obtener información sobre cómo añadir volúmenes de almacenamiento a SG6060 mediante la instalación de bandejas de expansión. No se pueden expandir otros nodos de almacenamiento del dispositivo.

Acerca de esta tarea

El almacenamiento subyacente de un nodo de almacenamiento se divide en volúmenes de almacenamiento. Los volúmenes de almacenamiento son dispositivos de almacenamiento basados en bloques con formato del sistema StorageGRID y montados para almacenar objetos. Cada nodo de almacenamiento puede admitir hasta 16 volúmenes de almacenamiento, que se denominan *object store* en Grid Manager.

> Los metadatos de objetos siempre se almacenan en el almacén de objetos 0.

Cada almacén de objetos se monta en un volumen que corresponde a su ID. Por ejemplo, el almacén de objetos con un ID de 0000 corresponde al `/var/local/rangedb/0` punto de montaje.

Antes de agregar nuevos volúmenes de almacenamiento, utilice Grid Manager para ver los almacenes de objetos actuales de cada nodo de almacenamiento, así como los puntos de montaje correspondientes. Esta información se puede usar al añadir volúmenes de almacenamiento.

Pasos

1. Seleccione **NODES** > ***site*** > ***Storage Node*** > **Storage**.
2. Desplácese hacia abajo para ver la cantidad de almacenamiento disponible para cada volumen y almacén de objetos.

   Para los nodos de almacenamiento del dispositivo, el nombre mundial de cada disco coincide con el identificador a nivel mundial (WWID) del volumen que aparece cuando se ven las propiedades de volumen estándar en el sistema operativo SANtricity (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
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

3. Siga las instrucciones para que su plataforma añada volúmenes de almacenamiento nuevos al nodo de almacenamiento.
   - "VMware: Añada volúmenes de almacenamiento al nodo de almacenamiento"
   - "Linux: Añada volúmenes SAN o de conexión directa al nodo de almacenamiento"

VMware: Añada volúmenes de almacenamiento al nodo de almacenamiento

Si un nodo de almacenamiento incluye menos de 16 volúmenes de almacenamiento, es posible aumentar su capacidad mediante VMware vSphere para añadir volúmenes.

Antes de empezar

- Tendrá acceso a las instrucciones de instalación de StorageGRID para implementaciones de VMware.
  - "Instale StorageGRID en VMware"
- Usted tiene la `Passwords.txt` archivo.
- Ya tienes "permisos de acceso específicos".

> No intente añadir volúmenes de almacenamiento a un nodo de almacenamiento mientras haya activo una actualización de software, un procedimiento de recuperación o otro procedimiento de ampliación.

Acerca de esta tarea

El nodo de almacenamiento no está disponible durante un breve periodo de tiempo cuando se añaden volúmenes de almacenamiento. Debe realizar este procedimiento en un nodo de almacenamiento a la vez para evitar que se vean afectados los servicios de grid orientados al cliente.

Pasos

1. Si es necesario, instale nuevo hardware de almacenamiento y cree nuevos almacenes de datos VMware.
2. Agregue uno o más discos duros a la máquina virtual para usarlos como almacenamiento (almacenes de objetos).
   a. Abra VMware vSphere Client.
   b. Edite la configuración de la máquina virtual para agregar uno o más discos duros adicionales.

   Los discos duros suelen configurarse como discos de máquina virtual (VMDK). Los VMDK se utilizan más habitualmente y son más fáciles de gestionar, mientras que los RDM pueden ofrecer un mejor rendimiento a cargas de trabajo que utilizan tamaños de objeto mayores (por ejemplo, mayores de 100 MB). Para obtener más información sobre cómo añadir discos duros a máquinas virtuales, consulte la documentación de VMware vSphere.
3. Reinicie la máquina virtual mediante la opción **Restart Guest OS** en VMware vSphere Client, o introduciendo el comando siguiente en una sesión ssh en la máquina virtual:`sudo reboot`

   > No utilice **Apagar** o **Restablecer** para reiniciar la máquina virtual.
4. Configure el nuevo almacenamiento para que lo utilice el nodo de almacenamiento:
   a. Inicie sesión en el nodo de grid:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

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

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

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

b. Configure los nuevos volúmenes de almacenamiento:

```
sudo add_rangedbs.rb
```

Este script encuentra todos los volúmenes de almacenamiento nuevos y solicita que se los formatee.

c. Introduzca **y** para aceptar el formato.

d. Si alguno de los volúmenes se ha formateado anteriormente, decida si desea reformatearlos.

- Introduzca **y** para cambiar el formato.
- Introduzca **n** para omitir el formateo.

La `setup_rangedbs.sh` el script se ejecuta automáticamente.

5. Compruebe que los servicios se inician correctamente:

a. Ver una lista del estado de todos los servicios del servidor:

```
sudo storagegrid-status
```

El estado se actualiza automáticamente.

a. Espere a que todos los servicios se ejecuten o se verifiquen.

b. Salir de la pantalla de estado:

```
Ctrl+C
```

6. Compruebe que el nodo de almacenamiento esté en línea:

a. Inicie sesión en Grid Manager mediante una "navegador web compatible".

b. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.

c. Seleccione ***site*** > ***Storage Node*** > **LDR** > **Storage**.

d. Seleccione la ficha **Configuración** y, a continuación, la ficha **Principal**.

e. Si la lista desplegable **Estado de almacenamiento - deseado** está establecida en sólo lectura o sin conexión, seleccione **en línea**.

f. Seleccione **aplicar cambios**.

7. Para ver los nuevos almacenes de objetos:

a. Seleccione **NODES** > ***site*** > ***Storage Node*** > **Storage**.

b. Consulte los detalles en la tabla **almacenes de objetos**.

Resultado

Es posible usar la capacidad ampliada de los nodos de almacenamiento para guardar los datos de objetos.

Linux: Añada volúmenes SAN o de conexión directa al nodo de almacenamiento

Si un nodo de almacenamiento incluye menos de 16 volúmenes de almacenamiento, puede aumentar su capacidad mediante la adición de nuevos dispositivos de almacenamiento en bloques, haciéndolos visibles para los hosts Linux y la adición de las nuevas asignaciones de dispositivos de bloque al archivo de configuración de StorageGRID que se utiliza para el nodo de almacenamiento.

Antes de empezar

- Tiene acceso a las instrucciones de instalación de StorageGRID para su plataforma Linux.
  - "Instalar StorageGRID en Red Hat Enterprise Linux"
  - "Instalar StorageGRID en Ubuntu o Debian"
- Usted tiene la `Passwords.txt` archivo.
- Ya tienes "permisos de acceso específicos".

> No intente añadir volúmenes de almacenamiento a un nodo de almacenamiento mientras haya activo una actualización de software, un procedimiento de recuperación o otro procedimiento de ampliación.

Acerca de esta tarea

El nodo de almacenamiento no está disponible durante un breve periodo de tiempo cuando se añaden volúmenes de almacenamiento. Debe realizar este procedimiento en un nodo de almacenamiento a la vez para evitar que se vean afectados los servicios de grid orientados al cliente.

Pasos

1. Instale el nuevo hardware de almacenamiento.

   Para obtener más información, consulte la documentación proporcionada por su proveedor de hardware.

2. Cree nuevos volúmenes de almacenamiento en bloques de los tamaños deseados.
   - Conecte las nuevas unidades y actualice la configuración de la controladora RAID según sea necesario, o asigne los nuevos LUN de SAN a las cabinas de almacenamiento compartido y permita que el host Linux acceda a ellas.
   - Utilice el mismo esquema de nomenclatura persistente que utilizó para los volúmenes de almacenamiento en el nodo de almacenamiento existente.
   - Si utiliza la función de migración de nodos StorageGRID, haga que los nuevos volúmenes sean visibles para otros hosts Linux que son destinos de migración para este nodo de almacenamiento. Para obtener más información, consulte las instrucciones de instalación de StorageGRID para su plataforma Linux.
3. Inicie sesión en el host Linux que admite el nodo de almacenamiento como raíz o con una cuenta que tenga permiso sudo.
4. Confirmar que los volúmenes de almacenamiento nuevos estén visibles en el host Linux.

   Es posible que tenga que volver a analizar los dispositivos.

5. Ejecute el siguiente comando para deshabilitar temporalmente el nodo de almacenamiento:

   ```
   sudo storagegrid node stop <node-name>
   ```

6. Mediante un editor de texto como vim o pico, edite el archivo de configuración del nodo para el nodo de almacenamiento, que puede encontrarse en `/etc/storagegrid/nodes/<node-name>.conf`.
7. Busque la sección del archivo de configuración del nodo que contiene las asignaciones de dispositivos del bloque de almacenamiento de objetos existentes.

   En el ejemplo: `BLOCK_DEVICE_RANGEDB_00` para `BLOCK_DEVICE_RANGEDB_03` son las asignaciones de dispositivos de bloques de almacenamiento de objetos existentes.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

8. Añada nuevas asignaciones de dispositivo de bloque de almacenamiento de objetos que correspondan a los volúmenes de almacenamiento en bloque que añadió para este nodo de almacenamiento.

   Asegúrese de comenzar en el siguiente `BLOCK_DEVICE_RANGEDB_nn`. No deje un hueco.

   - En función del ejemplo anterior, comience en `BLOCK_DEVICE_RANGEDB_04`.
   - En el ejemplo siguiente, se añadieron cuatro volúmenes de almacenamiento basado en bloques al nodo: `BLOCK_DEVICE_RANGEDB_04` para `BLOCK_DEVICE_RANGEDB_07`.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. Ejecute el siguiente comando para validar los cambios en el archivo de configuración del nodo para el nodo de almacenamiento:

   `sudo storagegrid node validate <node-name>`

   Solucione todos los errores o advertencias antes de continuar con el siguiente paso.

   Si observa un error similar al siguiente, significa que el archivo de configuración del nodo está intentando asignar el dispositivo de bloque utilizado por `<node-name>` para `<PURPOSE>` a la dada `<path-name>` En el sistema de archivos Linux, pero no hay un archivo especial de dispositivo de bloque válido (o softlink a un archivo especial de dispositivo de bloque) en esa ubicación.

   ```
   Checking configuration file for node <node-name>…
   ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
   <path-name> is not a valid block device
   ```

   Compruebe que ha introducido el valor correcto `<path-name>`.

10. Ejecute el siguiente comando para reiniciar el nodo con las nuevas asignaciones de dispositivo de bloque en su lugar:

    `sudo storagegrid node start <node-name>`

11. Inicie sesión en el nodo de almacenamiento como administrador con la contraseña que aparece en `Passwords.txt` archivo.
12. Compruebe que los servicios se inician correctamente:
    a. Ver una lista del estado de todos los servicios del servidor:

```
sudo storagegrid-status
```

El estado se actualiza automáticamente.

b. Espere a que todos los servicios se ejecuten o se verifiquen.

c. Salir de la pantalla de estado:

```
Ctrl+C
```

13. Configure el nuevo almacenamiento para que lo utilice el nodo de almacenamiento:

a. Configure los nuevos volúmenes de almacenamiento:

```
sudo add_rangedbs.rb
```

Este script encuentra todos los volúmenes de almacenamiento nuevos y solicita que se los formatee.

b. Introduzca **y** para formatear los volúmenes de almacenamiento.

c. Si alguno de los volúmenes se ha formateado anteriormente, decida si desea reformatearlos.

- Introduzca **y** para cambiar el formato.
- Introduzca **n** para omitir el formateo.

La `setup_rangedbs.sh` el script se ejecuta automáticamente.

14. Compruebe que el nodo de almacenamiento esté en línea:

a. Inicie sesión en Grid Manager mediante una "navegador web compatible".

b. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.

c. Seleccione ***site*** > ***Storage Node*** > **LDR** > **Storage**.

d. Seleccione la ficha **Configuración** y, a continuación, la ficha **Principal**.

e. Si la lista desplegable **Estado de almacenamiento - deseado** está establecida en sólo lectura o sin conexión, seleccione **en línea**.

f. Haga clic en **aplicar cambios**.

15. Para ver los nuevos almacenes de objetos:

a. Seleccione **NODES** > ***site*** > ***Storage Node*** > **Storage**.

b. Consulte los detalles en la tabla **almacenes de objetos**.

Resultado

Ahora se puede usar la capacidad ampliada de los nodos de almacenamiento para guardar datos de objetos.

Añada nodos de grid o sitio

Añada nodos de grid a un sitio existente o añada otro nuevo

Siga este procedimiento para agregar nodos de cuadrícula a sitios existentes o para agregar un sitio nuevo. Solo puede ejecutar un tipo de expansión a la vez.

Antes de empezar

- Usted tiene la "Acceso raíz o permiso de mantenimiento".
- Todos los nodos existentes del grid están activos y se ejecutan en todos los sitios.
- Se completan todos los procedimientos anteriores de ampliación, actualización, decomisionado o recuperación.

> Se le impide iniciar una expansión mientras otro procedimiento de expansión, actualización, recuperación o retirada activa está en curso. Sin embargo, si es necesario, puede pausar un procedimiento de retirada para iniciar una expansión.

Pasos

1. "Actualice las subredes de la red de cuadrícula".
2. "Implemente nuevos nodos de grid".
3. "Realizar la expansión".

Actualice las subredes de la red de cuadrícula

Al agregar nodos de cuadrícula o un sitio nuevo en una expansión, es posible que deba actualizar o agregar subredes a la red de cuadrícula.

StorageGRID mantiene una lista de las subredes de red que se utilizan para comunicarse entre los nodos de grid en la red de cuadrícula (eth0). Estas entradas incluyen las subredes utilizadas para la red de cuadrícula por cada sitio del sistema StorageGRID, así como las subredes utilizadas para NTP, DNS, LDAP u otros servidores externos a los que se acceda a través de la puerta de enlace de red de cuadrícula.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento.
- Tiene las direcciones de red, en notación CIDR, de las subredes que desea configurar.

Acerca de esta tarea

Si alguno de los nodos nuevos tiene una dirección IP de red de cuadrícula en una subred no utilizada anteriormente, debe agregar la nueva subred a la lista de subredes de red de cuadrícula antes de iniciar la expansión. De lo contrario, tendrá que cancelar la expansión, agregar la nueva subred e iniciar el procedimiento de nuevo.

Pasos

1. Seleccione **MANTENIMIENTO** > **Red** > **Red de red**.
2. Seleccione **Agregar otra subred** para agregar una nueva subred en la notación CIDR.

   Por ejemplo, introduzca `10.96.104.0/22`.

3. Introduzca la contraseña de aprovisionamiento y seleccione **Guardar**.
4. Espere hasta que se apliquen los cambios y, a continuación, descargue un nuevo paquete de recuperación.
   a. Seleccione **MANTENIMIENTO** > **sistema** > **paquete de recuperación**.

b. Introduzca la **frase de paso de aprovisionamiento**.

> El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID. También se utiliza para recuperar el nodo de administración principal.

Las subredes que ha especificado se configuran automáticamente para el sistema StorageGRID.

Implemente nuevos nodos de grid

Los pasos para implementar nuevos nodos de grid en una expansión son los mismos que los pasos que se usaron al instalar la cuadrícula por primera vez. Debe implementar todos los nodos de grid nuevos antes de ejecutar la ampliación.

Al expandir una cuadrícula, los nodos que añada no tienen que coincidir con los tipos de nodos existentes. Puede añadir nodos VMware, nodos basados en contenedores Linux o nodos de dispositivos.

VMware: Implemente nodos de grid

Debe implementar una máquina virtual en VMware vSphere para cada nodo de VMware que desee añadir a la ampliación.

Pasos

1. "Ponga en marcha el nuevo nodo como máquina virtual" Y conéctalo a una o más redes StorageGRID.

   Al poner en marcha el nodo, tiene la opción de reasignar puertos de nodo o aumentar las opciones de CPU o memoria.

2. Después de poner en marcha todos los nodos VMware nuevos, "realice el procedimiento de expansión".

Linux: Implemente nodos de grid

Puede implementar nodos de grid en hosts Linux nuevos o en hosts Linux existentes. Si necesita hosts Linux adicionales para admitir los requisitos de CPU, RAM y almacenamiento de los nodos StorageGRID que desea añadir a la cuadrícula, debe prepararlos de la misma manera que preparó los hosts cuando los instaló por primera vez. A continuación, se deben implementar los nodos de expansión del mismo modo que se pusieron en marcha los nodos de grid durante la instalación.

Antes de empezar

- Tiene las instrucciones de instalación de StorageGRID para su versión de Linux y ha revisado los requisitos de hardware y almacenamiento.
  - "Instalar StorageGRID en Red Hat Enterprise Linux"
  - "Instalar StorageGRID en Ubuntu o Debian"
- Si tiene pensado implementar nuevos nodos de grid en hosts existentes, debe confirmar que los hosts existentes tienen suficiente capacidad de CPU, RAM y almacenamiento para los nodos adicionales.
- Tiene pensado minimizar los dominios de fallos. Por ejemplo, no debe implementar todos los nodos de puerta de enlace en un solo host físico.

En una puesta en marcha de producción, no ejecute más de un nodo de almacenamiento en un solo host físico o virtual. El uso de un host dedicado para cada nodo de almacenamiento proporciona un dominio de fallo aislado.

- Si el nodo StorageGRID utiliza almacenamiento asignado de un sistema NetApp ONTAP, confirme que el volumen no tiene una política de organización en niveles de FabricPool habilitada. Al deshabilitar el almacenamiento en niveles de FabricPool para los volúmenes que se usan con los nodos StorageGRID, se simplifica la solución de problemas y las operaciones de almacenamiento.

Pasos

1. Si va a añadir hosts nuevos, acceda a las instrucciones de instalación para implementar nodos StorageGRID.
2. Para implementar los hosts nuevos, siga las instrucciones para preparar los hosts.
3. Para crear archivos de configuración del nodo y validar la configuración de StorageGRID, siga las instrucciones para implementar los nodos de grid.
4. Si va a añadir nodos a un nuevo host Linux, inicie el servicio de host StorageGRID.
5. Si va a añadir nodos a un host Linux existente, inicie los nodos nuevos con la CLI del servicio de host StorageGRID:`sudo storagegrid node start [<node name\>]`

Después de terminar

Después de implementar todos los nodos de grid nuevos, puede "realice la expansión".

Dispositivos: Implementación de nodos de administrador de almacenamiento, puerta de enlace o que no sean primarios

Para instalar el software StorageGRID en un nodo de dispositivo, use el instalador de dispositivos StorageGRID, que está incluido en el dispositivo. En una ampliación, cada dispositivo de almacenamiento funciona como un único nodo de almacenamiento, y cada dispositivo de servicios funciona como un único nodo de puerta de enlace o un nodo de administración que no es el principal. Cualquier dispositivo puede conectarse a la red de grid, a la red de administración y a la red de cliente.

Antes de empezar

- El dispositivo se ha instalado en un rack o armario, conectado a las redes y encendido.
- Completó la "Configure el hardware" pasos.

  La configuración del hardware del dispositivo incluye los pasos necesarios para configurar conexiones StorageGRID (enlaces de red y direcciones IP), así como los pasos opcionales para habilitar el cifrado de nodos, cambiar el modo RAID y reasignar los puertos de red.

- Todas las subredes de red de cuadrícula que aparecen en la página Configuración de IP del instalador de dispositivos StorageGRID se definieron en la lista de subredes de redes de cuadrícula del nodo de administración principal.
- El firmware del instalador de dispositivos StorageGRID del dispositivo de reemplazo es compatible con la versión de software de StorageGRID que se ejecuta actualmente en el grid. Si las versiones no son compatibles, debe actualizar el firmware del instalador de dispositivos StorageGRID.
- Tiene un ordenador portátil de servicio con un "navegador web compatible".
- Conoce una de las direcciones IP asignadas a la controladora de computación del dispositivo. Puede usar la dirección IP para cualquier red StorageGRID conectada.

Acerca de esta tarea

El proceso de instalación de StorageGRID en un nodo de dispositivo tiene las siguientes fases:

- Especifique o confirme la dirección IP del nodo de administración principal y el nombre del nodo de dispositivo.
- Inicia la instalación y espera a que los volúmenes estén configurados y el software esté instalado.

  Durante las tareas de instalación del dispositivo, la instalación se detiene. Para reanudar la instalación, inicia sesión en el Gestor de grid, aprueba todos los nodos de cuadrícula y completa el proceso de instalación de StorageGRID.

> Si necesita implementar varios nodos de dispositivos a la vez, puede automatizar el proceso de instalación mediante el `configure-sga.py` Script de instalación del dispositivo.

Pasos

1. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.

   `https://Controller_IP:8443`

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. En la sección de conexión **nodo de administración principal**, determine si necesita especificar la dirección IP para el nodo de administración principal.

   Si ha instalado anteriormente otros nodos en este centro de datos, el instalador de dispositivos de StorageGRID puede detectar esta dirección IP automáticamente, suponiendo que el nodo de administración principal o, al menos, otro nodo de grid con una configuración ADMIN_IP, esté presente en la misma subred.

3. Si no se muestra esta dirección IP o es necesario modificarla, especifique la dirección:

Opción	Descripción
Entrada IP manual	a. Desactive la casilla de verificación **Enable Admin Node discovery**. b. Introduzca la dirección IP de forma manual. c. Haga clic en **Guardar**. d. Espere a que el estado de la conexión para que la nueva dirección IP se prepare.

Opción	Descripción
Detección automática de todos los nodos principales de administración conectados	a. Seleccione la casilla de verificación **Enable Admin Node discovery**. b. Espere a que se muestre la lista de direcciones IP detectadas. c. Seleccione el nodo de administrador principal para la cuadrícula en la que se pondrá en marcha este nodo de almacenamiento del dispositivo. d. Haga clic en **Guardar**. e. Espere a que el estado de la conexión para que la nueva dirección IP se prepare.

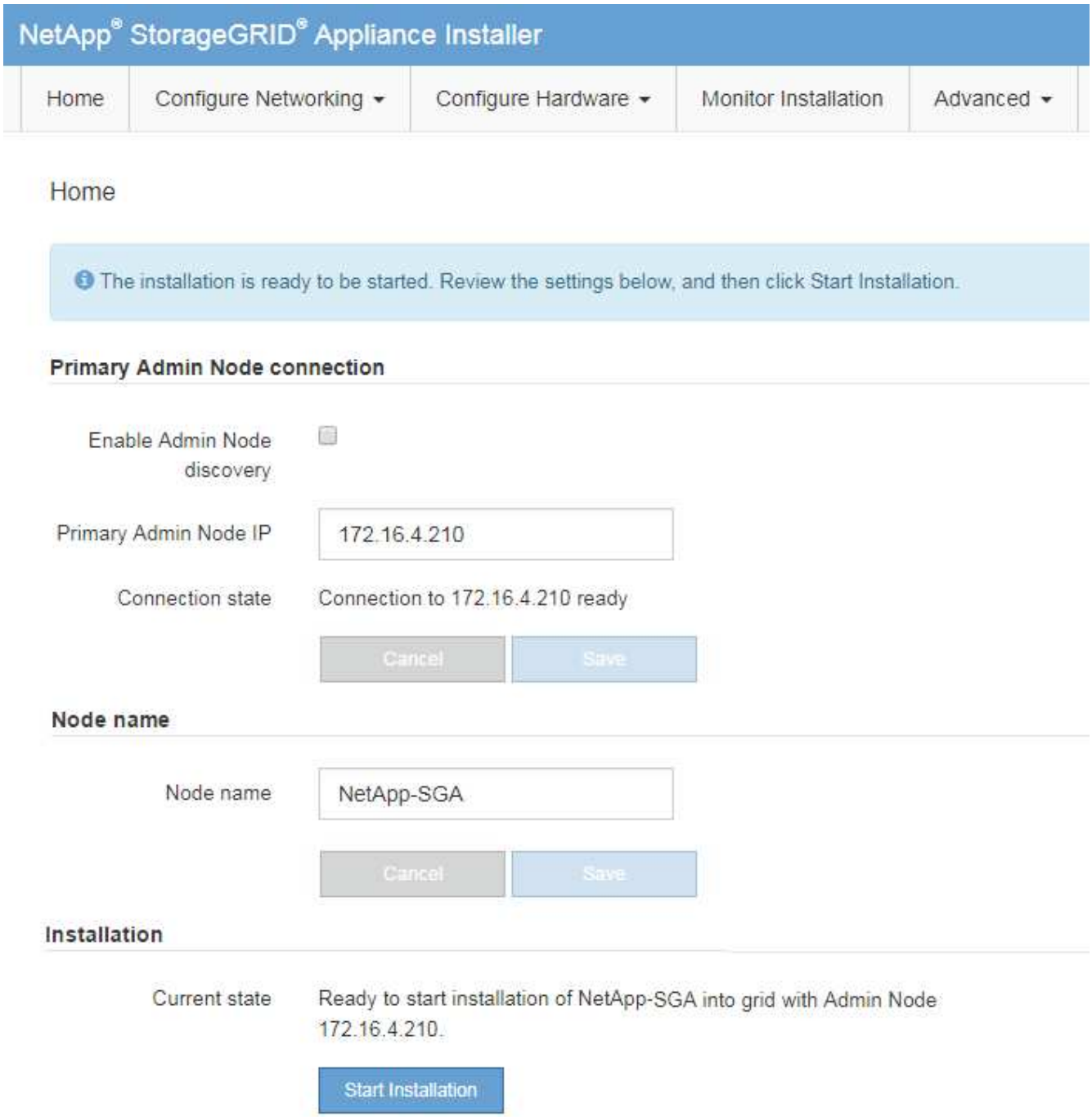
4. En el campo **Nombre de nodo**, introduzca el nombre que desea utilizar para este nodo de dispositivo y seleccione **Guardar**.

   El nombre del nodo está asignado a este nodo del dispositivo en el sistema StorageGRID. Se muestra en la página Nodes (ficha Overview) de Grid Manager. Si es necesario, puede cambiar el nombre cuando apruebe el nodo.

5. En la sección **Installation**, confirme que el estado actual es “Listo para iniciar la instalación de *node name* en la cuadrícula con el nodo de administración principal *admin_ip*” y que el botón **Start Installation** está habilitado.

   Si el botón **Iniciar instalación** no está activado, es posible que deba cambiar la configuración de red o la configuración del puerto. Para obtener instrucciones, consulte las instrucciones de mantenimiento de su aparato.

6. En la página de inicio del instalador de dispositivos StorageGRID, seleccione **Iniciar instalación**.



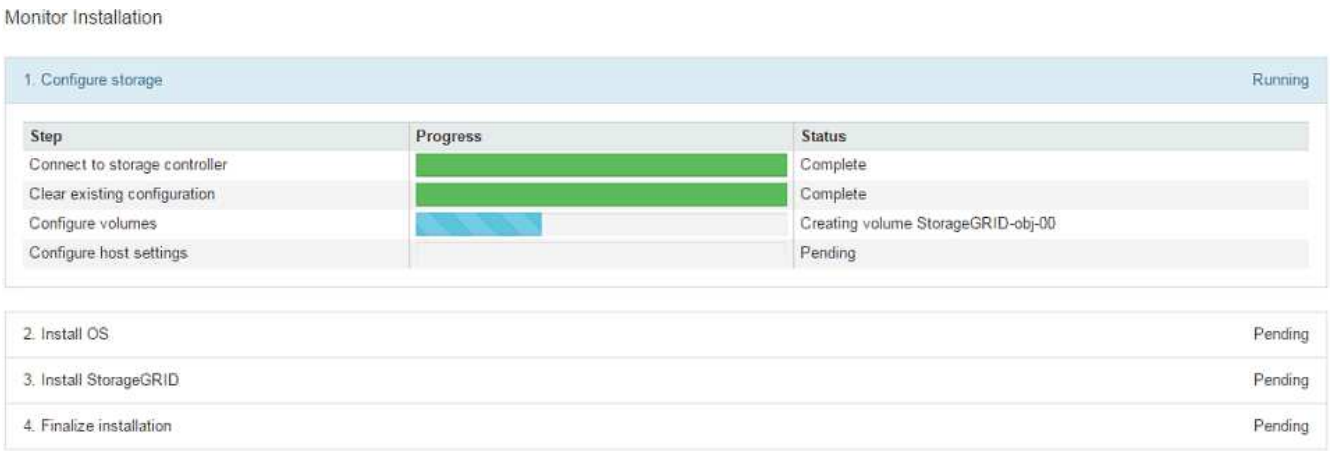
El estado actual cambia a «Instalación en curso» y se muestra la página de instalación del monitor.

7. Si su ampliación incluye varios nodos de dispositivos, repita los pasos anteriores para cada dispositivo.

> Si necesita implementar varios nodos de almacenamiento de dispositivos a la vez, puede automatizar el proceso de instalación utilizando el script de instalación de dispositivos configure-sga.py.

8. Si necesita acceder manualmente a la página instalación del monitor, seleccione **instalación del monitor** en la barra de menús.

   La página Monitor Installation (instalación del monitor) muestra el progreso de la instalación.



La barra de estado azul indica qué tarea está en curso actualmente. Las barras de estado verdes indican tareas que se han completado correctamente.

> Installer garantiza que las tareas completadas en una instalación anterior no se vuelvan a ejecutar. Si vuelve a ejecutar una instalación, las tareas que no necesitan volver a ejecutarse se muestran con una barra de estado verde y el estado “Omitida”.

9. Revise el progreso de las dos primeras etapas de instalación.

   1. Configurar el dispositivo

   Durante esta fase, ocurre uno de los siguientes procesos:

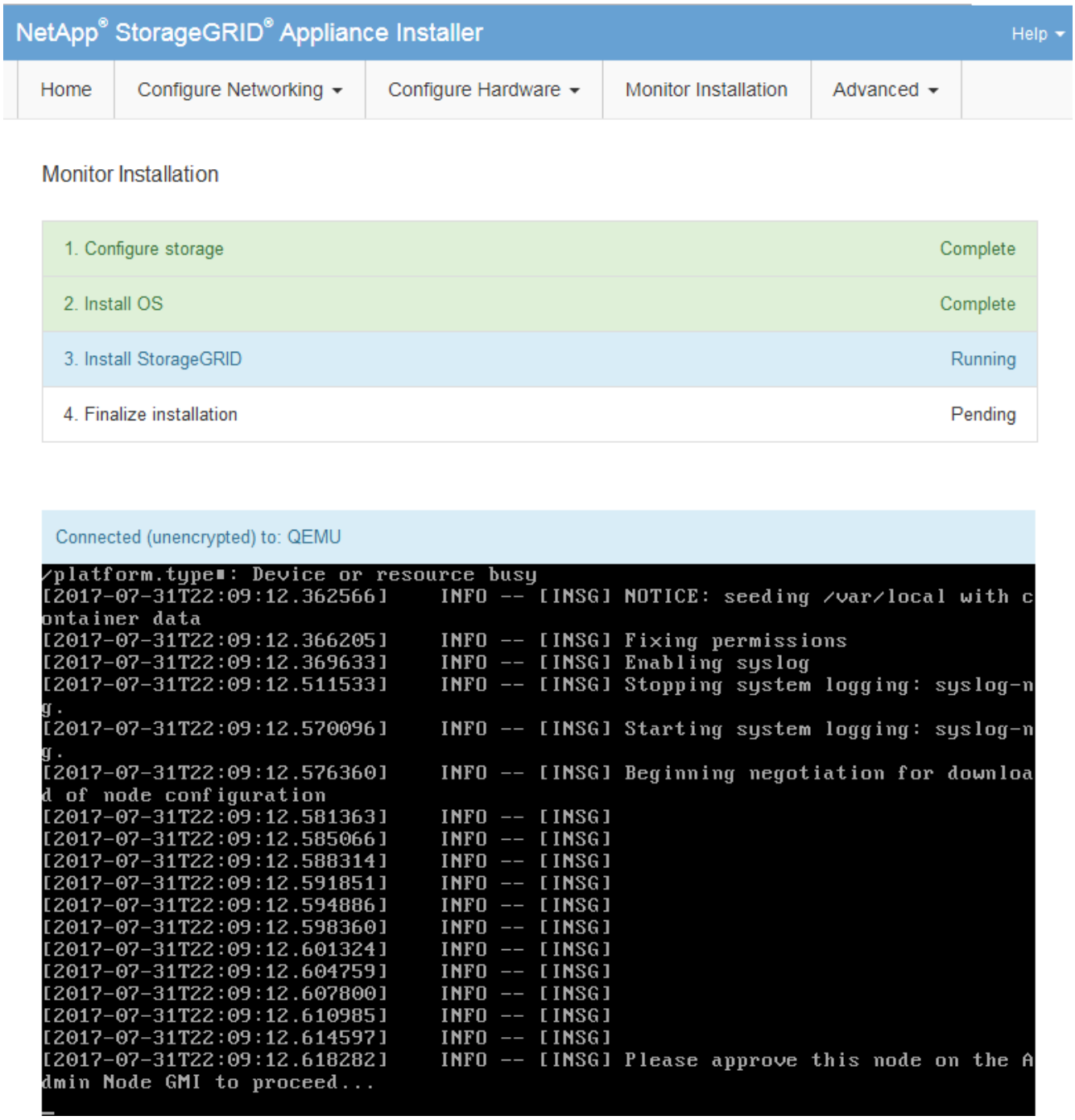
   - Para un dispositivo de almacenamiento, el instalador se conecta a la controladora de almacenamiento, borra cualquier configuración existente, se comunica con el sistema operativo SANtricity para configurar los volúmenes y configura los ajustes del host.
   - En un dispositivo de servicios, el instalador borra toda la configuración existente de las unidades en la controladora de computación y configura la configuración del host.

   2. Instalar OS

   Durante esta fase, el instalador copia la imagen del sistema operativo base para StorageGRID en el dispositivo.

10. Continúe supervisando el progreso de la instalación hasta que aparezca un mensaje en la ventana de la consola, pidiéndole que utilice el Administrador de cuadrícula para aprobar el nodo.

> Espere a que todos los nodos agregados en esta expansión estén listos para su aprobación antes de ir a Grid Manager para aprobar los nodos.



Realizar la expansión

Cuando se realiza la ampliación, los nuevos nodos de grid se añaden a la puesta en marcha de StorageGRID existente.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene la clave de acceso de aprovisionamiento.
- Se han implementado todos los nodos de grid que se están añadiendo en esta ampliación.
- Usted tiene la "Permiso de mantenimiento o acceso raíz".

- Si añade nodos de almacenamiento, confirma que se han completado todas las operaciones de reparación de datos realizadas como parte de una recuperación. Consulte "Compruebe los trabajos de reparación de datos".
- Si va a añadir nodos de almacenamiento y desea asignar un grado de almacenamiento personalizado a esos nodos, ya tiene "se ha creado el grado de almacenamiento personalizado". También tiene el permiso de acceso raíz o los permisos de mantenimiento y de ILM.
- Si va a añadir un sitio nuevo, ha revisado y actualizado las reglas de ILM. Debe asegurarse de que las copias de los objetos no se almacenen en el sitio nuevo hasta que se complete la expansión. Por ejemplo, si una regla utiliza el pool de almacenamiento predeterminado (**Todos los nodos de almacenamiento**), debe hacerlo "cree un nuevo pool de almacenamiento" Que solo contiene los nodos de almacenamiento existentes y. "Actualice las reglas de ILM" Y la política de ILM para utilizar el nuevo pool de almacenamiento. De lo contrario, los objetos se copiarán en el sitio nuevo tan pronto como el primer nodo de ese sitio se active.

Acerca de esta tarea

La expansión incluye las siguientes tareas principales de usuario:

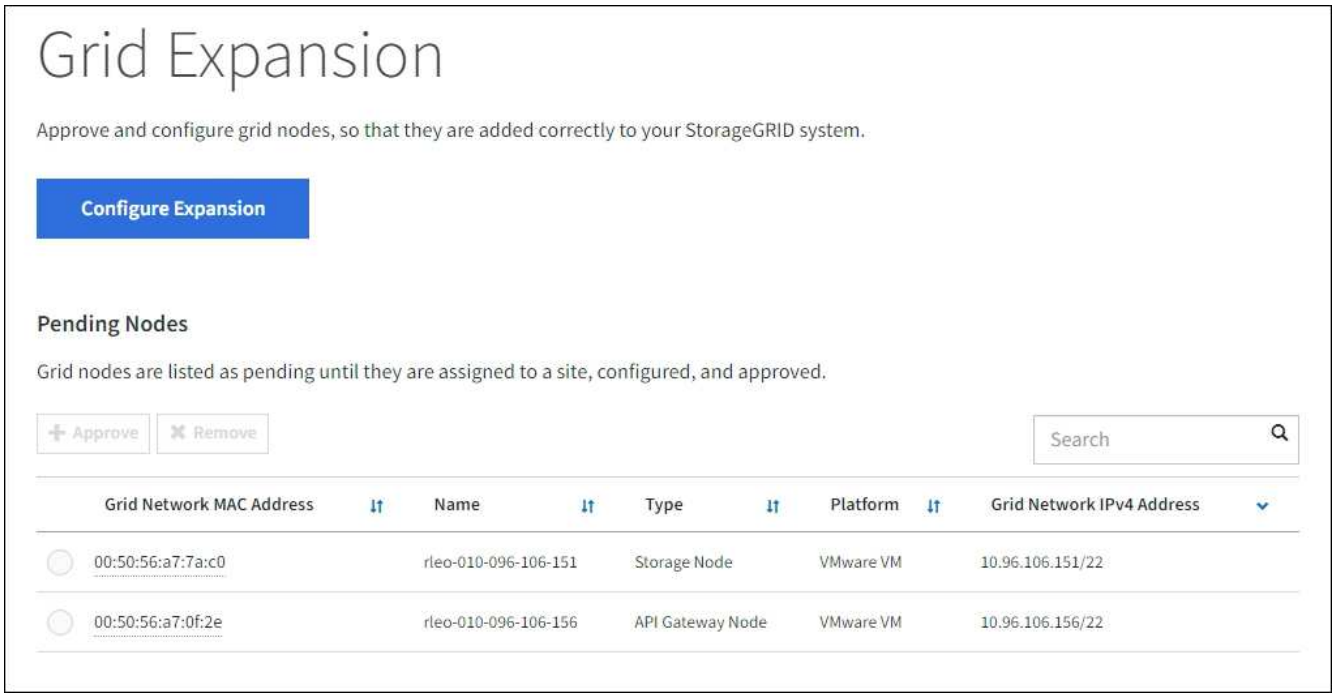
1. Configure la expansión.
2. Inicie la expansión.
3. Descargue un nuevo archivo de Recovery Package.
4. Supervise los pasos y etapas de expansión hasta que todos los nodos nuevos estén instalados y configurados y todos los servicios se hayan iniciado.

> Algunos pasos y etapas de expansión pueden tardar una cantidad significativa de tiempo en ejecutarse en una cuadrícula grande. Por ejemplo, la transmisión de Cassandra a un nuevo nodo de almacenamiento podría tardar solo unos minutos si la base de datos de Cassandra está vacía. Sin embargo, si la base de datos de Cassandra incluye una gran cantidad de metadatos de objetos, esta etapa puede tardar varias horas o más. No reinicie ningún nodo de almacenamiento durante las etapas de «Expansión del clúster de Cassandra» o «Inicio de Cassandra y transmisión de datos».

Pasos

1. Seleccione **MANTENIMIENTO** > **tareas** > **expansión**.

   Aparece la página expansión de cuadrícula. En la sección Pending Nodes, se enumeran los nodos listos para añadir.

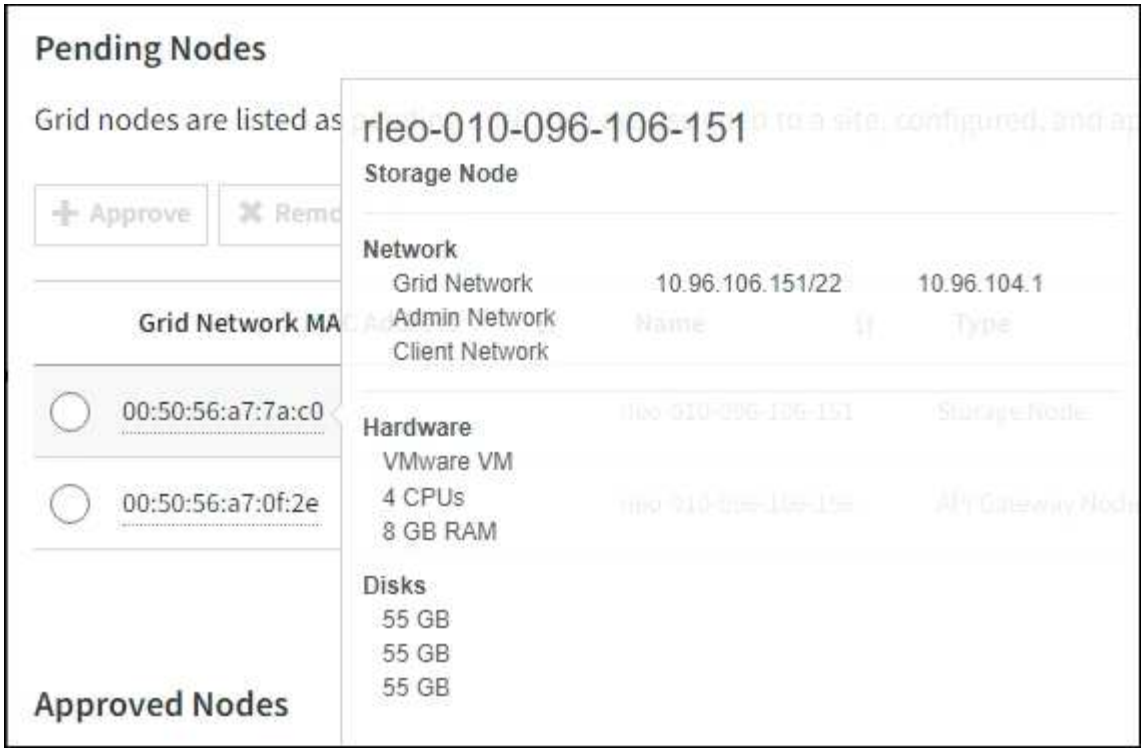


2. Seleccione **Configurar expansión**.

   Aparece el cuadro de diálogo selección de sitio.

3. Seleccione el tipo de expansión que está iniciando:
   - Si va a añadir un sitio nuevo, seleccione **Nuevo** e introduzca el nombre del sitio nuevo.
   - Si va a agregar uno o más nodos a un sitio existente, seleccione **Existente**.
4. Seleccione **Guardar**.
5. Revise la lista **nodos pendientes** y confirme que muestra todos los nodos de cuadrícula que ha implementado.

   Según sea necesario, puede colocar el cursor sobre la **Dirección MAC de red de cuadrícula** de un nodo para ver los detalles sobre ese nodo.



Si falta un nodo, confirme que se ha implementado correctamente.

6. En la lista de nodos pendientes, apruebe los nodos que desea añadir en esta expansión.
   a. Seleccione el botón de opción situado junto al primer nodo de cuadrícula pendiente que desee aprobar.
   b. Seleccione **aprobar**.

      Aparece el formulario de configuración del nodo de cuadrícula.

   c. Según sea necesario, modifique los ajustes generales:

Campo	Descripción
Sitio	Nombre de la ubicación a la que se asociará el nodo de cuadrícula. Si va a añadir varios nodos, asegúrese de seleccionar el sitio correcto para cada nodo. Si va a añadir un sitio nuevo, todos los nodos se añadirán al sitio nuevo.
Nombre	El nombre del sistema para el nodo. Los nombres del sistema son necesarios para las operaciones internas de StorageGRID y no se pueden cambiar.

Campo	Descripción
Rol de NTP	El rol de protocolo de tiempo de red (NTP) del nodo de grid: • Seleccione **Automático** (predeterminado) para asignar automáticamente el rol NTP al nodo. El rol primario se asignará a los nodos de administración, los nodos de almacenamiento con servicios ADC, los nodos de puerta de enlace y cualquier nodo de cuadrícula que tenga direcciones IP no estáticas. El rol de cliente se asignará a todos los demás nodos de grid. • Seleccione **Primario** para asignar manualmente el rol NTP principal al nodo. Al menos dos nodos en cada sitio deben tener el rol principal para proporcionar acceso redundante al sistema a orígenes de tiempo externos. • Seleccione **Client** para asignar manualmente el rol NTP del cliente al nodo.
Servicio ADC (solo nodos de almacenamiento)	Si este nodo de almacenamiento ejecutará el servicio de controlador de dominio administrativo (ADC). El servicio ADC realiza un seguimiento de la ubicación y disponibilidad de los servicios de red. Al menos tres nodos de almacenamiento en cada sitio deben incluir el servicio ADC. No puede agregar el servicio ADC a un nodo después de que se haya desplegado. • Seleccione **Sí** si el nodo de almacenamiento que va a reemplazar incluye el servicio ADC. Debido a que no puede retirar un nodo de almacenamiento si quedan muy pocos servicios ADC, esto garantiza que un nuevo servicio ADC esté disponible antes de eliminar el servicio antiguo. • Seleccione **Automático** para que el sistema determine si este nodo requiere el servicio ADC. Obtenga más información sobre "Quórum ADC".
Grado de almacenamiento (solo nodos de almacenamiento)	Utilice el grado de almacenamiento **default**, o seleccione el grado de almacenamiento personalizado que desea asignar a este nuevo nodo. Los pools de almacenamiento usan los grados de almacenamiento ILM, por lo que su selección puede afectar a los objetos que se colocarán en el nodo de almacenamiento.

d. Según sea necesario, modifique los ajustes de Grid Network, Admin Network y Client Network.

- **Dirección IPv4 (CIDR)**: Dirección de red CIDR para la interfaz de red. Por ejemplo: 172.16.10.100/24

> Si descubre que los nodos tienen direcciones IP duplicadas en la red de grid mientras aprueba nodos, debe cancelar la expansión, volver a desplegar las máquinas virtuales o los dispositivos con una IP no duplicada y reiniciar la expansión.

- **Gateway**: La puerta de enlace predeterminada del nodo de red. Por ejemplo: 172.16.10.1
- **Subredes (CIDR)**: Una o varias subredes para la Red de administración.

e. Seleccione **Guardar**.

El nodo de grid aprobado se mueve a la lista de nodos aprobados.

- Para modificar las propiedades de un nodo de cuadrícula aprobado, seleccione su botón de opción y seleccione **Editar**.
- Para volver a mover un nodo de cuadrícula aprobado a la lista nodos pendientes, seleccione el botón de opción correspondiente y seleccione **Restablecer**.
- Para quitar de forma permanente un nodo de grid aprobado, apague el nodo. A continuación, seleccione el botón de radio y seleccione **Quitar**.

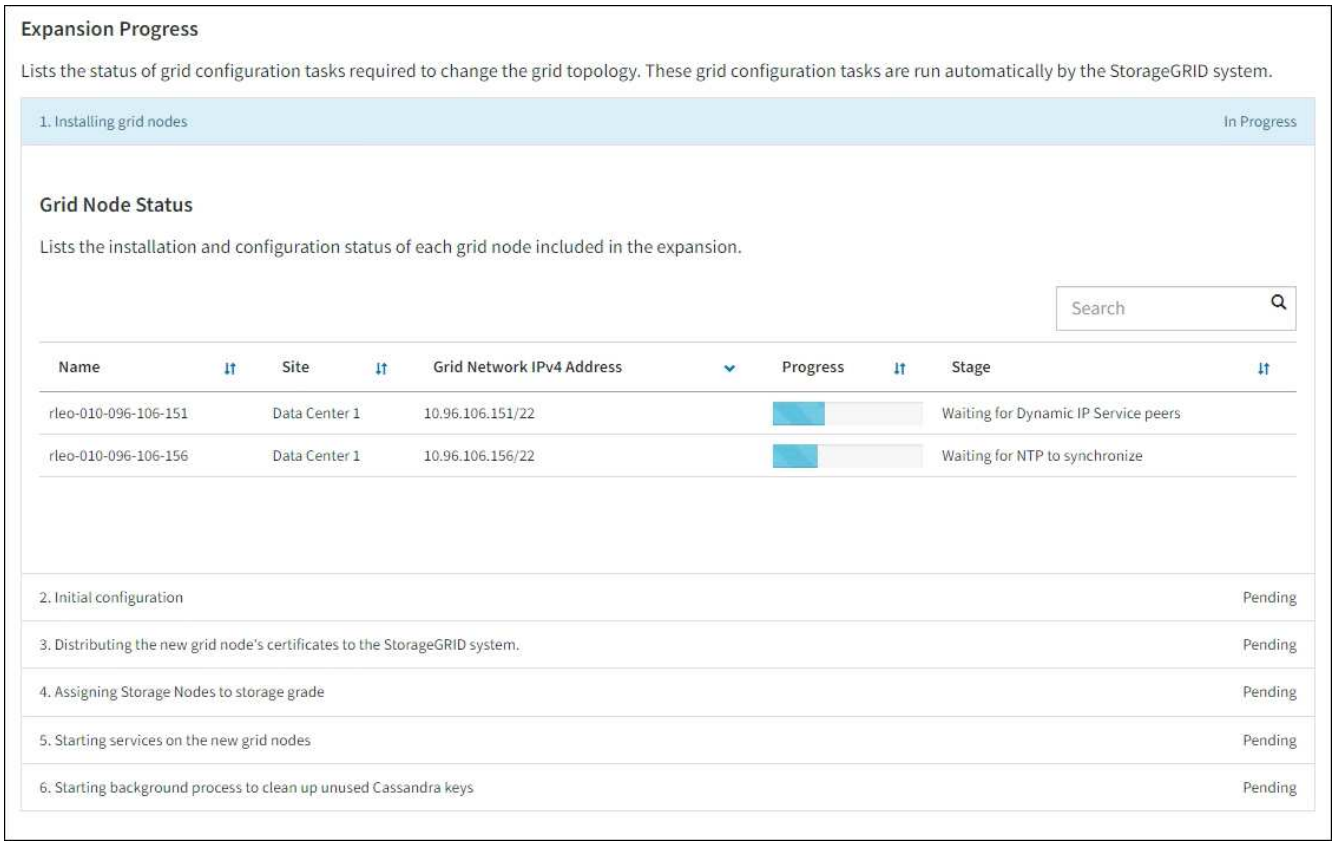
f. Repita estos pasos para cada nodo de cuadrícula pendiente que desee aprobar.

> Si es posible, debe aprobar todas las notas de cuadrícula pendientes y realizar una sola expansión. Se necesitará más tiempo si realiza varias expansiones pequeñas.

7. Cuando haya aprobado todos los nodos de cuadrícula, introduzca la **frase de paso de aprovisionamiento** y seleccione **expandir**.

Después de unos minutos, esta página se actualiza para mostrar el estado del procedimiento de expansión. Cuando las tareas que afectan a los nodos de cuadrícula individuales están en curso, la sección Estado de Nodo de Grid muestra el estado actual de cada nodo de cuadrícula.

> Durante el paso de instalación de nodos de grid para un dispositivo nuevo, el instalador de dispositivos StorageGRID muestra la instalación pasando de la fase 3 a la fase 4, Finalizar la instalación. Cuando finaliza la fase 4, se reinicia la controladora.



> Una expansión de sitio incluye una tarea adicional para configurar Cassandra para el nuevo sitio.

8. Tan pronto como aparezca el enlace **Download Recovery Package**, descargue el archivo del paquete de recuperación.

   Es necesario descargar una copia actualizada de la Lo antes posible. del archivo de paquete de recuperación después de realizar cambios en la topología de la cuadrícula en el sistema StorageGRID. El archivo de paquete de recuperación permite restaurar el sistema si se produce un fallo.

   a. Seleccione el enlace de descarga.
   b. Introduzca la frase de acceso de aprovisionamiento y seleccione **Iniciar descarga**.
   c. Cuando finalice la descarga, abra la `.zip` archive y confirme que puede acceder al contenido, incluido el `Passwords.txt` archivo.
   d. Copie el archivo del paquete de recuperación descargado (`.zip`) a dos ubicaciones seguras, seguras y separadas.

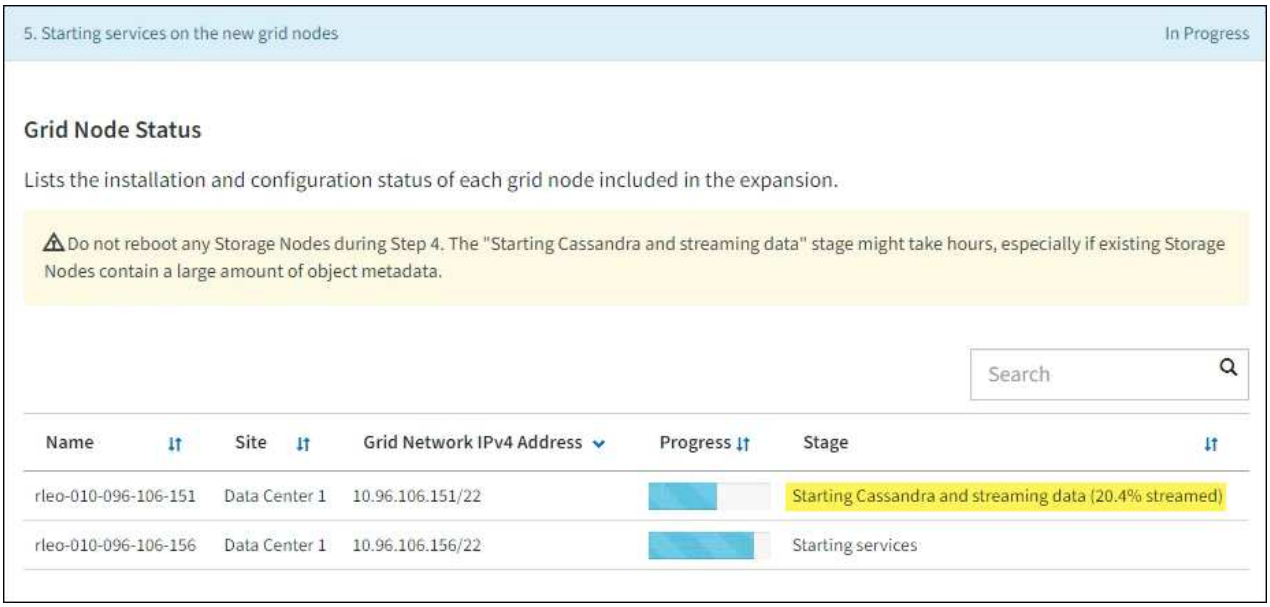
   > El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

9. Si agrega nodos de almacenamiento a un sitio existente o agrega un sitio, supervise las etapas de Cassandra, que se producen cuando se inician los servicios en los nuevos nodos de grid.

No reinicie ningún nodo de almacenamiento durante las etapas de «Expansión del clúster de Cassandra» o «Inicio de Cassandra y transmisión de datos». Estas fases pueden tardar varias horas en completarse para cada nodo de almacenamiento nuevo, especialmente si los nodos de almacenamiento existentes contienen una gran cantidad de metadatos de objetos.

Añadir nodos de almacenamiento

Si va a añadir nodos de almacenamiento a un sitio existente, revise el porcentaje que se muestra en el mensaje de estado Iniciar Cassandra y transmisión de datos.



Este porcentaje calcula lo completo que es la operación de retransmisión de Cassandra, que se basa en la cantidad total de datos de Cassandra disponibles y en la cantidad que ya se ha escrito en el nodo nuevo.

Agregando sitio

Si va a agregar un sitio nuevo, utilice `nodetool status` Para supervisar el progreso de la transmisión en secuencias de Cassandra y ver cuántos metadatos se han copiado en el sitio nuevo durante la fase de "ampliación del clúster Cassandra". La carga total de datos en el nuevo sitio debe estar dentro de aproximadamente el 20% del total de un sitio actual.

10. Continúe supervisando la expansión hasta que se hayan completado todas las tareas y vuelva a aparecer el botón **Configurar expansión**.

Después de terminar

En función de los tipos de nodos de cuadrícula que haya agregado, realice pasos adicionales de integración y configuración. Consulte "Pasos de configuración tras la ampliación".

Configure el sistema ampliado

Pasos de configuración tras la ampliación

Tras completar una ampliación, debe ejecutar los pasos de configuración e integración

adicionales.

Acerca de esta tarea

Debe completar las tareas de configuración que se indican a continuación para los nodos de cuadrícula o los sitios que está agregando en la expansión. Algunas tareas pueden ser opcionales, según las opciones seleccionadas al instalar y administrar el sistema, y cómo desee configurar los nodos y sitios agregados durante la expansión.

Pasos

1. Si agregó un sitio:
   - "Cree un pool de almacenamiento" Del sitio y de cada grado de almacenamiento seleccionado para los nuevos nodos de almacenamiento.
   - Confirme que la política de ILM cumple con los nuevos requisitos. Si se requieren cambios en las reglas, "crear nuevas reglas" y.. "Actualice la política de ILM". Si las reglas ya son correctas, "activar una nueva política" Sin cambios en las reglas para garantizar que StorageGRID use los nuevos nodos.
   - Confirme que es posible acceder a los servidores de Protocolo de tiempo de red (NTP) desde ese sitio. Consulte "Gestione servidores NTP".

     > Asegúrese de que al menos dos nodos de cada sitio puedan acceder a al menos cuatro fuentes de NTP externas. Si solo un nodo de un sitio puede acceder a los orígenes NTP, se producirán problemas de tiempo si ese nodo falla. Además, designar dos nodos por sitio como orígenes NTP primarios garantiza una sincronización precisa si un sitio está aislado del resto de la cuadrícula.

2. Si añadió uno o varios nodos de almacenamiento a un sitio existente:
   - "Ver detalles del pool de almacenamiento" Para confirmar que cada nodo que añadió se incluye en los pools de almacenamiento esperados y se utiliza en las reglas de ILM esperadas.
   - Confirme que la política de ILM cumple con los nuevos requisitos. Si se requieren cambios en las reglas, "crear nuevas reglas" y.. "Actualice la política de ILM". Si las reglas ya son correctas, "activar una nueva política" Sin cambios en las reglas para garantizar que StorageGRID use los nuevos nodos.
   - "Compruebe que el nodo de almacenamiento esté activo" y capaz de ingerir objetos.
   - Si no ha podido añadir el número recomendado de nodos de almacenamiento, reequilibre los datos con código de borrado. Consulte "Reequilibre los datos con código de borrado tras añadir nodos de almacenamiento".
3. Si agregó un nodo de puerta de enlace:
   - Si se utilizan grupos de alta disponibilidad para las conexiones de cliente, lo opcional es agregar el nodo de puerta de enlace a un grupo de alta disponibilidad. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad** para revisar la lista de grupos ha existentes y agregar el nuevo nodo. Consulte "Configuración de grupos de alta disponibilidad".
4. Si agregó un nodo de administración:
   a. Si está habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, cree una confianza de parte que confíe en el nuevo nodo de administración. No puede iniciar sesión en el nodo hasta que cree esta confianza de parte de confianza. Consulte "Configurar el inicio de sesión único".
   b. Si tiene previsto utilizar el servicio Load Balancer en los nodos de administración, puede agregar el nuevo nodo de administración a un grupo de alta disponibilidad. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad** para revisar la lista de grupos ha existentes y agregar el nuevo nodo. Consulte "Configuración de grupos de alta disponibilidad".

c. De manera opcional, copie la base de datos del nodo de administración desde el nodo de administración principal al nodo de administración de expansión si desea mantener la información de auditoría y atributo consistente en cada nodo de administración. Consulte "Copie la base de datos del nodo de administración".

d. Opcionalmente, copie la base de datos Prometheus del nodo de administración principal al nodo de administración de ampliación si desea mantener la coherencia de las métricas históricas en cada nodo de administración. Consulte "Copiar métricas de Prometheus".

e. De manera opcional, copie los registros de auditoría existentes del nodo de administración principal al nodo de administración de ampliación si desea mantener la información del registro histórico consistente en cada nodo de administración. Consulte "Copiar registros de auditoría".

5. Para comprobar si los nodos de expansión se han agregado con una red cliente que no es de confianza o si la red cliente de un nodo no es de confianza, vaya a **CONFIGURACIÓN** > **SEGURIDAD** > **CONTROL DE Firewall**.

   Si la red de cliente del nodo de expansión no es de confianza, las conexiones al nodo de la red de cliente se deben realizar mediante un extremo de equilibrador de carga. Consulte "Configurar puntos finales del equilibrador de carga" y.. "Gestionar los controles del firewall".

6. Configure el DNS.

   Si ha especificar la configuración de DNS por separado para cada nodo de grid, debe añadir una configuración de DNS personalizada por nodo para los nuevos nodos. Consulte "Modifique la configuración de DNS para un solo nodo de grid".

Para garantizar que el funcionamiento sea correcto, especifique dos o tres servidores DNS. Si especifica más de tres, es posible que solo se utilicen tres debido a las limitaciones conocidas del sistema operativo en algunas plataformas. Si tiene restricciones de enrutamiento en su entorno, puede "Personalice la lista de servidores DNS" Para nodos individuales (normalmente todos los nodos en un sitio) para usar un conjunto diferente de hasta tres servidores DNS.

Si es posible, utilice servidores DNS a los que cada sitio puede acceder localmente para asegurarse de que un sitio islandn pueda resolver los FQDN para destinos externos.

Compruebe que el nodo de almacenamiento esté activo

Después de que se complete una operación de ampliación que añade nuevos nodos de almacenamiento, el sistema StorageGRID deberá empezar automáticamente a usar los nuevos nodos de almacenamiento. Debe utilizar el sistema StorageGRID para comprobar que el nodo de almacenamiento nuevo esté activo.

Pasos

1. Inicie sesión en Grid Manager mediante una "navegador web compatible".
2. Seleccione **NODES** > ***Expansion Storage Node*** > **Storage**.
3. Coloque el cursor sobre el gráfico **Almacenamiento utilizado - Datos de objeto** para ver el valor de **Usado**, que es la cantidad del espacio total utilizable que se ha utilizado para los datos de objeto.
4. Compruebe que el valor de **utilizado** aumenta a medida que mueve el cursor a la derecha del gráfico.

Copie la base de datos del nodo de administrador

Al añadir nodos de administrador mediante un procedimiento de ampliación, otra opción es copiar la base de datos del nodo de administración principal en el nuevo nodo de administración. Copiar la base de datos le permite conservar información histórica sobre atributos, alertas y alertas.

Antes de empezar

- Completó los pasos de ampliación necesarios para añadir un nodo de administrador.
- Usted tiene la `Passwords.txt` archivo.
- Tiene la clave de acceso de aprovisionamiento.

Acerca de esta tarea

El proceso de activación del software StorageGRID crea una base de datos vacía para el servicio NMS en el nodo de administración de expansión. Cuando el servicio NMS se inicia en el nodo de administración de expansión, registra información para servidores y servicios que actualmente forman parte del sistema o que se agregan más tarde. Esta base de datos de Admin Node incluye la siguiente información:

- Historial de alertas
- Historial de alarmas
- Datos históricos de atributos, que se utilizan en los gráficos e informes de texto disponibles en la página **SUPPORT** > **Tools** > **Topología de cuadrícula**

Para garantizar que la base de datos Admin Node sea coherente entre los nodos, se puede copiar la base de datos del nodo de administración principal en el nodo de administración de expansión.

> Copiar la base de datos desde el nodo de administración principal (el nodo_____Source Admin) en un nodo de administración de expansión puede tardar hasta varias horas en completarse. Durante este período, no se puede acceder a Grid Manager.

Siga estos pasos para detener el servicio MI y el servicio API de administración tanto en el nodo de administración principal como en el nodo de administración de expansión antes de copiar la base de datos.

Pasos

1. Complete los siguientes pasos en el nodo de administración principal:
   a. Inicie sesión en el nodo de administrador:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   b. Ejecute el siguiente comando: `recover-access-points`
   c. Introduzca la clave de acceso de aprovisionamiento.
   d. Detenga EL servicio MI: `service mi stop`
   e. Detenga el servicio de la interfaz de programa de aplicaciones de gestión (API-Management): `service mgmt-api stop`

2. Complete los siguientes pasos en el nodo de administrador de ampliación:
   a. Inicie sesión en el nodo de administrador de ampliación:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   b. Detenga EL servicio MI: `service mi stop`
   c. Detenga el servicio API de gestión: `service mgmt-api stop`
   d. Añada la clave privada SSH al agente SSH. Introduzca:`ssh-add`
   e. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.
   f. Copie la base de datos del nodo de administración de origen al nodo de administración de expansión: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Cuando se le solicite, confirme que desea sobrescribir la base DE datos MI en el nodo de administración de expansión.

      La base de datos y sus datos históricos se copian en el nodo de administración de expansión. Una vez que finaliza la operación de copia, el script inicia el nodo de administración de expansión.

   h. Cuando ya no necesite un acceso sin contraseñas a otros servidores, quite la clave privada del agente SSH. Introduzca:`ssh-add -D`
3. Reinicie los servicios en el nodo de administración principal: `service servermanager start`

Copiar métricas de Prometheus

Tras añadir un nuevo nodo de administración, puede copiar de manera opcional las métricas históricas que mantiene Prometheus del nodo de administración principal al nuevo nodo de administración. Al copiar las métricas se garantiza que las métricas históricas sean consistentes entre los nodos de administrador.

Antes de empezar

- El nodo del administrador nuevo debe estar instalado y en ejecución.
- Usted tiene la `Passwords.txt` archivo.
- Tiene la clave de acceso de aprovisionamiento.

Acerca de esta tarea

Cuando se añade un nodo de administración, el proceso de instalación del software crea una nueva base de datos Prometheus. Puede mantener la coherencia de las métricas históricas entre nodos copiando la base de datos Prometheus del nodo de administración principal (el *Source Admin Node*) al nuevo nodo de administración.

> La copia de la base de datos Prometheus puede tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios se detengan en el nodo de administración de origen.

Pasos

1. Inicie sesión en el nodo de administrador de origen:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
2. Desde el nodo de administración de origen, detenga el servicio Prometheus: `service prometheus stop`
3. Complete los siguientes pasos en el nuevo nodo de administrador:
   a. Inicie sesión en el nuevo nodo de administrador:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   b. Detenga el servicio Prometheus: `service prometheus stop`
   c. Añada la clave privada SSH al agente SSH. Introduzca:`ssh-add`
   d. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.
   e. Copie la base de datos Prometheus del nodo de administración de origen en el nuevo nodo de administración: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. Cuando se le solicite, pulse **Intro** para confirmar que desea destruir la nueva base de datos Prometheus en el nuevo nodo de administración.

      La base de datos Prometheus original y sus datos históricos se copian al nuevo nodo de administración. Una vez realizada la operación de copia, el script inicia el nuevo nodo de administración. Aparece el siguiente estado:

```
Database cloned, starting services
```

   a. Cuando ya no necesite un acceso sin contraseñas a otros servidores, quite la clave privada del agente SSH. Introduzca:

```
ssh-add -D
```

4. Reinicie el servicio Prometheus en el nodo de administración de origen.

```
service prometheus start
```

Copiar registros de auditoría

Cuando agrega un nuevo nodo de administración a través de un procedimiento de expansión, su servicio AMS solo registra eventos y acciones que se producen después de que se une al sistema. Según sea necesario, se pueden copiar registros de auditoría

de un nodo de administrador instalado previamente en el nuevo nodo de administrador de ampliación de modo que este se encuentre sincronizado con el resto del sistema de StorageGRID.

Antes de empezar

- Completó los pasos de ampliación necesarios para añadir un nodo de administrador.
- Usted tiene la `Passwords.txt` archivo.

Acerca de esta tarea

Para que los mensajes de auditoría históricos estén disponibles en un nodo de administración nuevo, debe copiar los archivos de registro de auditoría manualmente desde un nodo de administración existente al nodo de administración de expansión.

> De manera predeterminada, se envía la información de auditoría al registro de auditoría en los nodos admin. Puede omitir estos pasos si se aplica alguna de las siguientes situaciones:
>
> - Se configuraron un servidor de syslog externo y registros de auditoría ahora se envían al servidor de syslog en lugar de a los nodos de administrador.
> - Ha especificado explícitamente que los mensajes de auditoría se deben guardar sólo en los nodos locales que los han generado.
>
> Consulte "Configurar los mensajes de auditoría y los destinos de registro" para obtener más detalles.

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@_primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.
2. Detenga el servicio AMS para evitar que cree un nuevo archivo: `service ams stop`
3. Navegue al directorio de exportación de auditoría:

   ```
   cd /var/local/log
   ```
4. Cambie el nombre del origen `audit.log` Archivo para asegurarse de que no sobrescribe el archivo en el nodo de administración de expansión al que está copiando:

   ```
   ls -l
   mv audit.log _new_name_.txt
   ```
5. Copie todos los archivos de registro de auditoría en la ubicación de destino en el nodo de administración de expansión:

```
scp -p * IP_address:/var/local/log
```

6. Si se le solicita la frase de acceso para `/root/.ssh/id_rsa`, Escriba la contraseña de acceso SSH para el nodo de administración principal que se muestra en `Passwords.txt` archivo.
7. Restaure el original `audit.log` archivo:

```
mv new_name.txt audit.log
```

8. Inicie el servicio AMS:

```
service ams start
```

9. Cierre la sesión en el servidor:

```
exit
```

10. Inicie sesión en el nodo de administrador de ampliación:
    a. Introduzca el siguiente comando: `ssh admin@expansion_Admin_Node_IP`
    b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
    c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
    d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

    Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.
11. Actualice la configuración del usuario y del grupo para los archivos de registro de auditoría:

```
cd /var/local/log
chown ams-user:bycast *
```

12. Cierre la sesión en el servidor:

```
exit
```

Reequilibre los datos con código de borrado tras añadir nodos de almacenamiento

Después de agregar nodos de almacenamiento, puede usar el procedimiento de reequilibrio de EC para redistribuir fragmentos con código de borrado entre los nodos de almacenamiento nuevos y existentes.

Antes de empezar

- Completó los pasos de ampliación para añadir los nuevos nodos de almacenamiento.
- Ha revisado el "consideraciones que tener en cuenta al reequilibrar los datos codificados a borrado".
- Usted entiende que los datos de objetos replicados no se moverán con este procedimiento y que el procedimiento de reequilibrio de EC no tenga en cuenta el uso de datos replicados en cada nodo de almacenamiento al determinar dónde se deben mover datos codificados con borrado.
- Usted tiene la `Passwords.txt` archivo.

Qué sucede cuando se ejecuta este procedimiento

Antes de iniciar el procedimiento, tenga en cuenta lo siguiente:

- El procedimiento de reequilibrio de EC no se iniciará si uno o más volúmenes están sin conexión (desmontados) o si están en línea (montados), pero en estado de error.
- El procedimiento de reequilibrio CE se reserva temporalmente una gran cantidad de almacenamiento. Es posible que se activen las alertas de almacenamiento, pero se resolverán cuando se complete el reequilibrio. Si no hay suficiente almacenamiento para la reserva, se producirá un error en el procedimiento de reequilibrio de la CE. Las reservas de almacenamiento se liberan cuando finaliza el procedimiento de reequilibrio de EC, tanto si el procedimiento ha fallado como si ha sido correcto.
- Si un volumen deja de estar conectado mientras el procedimiento de reequilibrio de EC está en curso, el procedimiento de reequilibrio finalizará. Cualquier fragmento de datos que ya haya movido permanecerá en sus nuevas ubicaciones y no se perderá ningún dato.

  Puede volver a ejecutar el procedimiento después de que todos los volúmenes estén nuevamente en línea.

- Cuando se ejecuta el procedimiento de reequilibrio de EC, el rendimiento de las operaciones de ILM y las operaciones del cliente S3 y Swift puede verse afectado.

  > Las operaciones de la API de S3 y Swift para cargar objetos (o piezas de objetos) pueden fallar durante el procedimiento de reequilibrio de EC si requieren más de 24 horas para completarse. Las OPERACIONES PUT DE larga duración fallarán si la regla de ILM aplicable utiliza una colocación equilibrada o estricta en la ingesta. Se informará del siguiente error: `500 Internal Server Error`.

- Durante este procedimiento, todos los nodos tienen un límite de capacidad de almacenamiento del 80 %. Los nodos que superan este límite, pero que aún se almacenan por debajo de la partición de datos de destino, se excluyen de:
  - El valor de desequilibrio del sitio
  - Cualquier condición de finalización de tareas

  > La partición de datos de destino se calcula dividiendo los datos totales de una ubicación entre el número de nodos.

- **Condiciones de finalización de trabajo**. La "Procedimiento de reequilibrio de EC" se considera completo cuando se cumple alguna de las siguientes condiciones:
  - No puede mover más datos con código de borrado.
  - Los datos de todos los nodos están dentro de una desviación del 5% de la partición de datos de destino.
  - El procedimiento ha estado en ejecución durante 30 días.

Pasos

1. Revise los detalles del almacenamiento de objetos actual para el sitio que planea reequilibrar.
   a. Selecciona **NODOS**.
   b. Seleccione el primer nodo de almacenamiento del sitio.
   c. Seleccione la ficha **almacenamiento**.
   d. Coloque el cursor sobre el gráfico Storage Used - Object Data para ver la cantidad actual de datos replicados y datos codificados de borrado en el nodo de almacenamiento.

e. Repita estos pasos para ver los otros nodos de almacenamiento del sitio.

2. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

3. Inicie el procedimiento:

   inicio de datos de balance --site «*site-name*»

   Para «*site-name*», especifique el primer sitio en el que ha agregado nuevos nodos o nodos de almacenamiento. Encierre `site-name` entre comillas.

   Se inicia el procedimiento de reequilibrio de EC y se devuelve un ID de trabajo.

4. Copie el ID del trabajo.
5. Controle el estado del procedimiento de reequilibrio de EC.
   - Para ver el estado de un único procedimiento de reequilibrio de EC:

     `rebalance-data status --job-id job-id`

     Para *`job-id`*, Especifique el código que se devolvió al iniciar el procedimiento.

   - Para ver el estado del procedimiento de reequilibrio de EC actual y de cualquier procedimiento completado anteriormente:

     `rebalance-data status`

     > Para obtener ayuda sobre el comando de reequilibrio de datos:
     >
     > `rebalance-data --help`

6. Realice pasos adicionales según el estado devuelto:
   - Si `State` es `In progress`, La operación de reequilibrio de EC todavía se está ejecutando. Deberá supervisar el procedimiento de forma periódica hasta que finalice.

     Utilice la `Site Imbalance` Valor para evaluar cómo el uso desequilibrado de los datos de código de borrado se realiza en los nodos de almacenamiento del sitio. Este valor puede ir desde 1,0 a 0, donde 0 indica que el uso de los datos con codificación de borrado está equilibrado en todos los nodos de almacenamiento del sitio.

   La tarea de reequilibrio de EC se considera completada y se detendrá cuando los datos de todos los nodos estén dentro de una desviación del 5 % de la partición de datos de destino.

   - Si `State` es `Success`, opcionalmente revisar el almacenamiento de objetos para ver los detalles

actualizados del sitio.

Los datos codificados con borrado ahora deberían tener más equilibrio entre los nodos de almacenamiento ubicados en las instalaciones.

- Si `State` es `Failure`:
  i. Confirmar que todos los nodos de almacenamiento del sitio están conectados a la cuadrícula.
  ii. Compruebe y resuelva las alertas que puedan afectar a estos nodos de almacenamiento.
  iii. Reinicie el procedimiento de reequilibrio de EC:

  ```
  rebalance-data start --job-id job-id
  ```

  iv. Ver el estado del nuevo procedimiento. Si `State` sigue quieto `Failure`, póngase en contacto con el soporte técnico.

7. Si el procedimiento de reequilibrio de EC genera demasiada carga (por ejemplo, se ven afectadas las operaciones de ingesta), detenga el procedimiento.

   ```
   rebalance-data pause --job-id job-id
   ```

8. Si necesita finalizar el procedimiento de reequilibrio de EC (por ejemplo, para poder realizar una actualización del software StorageGRID), introduzca lo siguiente:

   ```
   rebalance-data terminate --job-id job-id
   ```

   > Cuando finaliza un procedimiento de reequilibrio de EC, todos los fragmentos de datos que ya se hayan movido permanecen en sus nuevas ubicaciones. Los datos no se mueven de nuevo a la ubicación original.

9. Si utiliza la codificación de borrado en más de una instalación, ejecute este procedimiento para el resto de las ubicaciones afectadas.

Solucione los problemas de ampliación

Si encuentra errores durante el proceso de expansión de cuadrícula que no puede resolver o si falla una tarea de cuadrícula, recopile los archivos de registro y póngase en contacto con el soporte técnico.

Antes de comunicarse con el soporte técnico, recoja los archivos de registro requeridos para ayudar a la solución de problemas.

Pasos

1. Conéctese al nodo de ampliación que ha experimentado errores:

   a. Introduzca el siguiente comando:`ssh -p 8022 admin@grid_node_IP`

   > El puerto 8022 es el puerto SSH del sistema operativo base, mientras que el puerto 22 es el puerto SSH del motor del contenedor que ejecuta StorageGRID.

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

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

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

Después de iniciar sesión como root, la petición de datos cambia desde `$` para `#`.

2. Según la etapa en la que se haya alcanzado la instalación, recupere cualquiera de los siguientes registros disponibles en el nodo de grid:

Plataforma	Registros
VMware	• `/var/log/daemon.log` • `/var/log/storagegrid/daemon.log` • `/var/log/storagegrid/nodes/<node-name>.log`
Linux	• `/var/log/storagegrid/daemon.log` • `/etc/storagegrid/nodes/<node-name>.conf` (para cada nodo con fallos) • `/var/log/storagegrid/nodes/<node-name>.log` (para cada nodo con errores; es posible que no exista)

Mantener un sistema StorageGRID

Mantener su grid: Información general

Las tareas de mantenimiento de grid incluyen la retirada de un nodo o un sitio, el cambio de nombre a un grid, nodo o sitio, y el mantenimiento de redes. También puede realizar procedimientos de host y middleware y procedimientos de nodo de grid.

> En estas instrucciones, “Linux” se refiere a una implementación de Red Hat® Enterprise Linux®, Ubuntu® o Debian®. Para obtener una lista de las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Antes de empezar

- Debe conocer en gran medida el sistema StorageGRID.
- Ha revisado la topología del sistema StorageGRID y comprende la configuración de grid.
- Usted entiende que usted debe seguir todas las instrucciones exactamente y tener en cuenta todas las advertencias.
- Usted entiende que los procedimientos de mantenimiento no descritos no son compatibles o requieren un acuerdo de servicios.

Procedimientos de mantenimiento para aparatos

Para conocer los procedimientos de hardware, consulte "Instrucciones de mantenimiento para su dispositivo StorageGRID".

Descargue el paquete de recuperación

El archivo de paquete de recuperación permite restaurar el sistema StorageGRID en caso de producirse un fallo.

Antes de empezar

- Desde el nodo de administración principal, ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene la clave de acceso de aprovisionamiento.
- Ya tienes "permisos de acceso específicos".

Descargue el archivo de paquete de recuperación actual antes de realizar cambios en la topología de la cuadrícula en el sistema StorageGRID o antes de actualizar el software. A continuación, descargue una nueva copia del paquete de recuperación después de realizar cambios en la topología de la cuadrícula o después de actualizar el software.

Pasos

1. Seleccione **MANTENIMIENTO** > **sistema** > **paquete de recuperación**.
2. Ingrese la frase de contraseña de aprovisionamiento y seleccione **Iniciar descarga**.

   La descarga comienza inmediatamente.

3. Cuando finalice la descarga, abra la `.zip` archive y confirme que puede acceder al contenido, incluido el `Passwords.txt` archivo.
4. Copie el archivo del paquete de recuperación descargado (`.zip`) a dos ubicaciones seguras, seguras y separadas.

> El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

Retirada de nodos o sitio

Procedimiento de retirada: Descripción general

Puede realizar un procedimiento de retirada del servicio para quitar de forma permanente nodos de cuadrícula o de todo un sitio del sistema StorageGRID.

Para quitar un nodo de cuadrícula o un sitio, realice uno de los siguientes procedimientos de retirada:

- Realice una "retirada del nodo de grid" para quitar uno o varios nodos, que pueden estar en uno o varios sitios. Los nodos que quita pueden estar en línea y conectados al sistema StorageGRID, o bien pueden estar desconectados y desconectados.
- Realice una "retirada del sitio" para eliminar un sitio. Usted realiza un **retiro del sitio conectado** si todos los nodos están conectados a StorageGRID. Realiza un **desmantelamiento del sitio desconectado** si todos los nodos están desconectados de StorageGRID. Si el sitio contiene una combinación de nodos conectados y desconectados, debe volver a conectar todos los nodos desconectados.

> Antes de retirar un sitio desconectado, póngase en contacto con su representante de cuenta de NetApp. NetApp revisará sus requisitos antes de habilitar todos los pasos en el asistente del sitio de retirada. No debería intentar retirar un sitio desconectado si cree que podría recuperar el sitio o recuperar datos de objeto del sitio.

Nodos de retirada

Retirada de nodo de grid: Información general

Puede usar el procedimiento de retirada de nodo para quitar uno o varios nodos de cuadrícula en uno o varios sitios. No puede retirar el nodo de administración principal.

Cuándo decomisionar un nodo

Usar el procedimiento de retirada del nodo cuando se cumple alguna de las siguientes condiciones:

- Se añadió un nodo de almacenamiento más grande en una ampliación y desea quitar uno o varios nodos de almacenamiento más pequeños, al mismo tiempo que se conservan objetos.

> Si desea sustituir un aparato antiguo por otro más nuevo, tenga en cuenta "clonar el nodo del dispositivo" en lugar de añadir un nuevo dispositivo en una expansión y, a continuación, retirar el dispositivo antiguo.

- Necesita menos almacenamiento total.
- Ya no se requiere un nodo de puerta de enlace.
- Ya no se requiere un nodo administrador que no sea primario.
- El grid incluye un nodo desconectado que no se puede recuperar ni volver a conectar.
- El grid incluye un nodo de archivado.

Cómo decomisionar un nodo

Puede retirar los nodos de grid conectados o los nodos de grid desconectados.

Retirada de nodos conectados

En general, debe retirar los nodos de la cuadrícula solo cuando estén conectados al sistema StorageGRID y solo cuando todos los nodos estén en estado normal (tenga iconos verdes en las páginas **NODES** y en la página **Decomimission Nodes**).

Para ver instrucciones, consulte "Retirada de nodos de grid conectados".

Retirada de nodos desconectados

En algunos casos, es posible que necesite retirar un nodo de cuadrícula que no esté conectado actualmente a la cuadrícula (uno cuyo estado sea desconocido o administrativamente inactivo). Por ejemplo, sólo puede retirar un nodo de archivado si está desconectado.

Para ver instrucciones, consulte "Retirada de nodos de red desconectados".

Qué tener en cuenta antes de retirar un nodo

Antes de realizar cualquiera de los procedimientos, revise las consideraciones para cada tipo de nodo:

- "Consideraciones sobre el desmantelamiento del administrador, puerta de enlace o nodo de archivado"
- "Consideraciones para la retirada del nodo de almacenamiento"

Consideraciones sobre el desmantelamiento de los nodos de administración, puerta de enlace o archivo

Revise las consideraciones para retirar un nodo de administración, un nodo de gateway o un nodo de archivado.

Consideraciones para el nodo de administración

- No puede retirar el nodo de administración principal.
- No puede retirar un nodo de administración si una de sus interfaces de red forma parte de un grupo de alta disponibilidad. Primero es necesario quitar las interfaces de red del grupo de alta disponibilidad. Consulte las instrucciones para "Gestionar grupos de alta disponibilidad".
- Según sea necesario, puede cambiar de forma segura las políticas de ILM mientras decomisiona un nodo de administración.
- Si retira de servicio un nodo de administración y está habilitado el inicio de sesión único (SSO) para su sistema StorageGRID, debe recordar que debe eliminar la confianza de la parte que confía del nodo desde los Servicios de Federación de Active Directory (AD FS).
- Si utiliza "federación de grid", Asegúrese de que la dirección IP del nodo que está decomisionado no se ha especificado para una conexión de federación de grid.

- Cuando retire un nodo de administrador desconectado, perderá los registros de auditoría de ese nodo; sin embargo, estos registros también deben existir en el nodo de administración principal.

Consideraciones para el nodo de puerta de enlace

- No puede retirar un nodo de puerta de enlace si una de sus interfaces de red forma parte de un grupo de alta disponibilidad (HA). Primero es necesario quitar las interfaces de red del grupo de alta disponibilidad. Consulte las instrucciones para "Gestionar grupos de alta disponibilidad".
- Según sea necesario, puede cambiar con seguridad las políticas de ILM mientras decomisiona un nodo de puerta de enlace.
- Si utiliza "federación de grid", Asegúrese de que la dirección IP del nodo que está decomisionado no se ha especificado para una conexión de federación de grid.
- Puede retirar un nodo de puerta de enlace de forma segura mientras está desconectado.

Consideraciones para el nodo de archivado

> Compatibilidad con nodos de archivado y la opción Cloud Tiering - Simple Storage Service (S3) anticuados. La compatibilidad con los nodos de archivado se eliminará por completo en una futura versión.

- No puede retirar un nodo de archivado si aún está conectado a la cuadrícula. Para eliminar un nodo de archivado, confirme que el nodo ya no se está utilizando, que los datos se han migrado a una ubicación diferente y que el nodo está apagado. A continuación, utilice el procedimiento de decomiso para los nodos desconectados.
- Si el nodo de archivado sigue en uso, asegúrese de que la programación incluye tiempo suficiente para mover cualquier dato existente a los nodos de almacenamiento o a un pool de almacenamiento en la nube. Mover los datos desde un Nodo de archivado puede llevar varios días o semanas.

Pasos

1. Si actualmente está utilizando un nodo de archivado con la opción Cloud Tiering - Simple Storage Service (S3), "Migre sus objetos a un pool de almacenamiento en la nube".
2. Confirme que el nodo de archivado ya no está utilizando las reglas de ILM de las políticas de ILM activas.
   a. Vaya a la página **ILM** > **Pools de almacenamiento**.
   b. En la lista de pools de almacenamiento, seleccione los pools de almacenamiento que contengan sólo nodos de archivo.
   c. Seleccione la pestaña **ILM usage**.
   d. Si se muestra alguna regla de ILM, consulte la columna **Used in active policy** para determinar si el pool de almacenamiento del nodo de archivado se está utilizando en una política activa.
   e. Si se está utilizando el pool de almacenamiento, "Cree una nueva política de ILM" Que ya no utiliza el nodo de archivado.
   f. Activar la nueva política.
   g. Espere a que se muevan todos los objetos del pool de almacenamiento del nodo de archivado. Esto puede llevar varios días o semanas.
3. Una vez que esté seguro de que todos los objetos se han movido del nodo de archivado, apague el nodo.
4. Ejecute el "procedimiento de retirada para nodos desconectados".

Consideraciones para los nodos de almacenamiento

Consideraciones sobre el decomisionado de nodos de almacenamiento

Antes de decomisionar un nodo de almacenamiento, considere si puede clonar el nodo en su lugar. A continuación, si decide decomisionar el nodo, revise cómo gestiona los objetos y metadatos StorageGRID durante el procedimiento de decomisionar.

Cuándo clonar un nodo en lugar de decomisionarlo

Si desea reemplazar un nodo de almacenamiento de dispositivos antiguo por un dispositivo nuevo o más grande, considere la posibilidad de clonar el nodo del dispositivo en lugar de añadir un dispositivo nuevo en una expansión y luego retirar el dispositivo antiguo.

El clonado de nodos de dispositivos le permite reemplazar fácilmente un nodo de dispositivos existente con un dispositivo compatible en el mismo sitio de StorageGRID. El proceso de clonado transfiere todos los datos al dispositivo nuevo, pone el dispositivo nuevo en servicio y deja el dispositivo antiguo en estado previo a la instalación.

Puede clonar un nodo de dispositivo si necesita:

- Sustituya un aparato que esté llegando al final de su vida útil.
- Actualice un nodo existente para aprovechar la tecnología mejorada del dispositivo.
- Aumente la capacidad de almacenamiento Grid sin cambiar el número de nodos de almacenamiento en el sistema StorageGRID.
- Mejore la eficiencia del almacenamiento, como cambiando el modo RAID.

Consulte "Clonación de nodos del dispositivo: Información general" para obtener más detalles.

Consideraciones sobre los nodos de almacenamiento conectados

Revise las consideraciones que hay que tener en cuenta para decomisionar un nodo de almacenamiento conectado.

- No debe retirar más de 10 nodos de almacenamiento en un único procedimiento de nodo de retirada.
- En todo momento, el sistema debe incluir nodos de almacenamiento suficientes para satisfacer los requisitos operativos, incluido el "Quórum ADC" y el activo "Política de ILM". Para satisfacer esta restricción, es posible que deba añadir un nodo de almacenamiento nuevo en una operación de ampliación antes de retirar un nodo de almacenamiento existente.

  Use precaución al decomisionar nodos de almacenamiento en un grid que contenga nodos solo de metadatos basados en software. Si retira todos los nodos configurados para almacenar *both* objetos y metadatos, la capacidad de almacenar objetos se elimina de la cuadrícula. Consulte "Tipos de nodos de almacenamiento" Para obtener más información sobre nodos de almacenamiento solo de metadatos.

- Cuando elimina un nodo de almacenamiento, se transfieren grandes volúmenes de datos de objetos a través de la red. Aunque estas transferencias no deben afectar a las operaciones normales del sistema, pueden afectar a la cantidad total de ancho de banda de red que consume el sistema StorageGRID.
- Las tareas asociadas con el decomisionado de nodos de almacenamiento tienen una prioridad inferior a las tareas asociadas con las operaciones normales del sistema. Esto significa que el decomisionado no interfiere con las operaciones normales del sistema StorageGRID y no necesita programarse desde un punto de inactividad del sistema. Debido a que el desmantelamiento se realiza en segundo plano, es difícil

estimar cuánto tiempo tardará el proceso en completarse. En general, la retirada del servicio finaliza con mayor rapidez cuando el sistema está en silencio o si solo se elimina un nodo de almacenamiento al mismo tiempo.

- Es posible que demore días o semanas en retirar un nodo de almacenamiento. Planifique este procedimiento en consecuencia. Aunque el proceso de retirada del servicio está diseñado para no afectar a las operaciones del sistema, puede limitar otros procedimientos. En general, se deben realizar las actualizaciones o expansiones planificadas del sistema antes de quitar nodos de grid.
- Si necesita realizar otro procedimiento de mantenimiento mientras se están quitando nodos de almacenamiento, puede "detenga el procedimiento de decomiso" y retomarlo después de que se complete el otro procedimiento.

> El botón **Pausa** sólo se activa cuando se alcanzan las etapas de evaluación de ILM o de retirada de datos con código de borrado; sin embargo, la evaluación de ILM (migración de datos) continuará ejecutándose en segundo plano.

- No es posible ejecutar operaciones de reparación de datos en ningún nodo de grid cuando se está ejecutando una tarea de decomiso.
- No debe hacer ningún cambio en una política de ILM mientras se decomisiona un nodo de almacenamiento.
- Cuando retira un nodo de almacenamiento, es posible que se activen las siguientes alertas y alarmas, y que reciba notificaciones relacionadas por correo electrónico y SNMP:
  - **No se puede comunicar con la alerta de nodo**. Esta alerta se activa al retirar un nodo de almacenamiento que incluye el servicio ADC. La alerta se resuelve cuando finaliza la operación de retirada del servicio.
  - Alarma VSTU (Estado de verificación de objetos). Esta alarma de nivel de aviso indica que el nodo de almacenamiento entra en modo de mantenimiento durante el proceso de retirada de servicio.
  - Alarma DE CASA (estado del almacén de datos). Esta alarma de nivel principal indica que la base de datos de Cassandra está disminuyendo debido a que los servicios se han detenido.
- Para eliminar los datos de forma permanente y segura, debe borrar las unidades del nodo de almacenamiento una vez completado el procedimiento de retirada.

Consideraciones sobre los nodos de almacenamiento desconectados

Revise las consideraciones que hay que tener en cuenta para decomisionar un nodo de almacenamiento desconectado.

- Nunca decomisionar un nodo desconectado a menos que esté seguro de que no se pueda conectar o recuperar.

> No realice este procedimiento si cree que podría ser posible recuperar datos de objetos del nodo. En su lugar, póngase en contacto con el soporte técnico para determinar si es posible la recuperación del nodo.

- Cuando decomisiona un nodo de almacenamiento desconectado, StorageGRID utiliza datos de otros nodos de almacenamiento para reconstruir los datos de objeto y los metadatos que estaban en el nodo desconectado.
- Se pueden producir pérdidas de datos si decomisiona más de un nodo de almacenamiento desconectado. Es posible que el sistema no pueda reconstruir los datos si no hay suficientes copias de objetos, fragmentos codificados con borrado o metadatos de objetos disponibles. Cuando se decomisionan nodos

de almacenamiento en un grid con nodos solo de metadatos basados en software, la retirada de todos los nodos configurados para almacenar tanto objetos como metadatos elimina todo el almacenamiento de objetos del grid. Consulte "Tipos de nodos de almacenamiento" Para obtener más información sobre nodos de almacenamiento solo de metadatos.

> Si tiene más de un nodo de almacenamiento desconectado que no puede recuperar, póngase en contacto con el soporte técnico para determinar el mejor curso de acción.

- Al retirar un nodo de almacenamiento desconectado, StorageGRID inicia trabajos de reparación de datos al final del proceso de decomisionado. Estos trabajos intentan reconstruir los datos de objeto y los metadatos que se almacenaron en el nodo desconectado.
- Al retirar un nodo de almacenamiento desconectado, el procedimiento de retirada se completa con relativa rapidez. Sin embargo, los trabajos de reparación de datos pueden tardar días o semanas en ejecutarse y no son supervisados por el procedimiento de decomiso. Debe supervisar manualmente estos trabajos y reiniciarlos según sea necesario. Consulte "Compruebe los trabajos de reparación de datos".
- Si decomisiona un nodo de almacenamiento desconectado que contiene la única copia de un objeto, se perderá el objeto. Las tareas de reparación de datos solo pueden reconstruir y recuperar objetos si al menos una copia replicada o hay suficientes fragmentos codificados de borrado en los nodos de almacenamiento conectados actualmente.

¿Qué es el quórum ADC?

Es posible que no pueda retirar determinados nodos de almacenamiento en un sitio si quedan muy pocos servicios de controlador de dominio administrativo (ADC) tras el desmantelamiento.

El servicio ADC, que se encuentra en algunos nodos de almacenamiento, mantiene la información de topología de cuadrícula y proporciona servicios de configuración a la cuadrícula. El sistema StorageGRID requiere que se disponga de quórum de servicios de ADC en todas las instalaciones y en todo momento.

No puede retirar un nodo de almacenamiento si al quitar el nodo se haría que el quórum ADC ya no se cumpliera. Para cumplir con el quórum ADC durante un desmantelamiento, un mínimo de tres nodos de almacenamiento en cada sitio debe tener el servicio ADC. Si un sitio tiene más de tres nodos de almacenamiento con el servicio ADC, la sencilla mayoría de ellos deberá seguir estando disponible tras el desmantelamiento: `((0.5 * Storage Nodes with ADC) + 1)`

> Use precaución al decomisionar nodos de almacenamiento en un grid que contenga nodos solo de metadatos basados en software. Si retira todos los nodos configurados para almacenar *both* objetos y metadatos, la capacidad de almacenar objetos se elimina de la cuadrícula. Consulte "Tipos de nodos de almacenamiento" Para obtener más información sobre nodos de almacenamiento solo de metadatos.

Por ejemplo, supongamos que un sitio incluye actualmente seis nodos de almacenamiento con servicios ADC y que desea retirar tres nodos de almacenamiento. Debido al requisito de quórum de ADC, debe completar dos procedimientos de retirada, de la siguiente manera:

- En el primer procedimiento de retirada, debe asegurarse de que siguen estando disponibles cuatro nodos de almacenamiento con servicios ADC: `((0.5 * 6) + 1)`. Esto significa que solo puede decomisionar dos nodos de almacenamiento inicialmente.
- En el segundo procedimiento de retirada, puede eliminar el tercer nodo de almacenamiento porque el quórum ADC solo necesita tres servicios ADC para permanecer disponibles: `((0.5 * 4) + 1)`.

Si necesita retirar un nodo de almacenamiento pero no puede hacerlo debido a los requisitos de quórum ADC, agregue un nuevo nodo de almacenamiento en un "expansión" Y especifique que debe tener un servicio ADC. A continuación, retire el nodo de almacenamiento existente.

Revisar la configuración de almacenamiento y la política de ILM

Si tiene pensado decomisionar un nodo de almacenamiento, debe revisar la política de ILM del sistema StorageGRID antes de iniciar el proceso de decomisionado.

Durante el decomisionado, todos los datos de objetos se migran desde el nodo de almacenamiento retirado a otros nodos de almacenamiento.

> La política de ILM que tiene *durante* el decomiso será la que se utilice *after* el Decomisión. Debe asegurarse de que esta política cumple con sus requisitos de datos antes de iniciar la retirada y después de que se haya completado la retirada.

Debe revisar las reglas de cada una "Política de ILM activa" Para garantizar que el sistema StorageGRID seguirá teniendo la capacidad suficiente del tipo y en las ubicaciones correctas para acomodar el decomisionado de un nodo de almacenamiento.

Considere lo siguiente:

- ¿Será posible que los servicios de evaluación de ILM copien datos de objetos de modo que se cumplan las reglas de ILM?
- ¿Qué ocurre si un sitio deja de estar disponible temporalmente mientras se decomisiona? ¿Se pueden realizar copias adicionales en una ubicación alternativa?
- ¿Cómo afectará el proceso de retirada del servicio a la distribución final del contenido? Como se describe en "Consolide los nodos de almacenamiento", deberías "Añada nuevos nodos de almacenamiento" antes de retirar los antiguos. Si añade un nodo de almacenamiento de repuesto con mayor tamaño después de decomisionar un nodo de almacenamiento más pequeño, los nodos de almacenamiento antiguos pueden estar cerca de la capacidad y el nuevo nodo de almacenamiento podría tener prácticamente ningún contenido. La mayoría de las operaciones de escritura de datos de objetos nuevos se dirigirían entonces al nuevo nodo de almacenamiento, lo que reduciría la eficiencia general de las operaciones del sistema.
- ¿Incluirá el sistema, en todo momento, suficientes nodos de almacenamiento para satisfacer las políticas de ILM activas?

> Una política de ILM que no puede satisfacerse provocará retrasos y alertas y podría detener el funcionamiento del sistema StorageGRID.

Compruebe que la topología propuesta que se obtendrá como resultado del proceso de decomisionado cumple con la política de ILM evaluando las áreas enumeradas en la tabla.

Área a evaluar	Consideraciones a tener en cuenta
Capacidad disponible	¿Habrá suficiente capacidad de almacenamiento para acomodar todos los datos de objeto almacenados en el sistema StorageGRID, incluidas las copias permanentes de los datos de objeto actualmente almacenados en el nodo de almacenamiento que se van a retirar? ¿Habrá capacidad suficiente para manejar el crecimiento previsto de datos de objetos almacenados durante un intervalo de tiempo razonable una vez finalizado el decomisionado?
Ubicación del almacenamiento	Si queda suficiente capacidad en el sistema StorageGRID en su conjunto, ¿está la capacidad en las ubicaciones adecuadas para satisfacer las reglas empresariales del sistema StorageGRID?
Tipo de almacenamiento	¿Habrá suficiente almacenamiento del tipo apropiado después de haber finalizado el desmantelamiento? Por ejemplo, las reglas de ILM pueden mover contenido de un tipo de almacenamiento a otro a medida que envejece el contenido. En este caso, debe asegurarse de que haya disponible suficiente almacenamiento del tipo adecuado en la configuración final del sistema StorageGRID.

Consolide los nodos de almacenamiento

Es posible consolidar los nodos de almacenamiento para reducir el número de nodos de almacenamiento de un sitio o una puesta en marcha, y aumentar la capacidad de almacenamiento.

Cuando se consolidan los nodos de almacenamiento, se "Expanda el sistema StorageGRID" Al añadir nuevos nodos de almacenamiento de mayor capacidad y luego retirar los antiguos nodos de almacenamiento de menor capacidad. Durante el procedimiento de retirada del servicio, los objetos se migran de los nodos de almacenamiento antiguos a los nuevos nodos de almacenamiento.

> Si va a consolidar dispositivos antiguos y pequeños con modelos nuevos o con dispositivos de mayor capacidad, considere la opción "clonar el nodo del dispositivo" (o utilice clonado de nodos del dispositivo y el procedimiento de retirada si no está realizando un reemplazo uno a uno).

Por ejemplo, puede añadir dos nodos de almacenamiento nuevos con mayor capacidad para reemplazar tres nodos de almacenamiento anteriores. Primero, se debe usar el procedimiento de ampliación para añadir los dos nodos de almacenamiento nuevos y más grandes, y luego se debe usar el procedimiento de retirada para quitar los tres nodos de almacenamiento antiguos de menor capacidad.

Al añadir capacidad nueva antes de eliminar los nodos de almacenamiento existentes, tendrá la seguridad de una distribución de datos más equilibrada en el sistema StorageGRID. También puede reducir la posibilidad de que un nodo de almacenamiento existente pueda superar el nivel de Marca de agua de almacenamiento.

Si necesita quitar más de un nodo de almacenamiento, puede decomisionar secuencialmente o en paralelo

> Use precaución al decomisionar nodos de almacenamiento en un grid que contenga nodos solo de metadatos basados en software. Si retira todos los nodos configurados para almacenar *both* objetos y metadatos, la capacidad de almacenar objetos se elimina de la cuadrícula. Consulte "Tipos de nodos de almacenamiento" Para obtener más información sobre nodos de almacenamiento solo de metadatos.

- Si decomisiona nodos de almacenamiento secuencialmente, debe esperar a que el primer nodo de almacenamiento finalice el decomisionado antes de iniciar la retirada del siguiente nodo de almacenamiento.
- Si decomisiona nodos de almacenamiento en paralelo, los nodos de almacenamiento procesan de forma simultánea las tareas de retirada para todos los nodos de almacenamiento que se van a retirar del servicio. Esto puede dar lugar a una situación en la que todas las copias permanentes de un archivo se marcan como de solo lectura, desactivando temporalmente la eliminación en cuadrículas en las que está activada esta funcionalidad.

Compruebe los trabajos de reparación de datos

Antes de retirar un nodo de cuadrícula, debe confirmar que no hay ningún trabajo de reparación de datos activo. Si alguna reparación ha fallado, debe reiniciarla y dejar que se complete antes de realizar el procedimiento de retirada.

Acerca de esta tarea

Si necesita decomisionar un nodo de almacenamiento desconectado, también realizará estos pasos una vez que finalice el procedimiento de retirada para garantizar que el trabajo de reparación de datos se haya completado correctamente. Debe asegurarse de que todos los fragmentos codificados de borrado que estaban en el nodo eliminado se hayan restaurado correctamente.

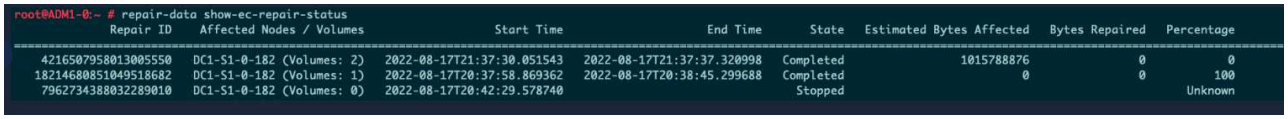
Estos pasos solo se aplican a sistemas que tienen objetos codificados de borrado.

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Compruebe si hay reparaciones en curso: `repair-data show-ec-repair-status`
   - Si nunca ha ejecutado un trabajo de reparación de datos, la salida es `No job found`. No es necesario reiniciar ningún trabajo de reparación.
   - Si el trabajo de reparación de datos se ejecutó anteriormente o se está ejecutando actualmente, la salida muestra información para la reparación. Cada reparación tiene un ID de reparación único.



Opcionalmente, puede utilizar Grid Manager para supervisar los procesos de restauración en curso y mostrar un historial de restauración. Consulte "Restaurar datos de objetos con Grid Manager".

3. Si el Estado para todas las reparaciones es `Completed`, no es necesario reiniciar ningún trabajo de reparación.
4. Si el estado para cualquier reparación es `Stopped`, debe reiniciar dicha reparación.
   a. Obtenga del resultado el ID de reparación de la reparación fallida.
   b. Ejecute el `repair-data start-ec-node-repair` comando.

      Utilice la `--repair-id` Opción para especificar el ID de reparación. Por ejemplo, si desea volver a intentar una reparación con el ID de reparación 949292, ejecute este comando: `repair-data start-ec-node-repair --repair-id 949292`

   c. Seguir realizando el seguimiento del estado de las reparaciones de datos de la CE hasta que el Estado de todas las reparaciones sea `Completed`.

Reúna los materiales necesarios

Antes de realizar un desmantelamiento de un nodo de cuadrícula, debe obtener la siguiente información.

Elemento	Notas
Paquete de recuperación `.zip` archivo	Debe "Descargue el paquete de recuperación más reciente" `.zip` archivo (`sgws-recovery-package-id-revision.zip`). Puede utilizar el archivo de paquete de recuperación para restaurar el sistema si se produce un fallo.
`Passwords.txt` archivo	Este archivo contiene las contraseñas que se necesitan para acceder a los nodos de grid en la línea de comandos y se incluye en el paquete de recuperación.
Clave de acceso de aprovisionamiento	La frase de contraseña se crea y documenta cuando se instala el sistema StorageGRID por primera vez. La clave de acceso de aprovisionamiento no está en la `Passwords.txt` archivo.
Descripción de la topología del sistema StorageGRID antes de decomisionar	Si está disponible, obtenga cualquier documentación que describa la topología actual del sistema.

Información relacionada

"Requisitos del navegador web"

Acceda a la página nodos de misión

Cuando accede a la página nodos de misión de descommisión de Grid Manager, puede ver de un vistazo qué nodos se pueden retirar del servicio.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".

> Use precaución al decomisionar nodos de almacenamiento en un grid que contenga nodos solo de metadatos basados en software. Si retira todos los nodos configurados para almacenar *both* objetos y metadatos, la capacidad de almacenar objetos se elimina de la cuadrícula. Consulte "Tipos de nodos de almacenamiento" Para obtener más información sobre nodos de almacenamiento solo de metadatos.

Pasos

1. Seleccione **MANTENIMIENTO** > **tareas** > **misión**.
2. Seleccione **nodos de misión**.

   Aparecerá la página nodos de misión. Desde esta página, puede:

   - Determine qué nodos de cuadrícula se pueden retirar del servicio actualmente.
   - Ver el estado de todos los nodos de grid
   - Ordene la lista en orden ascendente o descendente por **Nombre**, **Sitio**, **Tipo** o **tiene ADC**.
   - Introduzca los términos de búsqueda para encontrar rápidamente nodos concretos.

     En este ejemplo, la columna Decomision possible indica que puede decomisionar el nodo de puerta de enlace y uno de los cuatro nodos de almacenamiento.

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-	✓	No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC1-ARC1	Data Center 1	Archive Node	-	✓	No, you can't decommission an Archive Node unless the node is disconnected.
☐ DC1-G1	Data Center 1	API Gateway Node	-	✓	✓
DC1-S1	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S2	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S3	Data Center 1	Storage Node	Yes	✓	No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
☐ DC1-S4	Data Center 1	Storage Node	No	✓	✓

3. Revise la columna **DECOMmission possible** para cada nodo que desee retirar.

   Si un nodo de cuadrícula se puede retirar, esta columna incluye una marca de verificación verde y la columna izquierda incluye una casilla de verificación. Si un nodo no se puede retirar, esta columna describe el problema. Si hay más de una razón por la que un nodo no puede ser decomisionado, se muestra la razón más crítica.

Razón posible de retirada	Descripción	Pasos a resolver
No, *node type* decomisionado no es compatible.	No puede retirar el nodo de administración principal.	Ninguno.
No, al menos un nodo de grid está desconectado. **Nota:** este mensaje sólo se muestra para los nodos de red conectados.	No puede decomisionar un nodo de grid conectado si hay algún nodo de grid desconectado. La columna **Estado** incluye uno de estos iconos para los nodos de cuadrícula desconectados: • (Gris): Administrativamente abajo • (Azul): Desconocido	Debe volver a conectar todos los nodos desconectados o. "decomisionar todos los nodos desconectados" antes de poder quitar un nodo conectado. **Nota**: Si su red contiene varios nodos desconectados, el software requiere que los retire todos al mismo tiempo, lo que aumenta el potencial de resultados inesperados.
No, uno o más nodos necesarios están desconectados actualmente y deben recuperarse. **Nota:** este mensaje sólo se muestra para los nodos de red desconectados.	No puede retirar un nodo de grid desconectado si también se desconecta uno o más nodos necesarios (por ejemplo, un nodo de almacenamiento necesario para el quórum ADC).	a. Revise los mensajes de DECOMmission posibles para todos los nodos desconectados. b. Determine qué nodos no se pueden retirar porque son necesarios. ◦ Si el estado de un nodo requerido está administrativamente inactivo, vuelva a conectar el nodo. ◦ Si el estado de un nodo requerido es Desconocido, realice un procedimiento de recuperación de nodos para recuperar el nodo requerido.
No, miembro de los grupos de HA: *Nombre del grupo*. Antes de poder retirar este nodo, debe quitarlo de todos los grupos de alta disponibilidad.	No puede retirar un nodo de administración o un nodo de puerta de enlace si una interfaz de nodo pertenece a un grupo de alta disponibilidad (HA).	Edite el grupo de alta disponibilidad para quitar la interfaz del nodo o eliminar todo el grupo de alta disponibilidad. Consulte "Configuración de grupos de alta disponibilidad".

Razón posible de retirada	Descripción	Pasos a resolver
No, el sitio *x* requiere un mínimo de *n* nodos de almacenamiento con servicios ADC.	• Solo nodos de almacenamiento.* No puede retirar un nodo de almacenamiento si los nodos insuficientes permanecen en el sitio para admitir los requisitos del quórum ADC.	Realice una expansión. Agregue un nodo de almacenamiento nuevo al sitio y especifique que debe tener un servicio ADC. Consulte la información sobre "Quórum ADC".
No, uno o varios perfiles de código de borrado necesitan al menos *n* nodos de almacenamiento. Si el perfil no se utiliza en una regla de ILM, puede desactivarlo.	• Solo nodos de almacenamiento.* No puede retirar un nodo de almacenamiento a menos que queden suficientes nodos para los perfiles de codificación de borrado existentes. Por ejemplo, si existe un perfil de código de borrado para el código de borrado 4+2, deberá quedar al menos 6 nodos de almacenamiento.	Para cada perfil de código de borrado afectado, realice uno de los siguientes pasos en función de cómo se utilice el perfil: • **Utilizado en políticas de ILM activas**: Realizar una expansión. Añada suficientes nodos de almacenamiento nuevos para permitir que continúe la codificación de borrado. Consulte las instrucciones para "expandir el grid". • **Utilizado en una regla de ILM pero no en políticas de ILM activas**: Edite o elimine la regla y luego desactive el perfil de codificación de borrado. • **No se utiliza en ninguna regla de ILM**: Desactivar el perfil de codificación de borrado. **Nota:** Aparece un mensaje de error si intenta desactivar un perfil de codificación de borrado y los datos del objeto aún están asociados con el perfil. Es posible que deba esperar varias semanas antes de volver a intentar el proceso de desactivación. Descubra "desactivación de un perfil de código de borrado".
No, no puede decomisionar un nodo de archivado a menos que el nodo esté desconectado.	Si un nodo de archivado sigue conectado, no puede eliminarlo.	Complete los pasos de "Consideraciones para el nodo de archivado" y después "decomisionar el nodo desconectado".

Retirada de nodos de red desconectados

Es posible que deba retirar un nodo que no esté conectado actualmente a la cuadrícula (uno cuyo estado sea desconocido o administrativamente inactivo).

Antes de empezar

- Comprende las consideraciones para el decomisionado "Nodos Admin, Gateway y Archive" y las consideraciones para el desmantelamiento "Nodos de almacenamiento".
- Ha obtenido todos los requisitos previos.
- Se ha asegurado de que no hay ningún trabajo de reparación de datos activo. Consulte "Compruebe los trabajos de reparación de datos".
- Ha confirmado que la recuperación del nodo de almacenamiento no está en curso en ningún lugar de la cuadrícula. Si es así, debe esperar a que se complete cualquier recompilación de Cassandra como parte de la recuperación. A continuación, podrá continuar con el desmantelamiento.
- Se ha asegurado de que no se ejecutarán otros procedimientos de mantenimiento mientras el procedimiento de retirada del nodo se esté ejecutando, a menos que el procedimiento de retirada del nodo se detenga.
- La columna **DECOMmission possible** para el nodo desconectado o los nodos que desea retirar incluye una Marca de verificación verde.
- Tiene la clave de acceso de aprovisionamiento.

Acerca de esta tarea

Puede identificar los nodos desconectados buscando iconos desconocidos (azules) o administrativamente abajo (gris) en la columna **Estado**. En el ejemplo, el nodo de archivado denominado DC1-ARC1 está desconectado.

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1-105-230	Data Center 1	Admin Node	-		No, primary Admin Node decommissioning is not supported.
DC1-ARC1-105-237	Data Center 1	Archive Node	-		✓
DC1-G1-105-231	Data Center 1	API Gateway Node	-		No, at least one grid node is disconnected.

Antes de retirar el servicio de un nodo desconectado, tenga en cuenta lo siguiente:

- Este procedimiento está pensado principalmente para quitar un solo nodo desconectado. Si la cuadrícula contiene varios nodos desconectados, el software requiere que los retire todos al mismo tiempo, lo que aumenta la posibilidad de obtener resultados inesperados.

> Se pueden producir pérdidas de datos si decomisiona más de un nodo de almacenamiento desconectado a la vez. Consulte "Consideraciones sobre los nodos de almacenamiento desconectados".

> Use precaución al decomisionar nodos de almacenamiento en un grid que contenga nodos solo de metadatos basados en software. Si retira todos los nodos configurados para almacenar *both* objetos y metadatos, la capacidad de almacenar objetos se elimina de la cuadrícula. Consulte "Tipos de nodos de almacenamiento" Para obtener más información sobre nodos de almacenamiento solo de metadatos.

- Si no se puede quitar un nodo desconectado (por ejemplo, un nodo de almacenamiento necesario para el

quórum ADC), no se puede quitar ningún otro nodo desconectado.

Pasos

1. A menos que esté retirando un nodo de archivado (que debe estar desconectado), intente volver a conectar los nodos de grid desconectados o recuperarlos.

   Consulte "Procedimientos de recuperación de nodos de grid" si desea obtener instrucciones.

2. Si no puede recuperar un nodo de grid desconectado y desea decomisionar mientras está desconectado, seleccione la casilla de verificación de ese nodo.

   > Si la cuadrícula contiene varios nodos desconectados, el software requiere que los retire todos al mismo tiempo, lo que aumenta la posibilidad de obtener resultados inesperados.

   > Tenga cuidado al elegir retirar más de un nodo de grid desconectado a la vez, especialmente si selecciona varios nodos de almacenamiento desconectados. Si tiene más de un nodo de almacenamiento desconectado que no puede recuperar, póngase en contacto con el soporte técnico para determinar el mejor curso de acción.

3. Introduzca la clave de acceso de aprovisionamiento.

   El botón **Iniciar misión** está activado.

4. Haga clic en **Iniciar misión**.

   Aparece una advertencia que indica que ha seleccionado un nodo desconectado y que los datos del objeto se perderán si el nodo tiene la única copia de un objeto.

5. Revise la lista de nodos y haga clic en **Aceptar**.

   Se inicia el procedimiento de retirada y se muestra el progreso de cada nodo. Durante el procedimiento, se genera un nuevo paquete de recuperación que contiene el cambio de configuración de la cuadrícula.

6. En cuanto el nuevo paquete de recuperación esté disponible, haga clic en el enlace o seleccione **MANTENIMIENTO** > **Sistema** > **Paquete de recuperación** para acceder a la página Paquete de recuperación. A continuación, descargue la `.zip` archivo.

   Consulte las instrucciones para "Descarga del paquete de recuperación".

   > Descargue el Lo antes posible. del paquete de recuperación para asegurarse de que puede recuperar la red si hay algún problema durante el procedimiento de retirada de servicio.

   > El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

7. Supervise periódicamente la página de retirada para garantizar que todos los nodos seleccionados se han retirado correctamente.

   La retirada de los nodos de almacenamiento puede llevar días o semanas. Una vez completadas todas las tareas, la lista de selección de nodos se volverá a mostrar con un mensaje de éxito. Si se da de baja un nodo de almacenamiento desconectado, se muestra un mensaje de información que indica que se han iniciado los trabajos de reparación.

8. Una vez que los nodos se han apagado automáticamente como parte del procedimiento de retirada, quite las máquinas virtuales restantes u otros recursos asociados al nodo retirada del servicio.

   > No realice este paso hasta que los nodos se hayan apagado automáticamente.

9. Si va a retirar un nodo de almacenamiento, supervise el estado de los trabajos de reparación de **datos replicados** y **datos codificados por borrado (EC)** que se inician automáticamente durante el proceso de retirada del servicio.

Datos replicados

- Para obtener un porcentaje de finalización estimado para la reparación replicada, agregue el `show-replicated-repair-status` opción del comando repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Para determinar si las reparaciones están completas:
  a. Seleccione **NODES** > ***Storage Node que se está reparando*** > **ILM**.
  b. Revise los atributos en la sección Evaluación. Una vez completadas las reparaciones, el atributo **esperando - todo** indica 0 objetos.
- Para supervisar la reparación con más detalle:
  a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
  b. Seleccione ***grid*** > ***nodo de almacenamiento que se está reparando*** > **LDR** > **almacén de datos**.
  c. Utilice una combinación de los siguientes atributos para determinar, como sea posible, si las reparaciones replicadas se han completado.

  > Puede haber incoherencias en Cassandra y no se realiza un seguimiento de las reparaciones fallidas.

  - **Reparaciones intentadas (XRPA)**: Utilice este atributo para realizar un seguimiento del progreso de las reparaciones replicadas. Este atributo aumenta cada vez que un nodo de almacenamiento intenta reparar un objeto de alto riesgo. Cuando este atributo no aumenta durante un período más largo que el período de exploración actual (proporcionado por el atributo **período de exploración — estimado**), significa que el análisis de ILM no encontró objetos de alto riesgo que necesitan ser reparados en ningún nodo.

    > Los objetos de alto riesgo son objetos que corren el riesgo de perderse por completo. Esto no incluye objetos que no cumplen con la configuración de ILM.

  - **Período de exploración — estimado (XSCM)**: Utilice este atributo para estimar cuándo se aplicará un cambio de directiva a objetos ingeridos previamente. Si el atributo **reparos intentados** no aumenta durante un período más largo que el período de adquisición actual, es probable que se realicen reparaciones replicadas. Tenga en cuenta que el período de adquisición puede cambiar. El atributo **período de exploración — estimado (XSCM)** se aplica a toda la cuadrícula y es el máximo de todos los periodos de exploración de nodos. Puede consultar el historial de atributos **período de exploración — Estimated** de la cuadrícula para determinar un intervalo de tiempo adecuado.

Datos con código de borrado (EC)

Para supervisar la reparación de datos codificados mediante borrado y vuelva a intentar cualquier solicitud que pudiera haber fallado:

1. Determine el estado de las reparaciones de datos codificadas por borrado:
   - Seleccione **SUPPORT** > **Tools** > **Metrics** para ver el tiempo estimado hasta la finalización y el porcentaje de finalización del trabajo actual. A continuación, seleccione **EC Overview** en la sección Grafana. Consulte los paneles **tiempo estimado de trabajo de Grid EC hasta finalización** y **Porcentaje de trabajo de Grid EC completado**.

- Utilice este comando para ver el estado de un elemento específico `repair-data` operación:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilice este comando para enumerar todas las reparaciones:

  ```
  repair-data show-ec-repair-status
  ```

El resultado muestra información, como `repair ID`, para todas las reparaciones que se estén ejecutando anteriormente y actualmente.

2. Si el resultado muestra que la operación de reparación ha dado error, utilice el `--repair-id` opción de volver a intentar la reparación.

   Este comando vuelve a intentar una reparación de nodo con fallos mediante el ID de reparación 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Este comando reintenta realizar una reparación de volumen con fallos mediante el ID de reparación 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Después de terminar

Tan pronto como se hayan retirado los nodos desconectados y se hayan completado todos los trabajos de reparación de datos, puede retirar todos los nodos de red conectados según sea necesario.

A continuación, complete estos pasos una vez completado el procedimiento de retirada:

- Asegúrese de que las unidades del nodo de cuadrícula que se decomisionan se limpian. Utilice una herramienta o servicio de limpieza de datos disponible en el mercado para eliminar los datos de las unidades de forma permanente y segura.
- Si decomisionó un nodo del dispositivo y los datos del dispositivo estaban protegidos mediante el cifrado de nodos, utilice el instalador del dispositivo StorageGRID para borrar la configuración del servidor de gestión de claves (Clear KMS). Debe borrar la configuración de KMS si desea agregar el dispositivo a otra cuadrícula. Para ver instrucciones, consulte "Supervise el cifrado del nodo en modo de mantenimiento".

Retirada de nodos de grid conectados

Puede retirar y eliminar permanentemente los nodos conectados a la cuadrícula.

Antes de empezar

- Comprende las consideraciones para el decomisionado "Nodos Admin, Gateway y Archive" y las consideraciones para el desmantelamiento "Nodos de almacenamiento".
- Ha reunido todos los materiales necesarios.
- Se ha asegurado de que no hay ningún trabajo de reparación de datos activo.
- Ha confirmado que la recuperación del nodo de almacenamiento no está en curso en ningún lugar de la cuadrícula. Si es así, espere a que se complete cualquier reconstrucción de Cassandra realizada como parte de la recuperación. A continuación, podrá continuar con el desmantelamiento.

- Se ha asegurado de que no se ejecutarán otros procedimientos de mantenimiento mientras el procedimiento de retirada del nodo se esté ejecutando, a menos que el procedimiento de retirada del nodo se detenga.
- Tiene la clave de acceso de aprovisionamiento.
- Los nodos de grid están conectados.
- La columna **Decomiso posible** para el nodo o nodos que desea retirar incluye una marca de verificación verde.

> La retirada no se iniciará si uno o más volúmenes están sin conexión (sin montar) o si están en línea (montados), pero en estado de error.

> Si uno o más volúmenes quedan sin conexión mientras existe una decomisión en curso, el proceso de decomiso se completa una vez que estos volúmenes vuelvan a estar en línea.

- Todos los nodos de grid tienen un estado normal (verde) . Si ve uno de estos iconos en la columna **Estado**, debe intentar resolver el problema:

.	Color	Gravedad
	Amarillo	Aviso
	Naranja claro	Menor
	Naranja oscuro	Importante
	Rojo	Crítico

- Si anteriormente había retirado un nodo de almacenamiento desconectado, todos los trabajos de reparación de datos se completaron correctamente. Consulte "Compruebe los trabajos de reparación de datos".

> No elimine la máquina virtual de un nodo de grid ni otros recursos hasta que se le indique que lo haga en este procedimiento.

> Use precaución al decomisionar nodos de almacenamiento en un grid que contenga nodos solo de metadatos basados en software. Si retira todos los nodos configurados para almacenar *both* objetos y metadatos, la capacidad de almacenar objetos se elimina de la cuadrícula. Consulte "Tipos de nodos de almacenamiento" Para obtener más información sobre nodos de almacenamiento solo de metadatos.

Acerca de esta tarea

Cuando un nodo se retira, sus servicios se deshabilitan y el nodo se apaga automáticamente.

Pasos

1. En la página Decommission Nodes, seleccione la casilla de verificación de cada nodo de cuadrícula que

desee decomisionar.

2. Introduzca la clave de acceso de aprovisionamiento.

   El botón **Iniciar misión** está activado.

3. Selecciona **Iniciar decomiso**.
4. Revise la lista de nodos en el cuadro de diálogo de confirmación y seleccione **OK**.

   Se inicia el procedimiento de retirada del nodo y se muestra el progreso de cada nodo.

   > No desconecte un nodo de almacenamiento después de iniciar el procedimiento de retirada. El cambio de estado puede provocar que parte del contenido no se copie en otras ubicaciones.

5. En cuanto el nuevo paquete de recuperación esté disponible, seleccione el enlace Paquete de recuperación en el banner o seleccione **MANTENIMIENTO** > **Sistema** > **Paquete de recuperación** para acceder a la página Paquete de recuperación. A continuación, descargue la `.zip` archivo.

   Consulte "Descarga del paquete de recuperación".

   > Descargue el Lo antes posible. del paquete de recuperación para asegurarse de que puede recuperar la red si hay algún problema durante el procedimiento de retirada de servicio.

6. Supervise periódicamente la página nodos de misión de descommisión para garantizar que todos los nodos seleccionados se han retirado correctamente.

   > La retirada de los nodos de almacenamiento puede llevar días o semanas.

   Una vez completadas todas las tareas, la lista de selección de nodos se volverá a mostrar con un mensaje de éxito.

Después de terminar

Complete estos pasos después de completar el procedimiento de retirada del nodo:

1. Siga los pasos adecuados para su plataforma. Por ejemplo:
   - **Linux**: Es posible que desee desconectar los volúmenes y eliminar los archivos de configuración de nodo creados durante la instalación. Consulte "Instalar StorageGRID en Red Hat Enterprise Linux" y.. "Instalar StorageGRID en Ubuntu o Debian".
   - **VMware**: Es posible que desee utilizar la opción de vCenter “Eliminar del disco” para eliminar la máquina virtual. También puede ser necesario eliminar los discos de datos que sean independientes de la máquina virtual.
   - **Dispositivo StorageGRID**: El nodo del dispositivo vuelve automáticamente a un estado no desplegado en el que puede acceder al instalador del dispositivo StorageGRID. Puede apagar el dispositivo o añadirlo a otro sistema StorageGRID.
2. Asegúrese de que las unidades del nodo de cuadrícula que se decomisionan se limpian. Utilice una herramienta o servicio de limpieza de datos disponible en el mercado para eliminar los datos de las unidades de forma permanente y segura.
3. Si decomisionó un nodo del dispositivo y los datos del dispositivo estaban protegidos mediante el cifrado

de nodos, utilice el instalador del dispositivo StorageGRID para borrar la configuración del servidor de gestión de claves (Clear KMS). Debe borrar la configuración de KMS si desea agregar el dispositivo a otra cuadrícula. Para ver instrucciones, consulte "Supervise el cifrado del nodo en modo de mantenimiento".

Pausar y reanudar el proceso de retirada de los nodos de almacenamiento

Si necesita realizar un segundo procedimiento de mantenimiento, puede pausar el procedimiento de retirada de un nodo de almacenamiento durante determinadas fases. Una vez finalizado el otro procedimiento, puede reanudar el decomisionado.

> El botón **Pausa** sólo se activa cuando se alcanzan las etapas de evaluación de ILM o de retirada de datos con código de borrado; sin embargo, la evaluación de ILM (migración de datos) continuará ejecutándose en segundo plano.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".

Pasos

1. Seleccione **MANTENIMIENTO** > **tareas** > **misión**.

   Aparece la página de retirada.

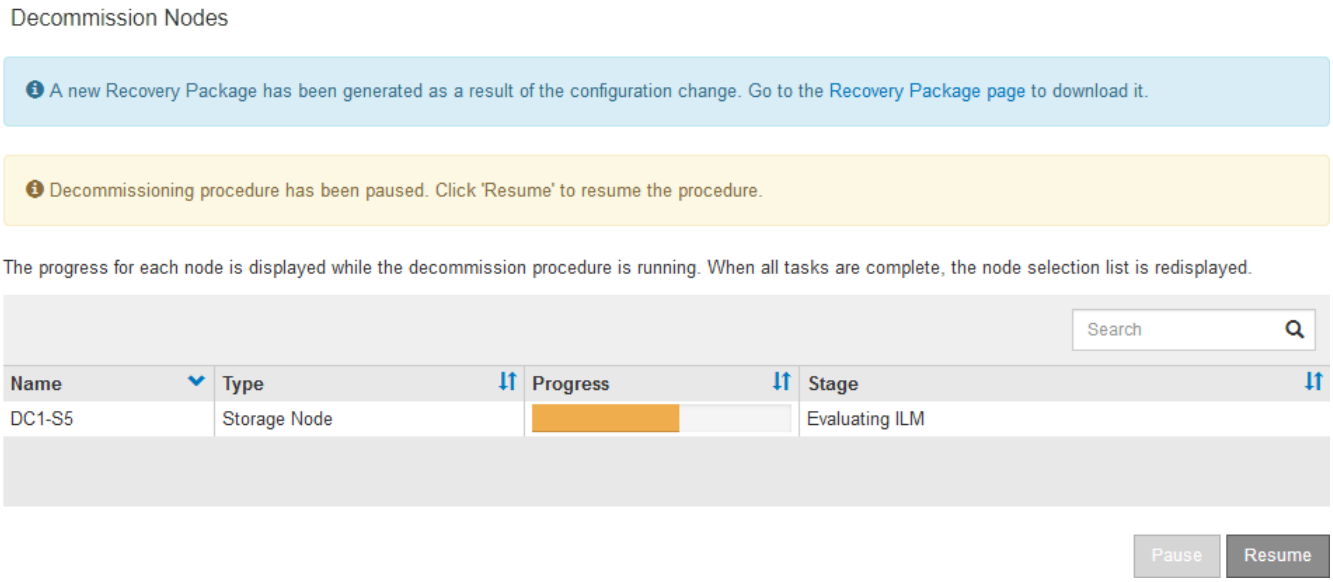
2. Seleccione **nodos de misión**.

   Aparecerá la página nodos de misión. Cuando el procedimiento de retirada de servicio alcanza cualquiera de las siguientes fases, el botón **Pausa** está activado.

   - Evaluando ILM
   - Desmantelamiento de datos codificados de borrado

3. Seleccione **Pausa** para suspender el procedimiento.

   La etapa actual está en pausa y el botón **Reanudar** está activado.



4. Una vez finalizado el otro procedimiento de mantenimiento, seleccione **Reanudar** para continuar con la retirada.

Solucione problemas de decomisionado de nodos

Si el procedimiento de retirada del nodo se detiene debido a un error, puede realizar pasos específicos para solucionar el problema.

Antes de empezar

Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".

Acerca de esta tarea

Si apaga el nodo de cuadrícula que se va a retirar del servicio, la tarea se detiene hasta que se reinicia el nodo de cuadrícula. El nodo de grid debe estar en línea.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. En el árbol de topología de cuadrícula, expanda cada entrada de nodo de almacenamiento y compruebe que los servicios DDS y LDR están en línea.

   Para realizar el decomisionado del nodo de almacenamiento, todos los nodos y todos los servicios deben estar en buen estado al iniciar un decomisionado del nodo y el sitio en línea.

3. Para ver las tareas de la cuadrícula activa, seleccione **nodo de administración principal** > **CMN** > **tareas de cuadrícula** > **Descripción general**.
4. Compruebe el estado de la tarea de decomisionado de la cuadrícula.

   a. Si el estado de la tarea de eliminación de la cuadrícula indica un problema al guardar los paquetes de tareas de la cuadrícula, seleccione **nodo de administración principal** > **CMN** > **Eventos** > **Descripción general**.

   b. Compruebe el número de relés de auditoría disponibles.

      Si el atributo retransmisión de auditoría disponible es uno o superior, el servicio CMN está conectado al menos a un servicio ADC. Los servicios ADC actúan como relés de auditoría.

   El servicio CMN debe estar conectado a al menos un servicio ADC y la mayoría (el 50 por ciento más uno) de los servicios ADC del sistema StorageGRID debe estar disponible para que una tarea de cuadrícula pueda moverse de una fase de desmantelamiento a otra y terminar.

   a. Si el servicio CMN no está conectado a suficientes servicios ADC, asegúrese de que los nodos de almacenamiento están conectados y compruebe la conectividad de red entre los nodos de administración principal y de almacenamiento.

Sitio de decomisionar

Consideraciones para quitar un sitio

Antes de utilizar el procedimiento de retirada del sitio para quitar un sitio, debe revisar las consideraciones.

Qué sucede al retirar un sitio

Al retirar un sitio, StorageGRID quita de forma permanente todos los nodos del sitio y el sitio propio del sistema StorageGRID.

Una vez completado el procedimiento de retirada de instalaciones:

- Ya no puede utilizar StorageGRID para ver ni acceder al sitio ni a ninguno de los nodos del sitio.
- Ya no puede utilizar pools de almacenamiento ni perfiles de código de borrado que hagan referencia al sitio. Cuando StorageGRID decomisiona un sitio, elimina automáticamente estos pools de almacenamiento y desactiva estos perfiles de código de borrado.

Diferencias entre el sitio conectado y los procedimientos de retirada de sitios desconectados

Puede usar el procedimiento de retirada del sitio para quitar un sitio en el que todos los nodos están conectados a StorageGRID (conocido como decomiso de un sitio conectado) o para quitar un sitio en el que todos los nodos estén desconectados de StorageGRID (conocido como decomiso de sitio desconectado). Antes de comenzar, debe comprender las diferencias entre estos procedimientos.

> Si un sitio contiene una mezcla de conectado ( ) y nodos desconectados (o.), debe volver a conectar todos los nodos sin conexión.

- Una retirada de sitio conectado permite quitar un sitio operativo del sistema StorageGRID. Por ejemplo, puede realizar una retirada de sitio conectado para eliminar un sitio que sea funcional pero que ya no sea necesario.
- Cuando StorageGRID quita un sitio conectado, utiliza ILM para gestionar los datos de los objetos del sitio. Antes de iniciar una retirada de sitios conectados, debe eliminar el sitio de todas las reglas de ILM y activar una nueva política de ILM. ILM procesos para migrar datos de objetos y los procesos internos para quitar un sitio pueden producirse a la vez, pero la práctica recomendada es permitir que se completen los pasos de ILM antes de iniciar el procedimiento de retirada real.
- Una retirada de sitio desconectada permite quitar un sitio con errores del sistema StorageGRID. Por ejemplo, puede realizar un retiro de sitio desconectado para quitar un sitio que ha sido destruido por un incendio o inundación.

  Cuando StorageGRID quita un sitio desconectado, este considera que todos los nodos son irrecuperables y no intenta conservar los datos. Sin embargo, antes de iniciar una retirada de sitios desconectada, debe eliminar el sitio de todas las reglas de ILM y activar una nueva política de ILM.

> Antes de realizar un procedimiento de retirada de sitio desconectado, debe ponerse en contacto con el representante de su cuenta de NetApp. NetApp revisará sus requisitos antes de habilitar todos los pasos en el asistente del sitio de retirada. No debería intentar retirar un sitio desconectado si cree que podría recuperar el sitio o recuperar datos de objeto del sitio.

Requisitos generales para quitar un sitio conectado o desconectado

Antes de quitar un sitio conectado o desconectado, debe tener en cuenta los siguientes requisitos:

- No puede retirar un sitio que incluya el nodo de administración principal.
- No puede retirar un sitio que incluya un nodo de archivado.
- No puede decomisionar un sitio si alguno de los nodos tiene una interfaz que pertenezca a un grupo de

alta disponibilidad. Debe editar el grupo de alta disponibilidad para quitar la interfaz del nodo o quitar todo el grupo de alta disponibilidad.

- No puede retirar un sitio si contiene una mezcla de conectado ( ) y desconectados (o.) nodos.
- No puede retirar un sitio si algún nodo de cualquier otro sitio está desconectado (o.).
- No puede iniciar el procedimiento de retirada del sitio si hay una operación de reparación ec-nodo-en curso. Consulte "Compruebe los trabajos de reparación de datos" realizar un seguimiento de las reparaciones de datos codificados a borrado.
- Mientras se está ejecutando el procedimiento de retirada de instalaciones:
  - No se pueden crear reglas de ILM que hagan referencia al sitio que se va a retirar. Tampoco puede editar una regla de ILM existente para hacer referencia al sitio.
  - No se pueden llevar a cabo otros procedimientos de mantenimiento, como la ampliación o la actualización.

> Si necesita realizar otro procedimiento de mantenimiento durante la retirada de un sitio conectado, puede hacerlo "Detenga el procedimiento mientras se quitan los nodos de almacenamiento". El botón **Pausa** sólo se activa cuando se alcanzan las etapas de evaluación de ILM o de retirada de datos con código de borrado; sin embargo, la evaluación de ILM (migración de datos) continuará ejecutándose en segundo plano. Una vez completado el segundo procedimiento de mantenimiento, puede reanudar el decomisionado.

  - Si necesita recuperar algún nodo después de iniciar el procedimiento de retirada del sitio, debe ponerse en contacto con el servicio de soporte de.
- No puede retirar más de un sitio a la vez.
- Si el sitio incluye uno o más nodos de administración y el inicio de sesión único (SSO) está habilitado para el sistema StorageGRID, debe quitar todas las confianzas de partes que dependan del sitio de los Servicios de Federación de Active Directory (AD FS).

Requisitos para la gestión del ciclo de vida de la información (ILM)

Como parte de la eliminación de un sitio, debe actualizar la configuración de ILM. El asistente para el sitio de retirada le guía a través de una serie de pasos previos para garantizar lo siguiente:

- El sitio no está referido por ninguna política de ILM. Si es, debe editar las políticas o crear y activar políticas con nuevas reglas de ILM.
- Las reglas de ILM no hacen referencia al sitio, incluso si no se utilizan en ninguna política. Debe eliminar o editar todas las reglas que hacen referencia al sitio.

Cuando StorageGRID decomisiona el sitio, desactivará automáticamente todos los perfiles de código de borrado no utilizados que hagan referencia al sitio y eliminará automáticamente los grupos de almacenamiento no utilizados que hagan referencia al sitio. Si existe un pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores), se elimina porque utiliza todos los sitios.

> Antes de quitar un sitio, puede que sea necesario crear nuevas reglas de ILM y activar una nueva política de ILM. En estas instrucciones, se asume que comprende bien cómo funciona ILM y que está familiarizado con la creación de pools de almacenamiento, perfiles de codificación de borrado, reglas de ILM, y la simulación y activación de una política de ILM. Consulte "Gestión de objetos con ILM".

Consideraciones sobre los datos del objeto en un sitio conectado

Si va a realizar una retirada de sitios conectados, debe decidir qué hacer con los datos de objetos existentes en el sitio al crear nuevas reglas de ILM y una nueva política de ILM. Puede realizar una de las siguientes acciones o ambas:

- Mueva los datos del objeto del sitio seleccionado a uno o más sitios de la cuadrícula.

  Ejemplo para el traslado de datos: Suponga que desea retirar un sitio en Raleigh porque agregó un nuevo sitio en Sunnyvale. En este ejemplo, desea mover todos los datos del objeto del sitio antiguo al sitio nuevo. Antes de actualizar las reglas de ILM y las políticas de ILM, debe revisar la capacidad en ambos sitios. Debe asegurarse de que el site de Sunnyvale tenga suficiente capacidad para acomodar los datos de objetos desde el site de Raleigh y que permanecerá en Sunnyvale la capacidad adecuada para su crecimiento futuro.

  > Para garantizar que haya capacidad adecuada disponible, es posible que deba hacerlo "expanda una cuadrícula" Cuando se añaden volúmenes de almacenamiento o nodos de almacenamiento a un sitio existente o se añade un sitio nuevo antes de realizar este procedimiento.

- Eliminar copias de objeto del sitio seleccionado.

  Ejemplo para eliminar datos: Suponga que actualmente utiliza una regla ILM de 3 copias para replicar datos de objetos en tres sitios. Antes de retirar un sitio, puede crear una regla de ILM equivalente con 2 copias para almacenar datos en solo dos sitios. Cuando activa una nueva política de ILM que usa la regla de dos copias, StorageGRID elimina las copias del tercer sitio porque ya no satisfacen los requisitos de ILM. Sin embargo, los datos del objeto se seguirán protegiendo y la capacidad de los dos sitios restantes será la misma.

  > No cree nunca una regla de ILM de una sola copia para acomodar la eliminación de un sitio. Una regla de ILM que crea solo una copia replicada en cualquier periodo de tiempo pone los datos en riesgo de pérdida permanente. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

Requisitos adicionales para una retirada de sitios conectados

Antes de que StorageGRID pueda eliminar un sitio conectado, debe asegurarse de lo siguiente:

- Todos los nodos del sistema StorageGRID deben tener un estado de conexión de **conectado** ( ); sin embargo, los nodos pueden tener alertas activas.

  > Puede completar los pasos 1-4 del Asistente para sitio de retirada si uno o más nodos están desconectados. Sin embargo, no puede completar el paso 5 del asistente, que inicia el proceso de retirada, a menos que todos los nodos estén conectados.

- Si el sitio que desea eliminar contiene un nodo de gateway o un nodo de administración que se utiliza para el equilibrio de carga, es posible que deba hacerlo "expanda una cuadrícula" para agregar un nuevo nodo equivalente en otro sitio. Asegúrese de que los clientes pueden conectarse al nodo de repuesto antes de iniciar el procedimiento de retirada del sitio.
- Si el sitio que va a eliminar contiene cualquier nodo de puerta de enlace o nodo de administración que se

encuentre en un grupo de alta disponibilidad (ha), puede completar los pasos 1-4 del asistente para sitio de retirada. Sin embargo, no puede completar el Paso 5 del asistente, que inicia el proceso de decomiso hasta que elimine estos nodos de todos los grupos HA. Si los clientes existentes se conectan a un grupo de alta disponibilidad que incluye nodos del sitio, debe asegurarse de que pueden continuar conectando a StorageGRID después de eliminar el sitio.

- Si los clientes se conectan directamente a nodos de almacenamiento del sitio que va a quitar, debe asegurarse de que pueden conectarse a nodos de almacenamiento en otros sitios antes de iniciar el procedimiento de retirada del sitio.
- Debe proporcionar espacio suficiente en los sitios restantes para acomodar cualquier dato de objetos que se moverá debido a los cambios en cualquier política de ILM activa. En algunos casos, es posible que deba hacerlo "expanda una cuadrícula" Añadiendo nodos de almacenamiento, volúmenes de almacenamiento o sitios nuevos antes de completar una retirada de sitio conectado.
- Debe dejar tiempo suficiente para completar el procedimiento de retirada. Los procesos de ILM de StorageGRID pueden tardar días, semanas o incluso meses en mover o eliminar datos de objetos del sitio antes de dejar de lado el sitio.

> La transferencia o eliminación de datos de objetos de un sitio puede llevar días, semanas o incluso meses, en función de la cantidad de datos almacenados en el sitio, la carga en el sistema, las latencias de red y la naturaleza de los cambios de ILM necesarios.

- Siempre que sea posible, debe completar los pasos 1-4 del Asistente para sitio de retirada tan pronto como pueda. El procedimiento de retirada de servicio se completará más rápidamente y con menos interrupciones e impactos en el rendimiento si permite que los datos se muevan desde el sitio antes de iniciar el procedimiento de retirada real (seleccionando **Iniciar misión** en el paso 5 del asistente).

Requisitos adicionales para una retirada de sitios desconectada

Antes de que StorageGRID pueda quitar un sitio desconectado, debe asegurarse de lo siguiente:

- Se ha puesto en contacto con el representante de cuentas de NetApp. NetApp revisará sus requisitos antes de habilitar todos los pasos en el asistente del sitio de retirada.

> No debería intentar retirar un sitio desconectado si cree que podría recuperar el sitio o recuperar cualquier dato de objeto del sitio. Consulte "Cómo el soporte técnico recupera un sitio".

- Todos los nodos del sitio deben tener el estado de conexión de uno de los siguientes:
  - **Desconocido** ( ): Por un motivo desconocido, un nodo está desconectado o los servicios del nodo están inactivos 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.
  - **Administrativamente abajo** ( ): 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.
- Todos los nodos de todos los demás sitios deben tener un estado de conexión de **conectado** ( ); sin embargo, estos otros nodos pueden tener alertas activas.
- Debe entender que ya no podrá utilizar StorageGRID para ver o recuperar los datos de objeto almacenados en el sitio. Cuando StorageGRID realiza este procedimiento, no intenta conservar ningún dato del sitio desconectado.

Si sus reglas y políticas de ILM se diseñaron para proteger contra la pérdida de un solo sitio, seguirán existiendo copias de los objetos en los sitios restantes.

- Debe entender que si el sitio contenía la única copia de un objeto, el objeto se pierde y no se puede recuperar.

Consideraciones de coherencia al eliminar un sitio

La consistencia de un bloque de S3 o un contenedor de Swift determina si StorageGRID replica por completo los metadatos de objetos en todos los nodos y sitios antes de indicar al cliente que la ingesta del objeto se ha realizado correctamente. La consistencia proporciona un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en distintos nodos de almacenamiento y sitios.

Cuando StorageGRID quita un sitio, éste debe asegurarse de que no se escribe ningún dato en el sitio que se va a quitar. Como resultado, anula temporalmente la coherencia de cada cubo o contenedor. Tras iniciar el proceso de retirada del sitio, StorageGRID utiliza temporalmente consistencia de sitio seguro para evitar que los metadatos del objeto se escriban en el sitio que se está quitando.

Como resultado de esta sustitución temporal, tenga en cuenta que cualquier operación de escritura, actualización y eliminación de cliente que se produzca durante un decomiso de sitio puede fallar si varios nodos dejan de estar disponibles en los sitios restantes.

Reúna los materiales necesarios

Antes de retirar de servicio un sitio, debe obtener los siguientes materiales.

Elemento	Notas
Paquete de recuperación `.zip` archivo	Debe descargar el paquete de recuperación más reciente `.zip` archivo (`sgws-recovery-package-id-revision.zip`). Puede utilizar el archivo de paquete de recuperación para restaurar el sistema si se produce un fallo. "Descargue el paquete de recuperación"
`Passwords.txt` archivo	Este archivo contiene las contraseñas que se necesitan para acceder a los nodos de grid en la línea de comandos y se incluye en el paquete de recuperación.
Clave de acceso de aprovisionamiento	La frase de contraseña se crea y documenta cuando se instala el sistema StorageGRID por primera vez. La clave de acceso de aprovisionamiento no está en la `Passwords.txt` archivo.
Descripción de la topología del sistema StorageGRID antes de decomisionar	Si está disponible, obtenga cualquier documentación que describa la topología actual del sistema.

Información relacionada

"Requisitos del navegador web"

Paso 1: Seleccione Sitio

Para determinar si un sitio se puede retirar del servicio, comience por acceder al asistente del sitio de retirada.

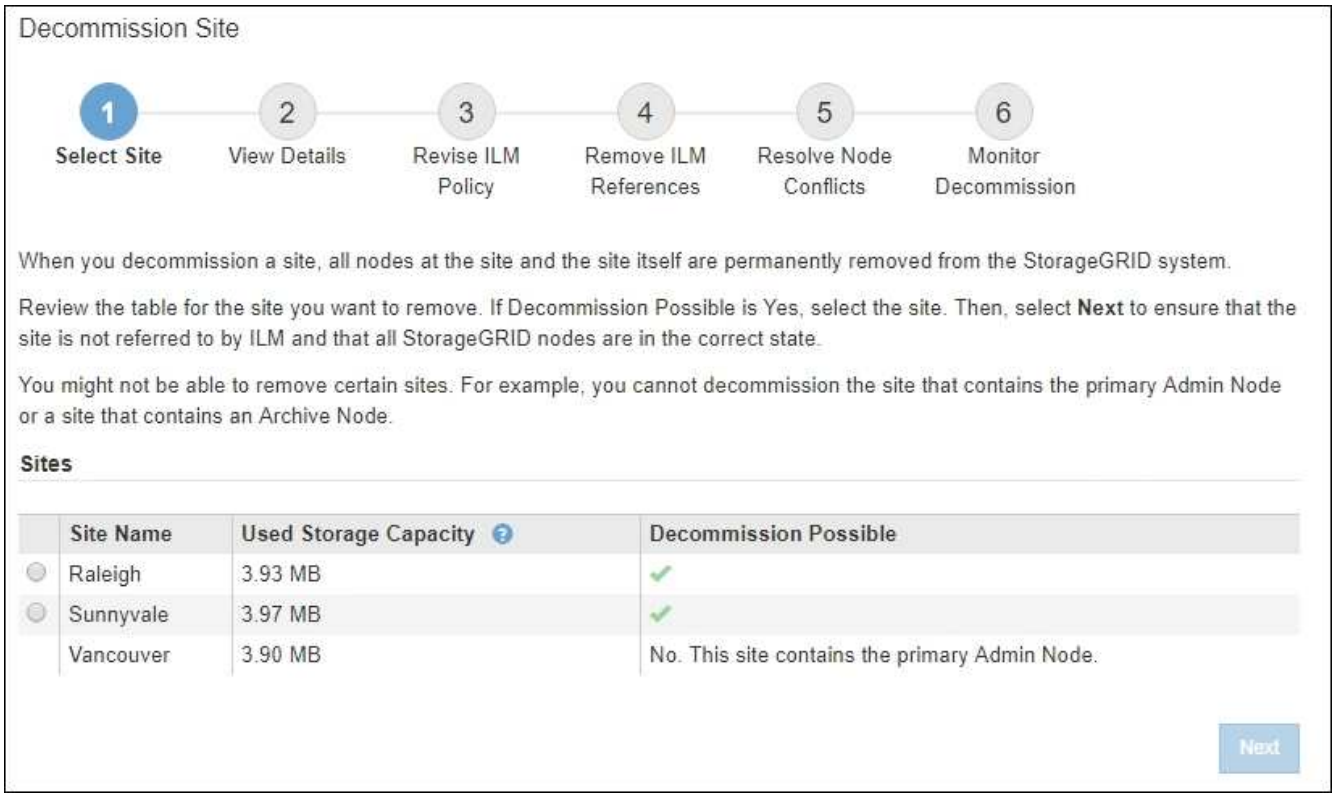
Antes de empezar

- Usted ha obtenido todos los materiales requeridos.
- Ha revisado las consideraciones para eliminar un sitio.
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz o permisos de mantenimiento e ILM".

Pasos

1. Seleccione **MANTENIMIENTO** > **tareas** > **misión**.
2. Seleccione **Sitio de misión**.

   Aparece el paso 1 (Seleccionar sitio) del asistente de ubicación de misión. Este paso incluye una lista alfabética de los sitios de su sistema StorageGRID.



3. Consulte los valores de la columna **capacidad de almacenamiento utilizada** para determinar cuánto almacenamiento se está utilizando actualmente para los datos de objetos de cada sitio.

   La capacidad de almacenamiento utilizada es una estimación. Si los nodos están sin conexión, la capacidad de almacenamiento utilizada es el último valor conocido del sitio.

   - Para la retirada de un sitio conectado, este valor representa la cantidad de datos de objeto que debe moverse a otros sitios o eliminarse mediante ILM antes de poder retirar este sitio de forma segura.
   - Para una retirada de sitios desconectada, este valor representa cuánto del almacenamiento de datos del sistema quedará inaccesible cuando usted retire este sitio.

Si su política de ILM se diseñó para ofrecer protección contra la pérdida de un solo sitio, las copias de sus datos de objetos aún deben existir en los sitios restantes.

4. Revise las razones en la columna **DECOMmission posible** para determinar qué sitios pueden ser retirados del servicio actualmente.

Si hay más de una razón por la que un sitio no puede ser desmantelado, se muestra la razón más crítica.

Razón posible de retirada	Descripción	Paso siguiente
Marca de verificación verde ( )	Puede retirar este sitio.	Vaya a. el siguiente paso.
No Este sitio contiene el nodo de administración principal.	No puede retirar un sitio que contenga el nodo de administración principal.	Ninguno. No puede realizar este procedimiento.
No Este sitio contiene uno o varios nodos de archivado.	No puede retirar un sitio que contenga un nodo de archivado.	Ninguno. No puede realizar este procedimiento.
No Todos los nodos de este sitio están desconectados. Póngase en contacto con el representante de cuenta de NetApp.	No puede realizar una retirada del sitio conectado a menos que todos los nodos del sitio estén conectados ( ).	Si desea realizar una retirada de sitios sin conexión, debe ponerse en contacto con su representante de cuenta de NetApp, que revisará sus requisitos y activará el resto del asistente para la retirada de sitios. **IMPORTANTE**: Nunca desconecte los nodos en línea para poder eliminar un sitio. Perderá datos.

El ejemplo muestra un sistema StorageGRID con tres sitios. La marca de verificación verde ( ) Para los sitios de Raleigh y Sunnyvale indica que puede retirar esos sitios. Sin embargo, no puede retirar el sitio de Vancouver porque contiene el nodo de administración principal.

1. Si es posible retirar el servicio, seleccione el botón de opción de la planta.

   El botón **Siguiente** está activado.

2. Seleccione **Siguiente**.

   Se muestra el paso 2 (Ver detalles).

Paso 2: Ver detalles

En el paso 2 (Ver detalles) del asistente del sitio de decoración, puede revisar qué nodos están incluidos en el sitio, ver cuánto espacio se ha utilizado en cada nodo de

almacenamiento y evaluar cuánto espacio libre está disponible en los otros sitios de la cuadrícula.

Antes de empezar

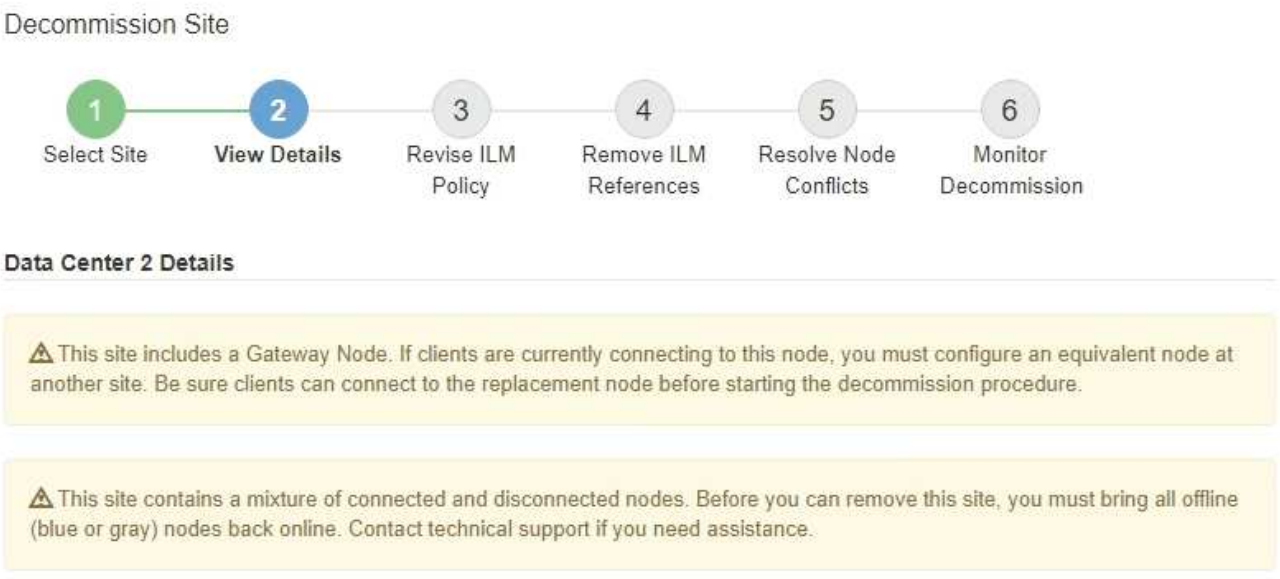
Antes de retirar un sitio, debe revisar la cantidad de datos de objeto que hay en el sitio.

- Si está realizando una retirada de sitios conectados, debe comprender cuántos datos de objetos hay actualmente en el sitio antes de actualizar ILM. En función de las capacidades del sitio y de sus necesidades de protección de datos, puede crear nuevas reglas de ILM para mover datos a otros sitios o eliminar datos de objetos del sitio.
- Realice las expansiones de nodos de almacenamiento necesarias antes de iniciar el procedimiento de retirada del servicio, si es posible.
- Si está realizando una retirada de sitio desconectado, debe entender cuántos datos de objeto se volverán permanentemente inaccesibles al quitar el sitio.

> Si está realizando una retirada del sitio desconectada, ILM no podrá mover ni eliminar datos de objetos. Se perderán todos los datos que permanezcan en las instalaciones. Sin embargo, si su política de ILM se diseñó para protegerse contra la pérdida de un solo sitio, las copias de los datos de objetos siguen existiendo en los sitios restantes. Consulte "Habilite la protección contra pérdida de sitio".

Pasos

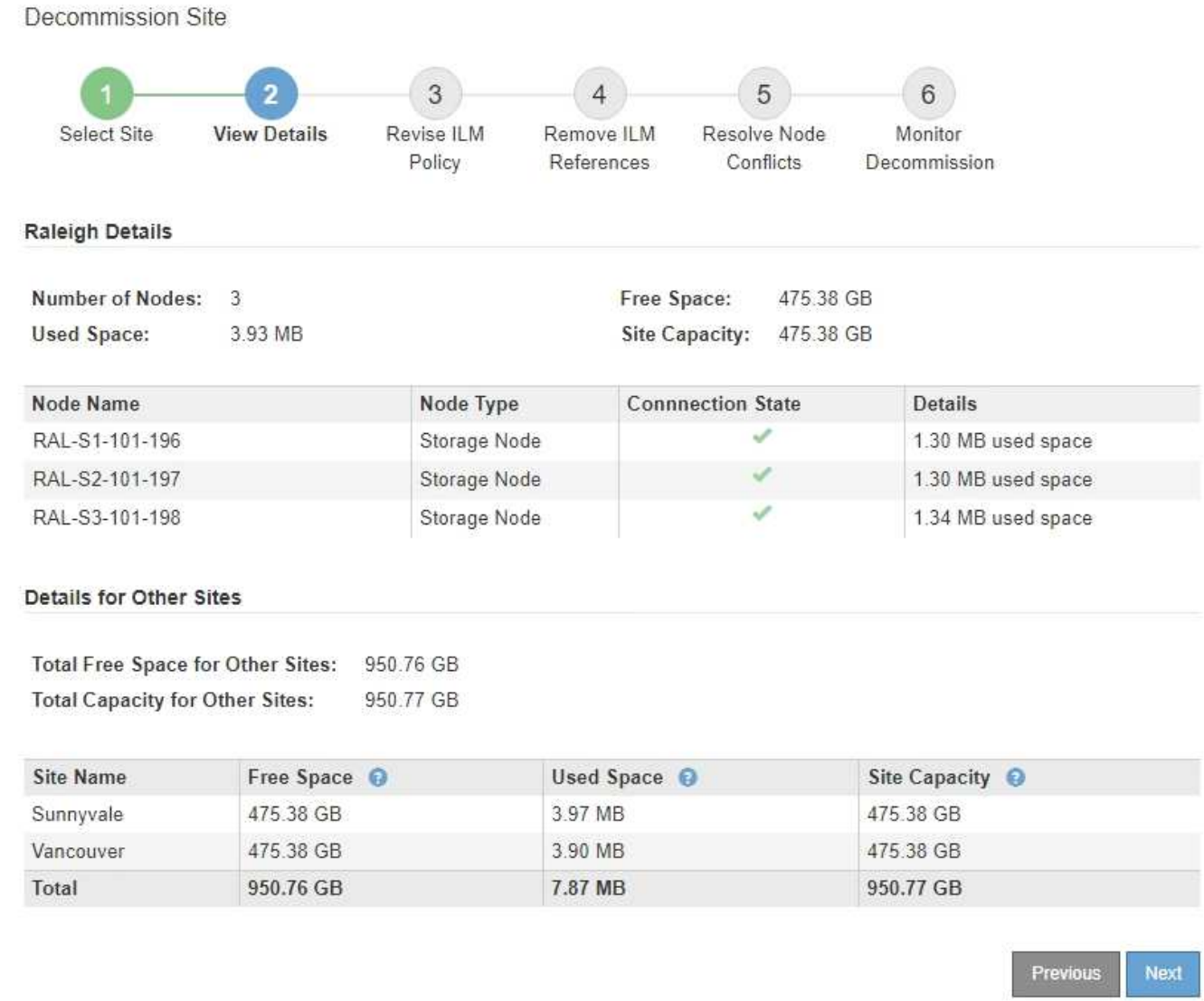
1. En el paso 2 (Ver detalles), revise las advertencias relacionadas con el sitio que seleccionó para quitar.



   Aparecerá una advertencia en los siguientes casos:

   - El sitio incluye un nodo de puerta de enlace. Si los clientes S3 y Swift se están conectando actualmente a este nodo, debe configurar un nodo equivalente en otro sitio. Asegúrese de que los clientes pueden conectarse al nodo de repuesto antes de continuar con el procedimiento de retirada.
   - El sitio contiene una mezcla de conectado ( ) y nodos desconectados (o.). Antes de poder quitar este sitio, deben volver a conectar todos los nodos sin conexión.

2. Revise los detalles sobre el sitio que ha seleccionado para eliminar.



Se incluye la siguiente información para el sitio seleccionado:

- Número de nodos
- El espacio total usado, el espacio libre y la capacidad de todos los nodos de almacenamiento del sitio.
  - Para una retirada de sitios conectados, el valor **espacio usado** representa la cantidad de datos de objetos que deben moverse a otros sitios o eliminarse con ILM.
  - Para un retiro de sitio desconectado, el valor **espacio usado** indica cuántos datos de objeto serán inaccesibles cuando usted quita el sitio.
- Nombres de nodo, tipos y estados de conexión:
  - (Conectado)
  - (Administrativamente abajo)
  - (Desconocido)
- Detalles sobre cada nodo:
  - Para cada nodo de almacenamiento, la cantidad de espacio que se ha usado para los datos de objetos.

- Para los nodos de administrador y los nodos de puerta de enlace, si el nodo se utiliza actualmente en un grupo de alta disponibilidad (ha). No puede decomisionar un nodo de administración ni un nodo de puerta de enlace que se utilice en un grupo de alta disponibilidad. Antes de iniciar el decomiso, edite los grupos de alta disponibilidad para quitar todos los nodos del sitio o quitar el grupo de alta disponibilidad si solo incluye nodos de este sitio. Para ver instrucciones, consulte "Gestione grupos de alta disponibilidad".

3. En la sección Detalles de otros sitios de la página, evalúe cuánto espacio hay disponible en los otros sitios de la cuadrícula.

Details for Other Sites

Total Free Space for Other Sites:	950.76 GB
Total Capacity for Other Sites:	950.77 GB

Site Name	Free Space	Used Space	Site Capacity
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

Si va a realizar una retirada de sitios conectados y va a utilizar ILM para mover datos de objetos del sitio seleccionado (en lugar de eliminarlos solamente), debe asegurarse de que los otros sitios tengan suficiente capacidad para acomodar los datos movidos y de que la capacidad adecuada quede para un crecimiento futuro.

Aparecerá una advertencia si el **espacio usado** del sitio que desea quitar es mayor que el **espacio libre total para otros sitios**. Es posible que deba realizar una ampliación antes de realizar este procedimiento para garantizar que haya disponible la capacidad de almacenamiento adecuada una vez se ha eliminado el sitio.

4. Seleccione **Siguiente**.

Aparece el paso 3 (revisar la política de ILM).

Paso 3: Revisar las políticas de ILM

En el Paso 3 (Revisar políticas de ILM) del asistente del sitio de retirada, puede determinar si alguna política de ILM hace referencia al sitio.

Antes de empezar

Usted tiene una buena comprensión de cómo hacerlo "Gestione objetos con ILM". Está familiarizado con la creación de pools de almacenamiento y reglas de ILM, así como con la simulación y activación de una política de ILM.

Acerca de esta tarea

StorageGRID no puede retirar un sitio si alguna regla de gestión de la vida útil de la información de alguna política (activa o inactiva) hace referencia a ese sitio.

Si alguna política de ILM hace referencia al sitio que desea retirar, debe eliminar esas políticas o editarlas para que cumplan con estos requisitos:

- Proteja completamente todos los datos de objetos.
- No consulte el sitio en el que está decomisionado.
- No utilice pools de almacenamiento que hagan referencia al sitio ni utilice la opción Todos los sitios.
- No utilice perfiles de código de borrado que hagan referencia al sitio.
- No utilice la regla Hacer 2 copias de StorageGRID 11,6 o instalaciones anteriores.

> No cree nunca una regla de ILM de una sola copia para acomodar la eliminación de un sitio. Una regla de ILM que crea solo una copia replicada en cualquier periodo de tiempo pone los datos en riesgo de pérdida permanente. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como las actualizaciones.

> Si está realizando una retirada de sitio *Connected site*, debe tener en cuenta cómo StorageGRID debe gestionar los datos de objeto actualmente en el sitio que desea eliminar. En función de sus requisitos de protección de datos, las nuevas reglas pueden mover los datos de objetos existentes a diferentes sitios o pueden eliminar cualquier copia de objetos adicionales que ya no sean necesarias.

Póngase en contacto con el soporte técnico si necesita ayuda para diseñar una nueva política.

Pasos

1. En el Paso 3 (revisar políticas de ILM), determine si alguna política de ILM hace referencia al sitio que ha seleccionado para decomisionar.
2. Si no aparece ninguna política, seleccione **Siguiente** para ir a. "Paso 4: Eliminar referencias de ILM".
3. Si aparece una o más políticas *active* ILM, clone cada política existente o cree nuevas políticas que no hagan referencia al sitio al que se va a retirar:

   a. Seleccione el enlace de la política en la columna Nombre de Política.

      La página de detalles de política de ILM de la política se muestra en una nueva pestaña del navegador. La página Sitio de retirada permanecerá abierta en la pestaña otros.

   b. Siga estas directrices e instrucciones según sea necesario:

      - Trabajar con reglas de ILM:
        - "Cree uno o varios pools de almacenamiento" que no hacen referencia al sitio.
        - "Edite o reemplace las reglas" que hacen referencia al sitio.

          > No seleccione la regla **Hacer 2 copias** porque esa regla usa el grupo de almacenamiento **Todos los nodos de almacenamiento**, que no está permitido.

      - Funciona con políticas de ILM:
        - "Clonar una política de ILM existente" o. "Cree una nueva política de ILM".
        - Asegúrese de que la regla predeterminada y otras reglas no hacen referencia al sitio.

Debe confirmar que las reglas de ILM se encuentran en el orden correcto. Cuando se activa la directiva, las reglas del orden indicado evalúan los objetos nuevos y existentes, empezando por la parte superior.

c. Ingerir objetos de prueba y simular la política para asegurarse de que se aplican las reglas correctas.

Los errores de un política de ILM pueden provocar la pérdida de datos irrecuperable. Revise y simule cuidadosamente la directiva antes de activarla para confirmar que funcionará según lo previsto.

Cuando se activa una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, incluidos los existentes y los objetos recién procesados. Antes de activar una nueva política de ILM, revise los cambios que se produzcan en la ubicación de los objetos replicados y los códigos de borrado existentes. El cambio de la ubicación de un objeto existente podría dar lugar a problemas temporales de recursos cuando se evalúan e implementan las nuevas colocaciones.

d. Active las nuevas políticas y asegúrese de que las políticas antiguas están ahora inactivas.

Si desea activar varias políticas, "Siga los pasos para crear etiquetas de políticas de ILM".

Si va a realizar una retirada de sitios conectados, StorageGRID empieza a eliminar datos de objetos del sitio seleccionado en cuanto activa la nueva política de gestión del ciclo de vida de la información. Mover o eliminar todas las copias de objetos puede llevar semanas. Aunque puede iniciar con seguridad un decomiso de sitio mientras los datos del objeto siguen estando en el sitio, el procedimiento de retirada se completará más rápidamente y con menos interrupciones e impactos en el rendimiento si permite que los datos se muevan desde el sitio antes de iniciar el procedimiento de retirada real (Seleccionando **Iniciar misión** en el paso 5 del asistente).

4. Para cada política *inactive*, edítela o elimínela seleccionando primero el enlace para cada política como se describe en los pasos anteriores.
   - "Edite la política" por lo tanto, no se refiere al sitio que se va a retirar.
   - "Eliminar una política".
5. Cuando termine de realizar cambios en las reglas y políticas de ILM, no debe haber más políticas en el paso 3 (revisar políticas de ILM). Seleccione **Siguiente**.

   Aparece el paso 4 (Eliminar referencias de ILM).

Paso 4: Eliminar referencias de ILM

En el paso 4 (Eliminar referencias de ILM) del asistente del sitio de retirada, debe eliminar o editar las reglas de ILM no utilizadas que hagan referencia al sitio, incluso si las reglas no se usan en ninguna política de ILM.

Pasos

1. Determine si alguna regla de ILM sin usar se refiere al sitio.

   Si aparece alguna regla de ILM, esas reglas siguen refiriéndose al sitio, pero no se utilizan en ninguna política.

Cuando StorageGRID decomisiona el sitio, desactivará automáticamente todos los perfiles de código de borrado no utilizados que hagan referencia al sitio y eliminará automáticamente los grupos de almacenamiento no utilizados que hagan referencia al sitio. El pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores) se elimina porque utiliza el sitio Todos los sitios.

2. Edite o elimine cada regla no utilizada:
   - Para editar una regla, vaya a la página de reglas de ILM y actualice todas las ubicaciones con un perfil de código de borrado o un pool de almacenamiento que haga referencia al sitio. A continuación, vuelva a **Paso 4 (Eliminar referencias de ILM)**.
   - Para eliminar una regla, seleccione el icono de papelera Y seleccione **OK**.

     Debe eliminar la regla **Hacer 2 copias** antes de poder retirar un sitio.

3. Confirme que ninguna regla de ILM no utilizada hace referencia al sitio y que el botón **Siguiente** está habilitado.
4. Seleccione **Siguiente**.

   Los pools de almacenamiento restantes y los perfiles de codificación de borrado que hagan referencia al sitio dejarán de ser válidos cuando se elimine el sitio. Cuando StorageGRID decomisiona el sitio, desactivará automáticamente todos los perfiles de código de borrado no utilizados que hagan referencia al sitio y eliminará automáticamente los grupos de almacenamiento no utilizados que hagan referencia al sitio. El pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores) se elimina porque utiliza el sitio Todos los sitios.

   Aparece el paso 5 (resolver conflictos de nodos).

Paso 5: Resolver conflictos de nodos (e iniciar retirada)

En el paso 5 (resolver conflictos de nodos) del asistente para sitio de retirada, puede determinar si alguno de los nodos del sistema StorageGRID está desconectado o si alguno de los nodos del sitio seleccionado pertenece a un grupo de alta disponibilidad (ha). Después de resolver cualquier conflicto de nodo, se inicia el procedimiento de retirada desde esta página.

Antes de empezar

Debe asegurarse de que todos los nodos del sistema StorageGRID tengan el estado correcto, de la siguiente manera:

- Todos los nodos del sistema StorageGRID deben estar conectados ( ).

  Si está realizando una retirada de sitios desconectada, todos los nodos del sitio que va a quitar deben estar desconectados y todos los nodos del resto de sitios deben estar conectados.

  La retirada no se iniciará si uno o más volúmenes están sin conexión (sin montar) o si están en línea (montados), pero en estado de error.

Si uno o más volúmenes quedan sin conexión mientras existe una decomisión en curso, el proceso de decomiso se completa una vez que estos volúmenes vuelvan a estar en línea.

- Ningún nodo del sitio que va a quitar puede tener una interfaz que pertenezca a un grupo de alta disponibilidad.

Acerca de esta tarea

Si alguno de los nodos aparece en la lista del paso 5 (resolver conflictos de nodos), debe corregir el problema antes de poder iniciar la retirada.

Antes de iniciar el procedimiento de retirada del sitio desde esta página, revise las siguientes consideraciones:

- Debe dejar tiempo suficiente para completar el procedimiento de retirada.

La transferencia o eliminación de datos de objetos de un sitio puede llevar días, semanas o incluso meses, en función de la cantidad de datos almacenados en el sitio, la carga en el sistema, las latencias de red y la naturaleza de los cambios de ILM necesarios.

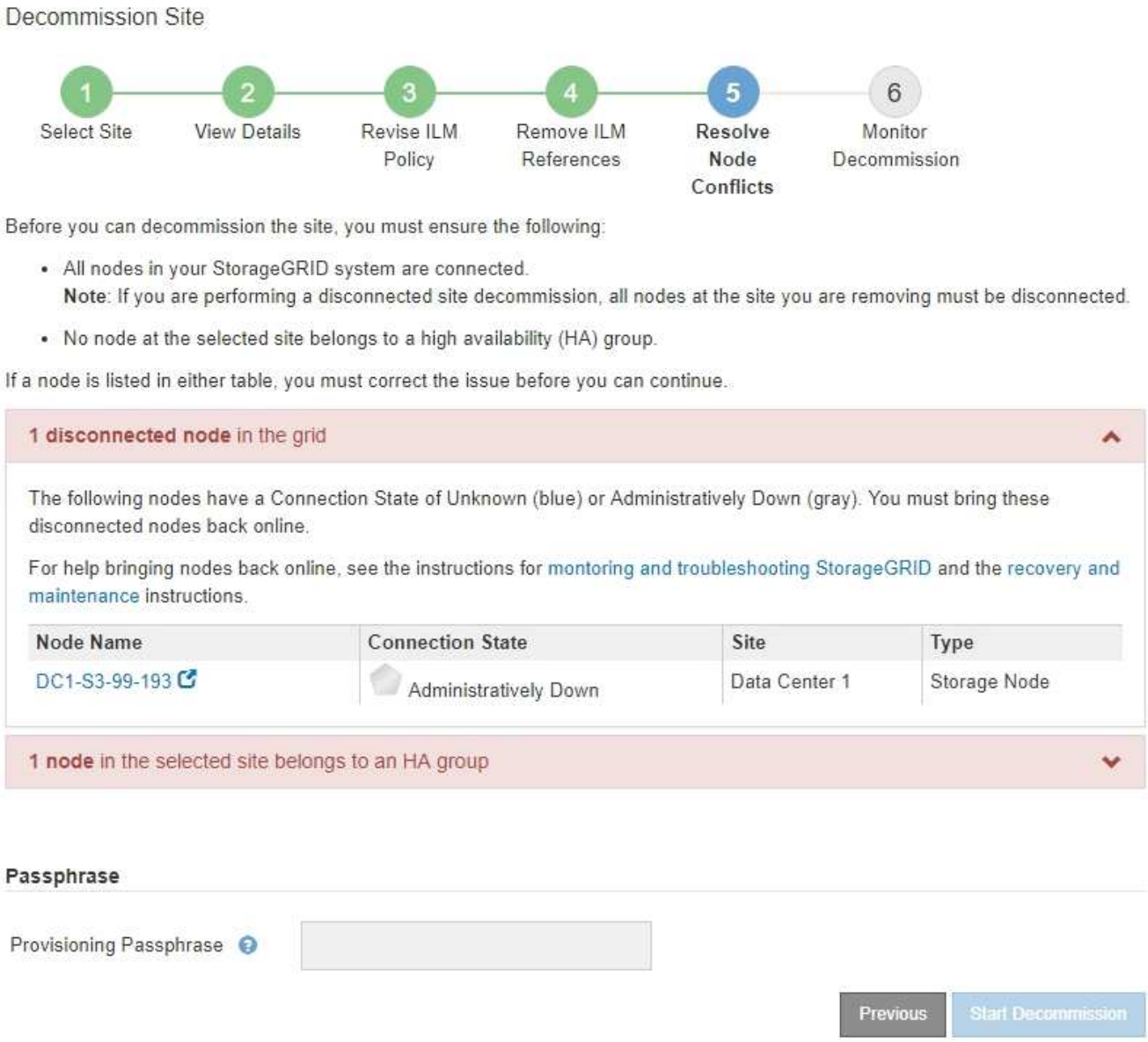
- Mientras se está ejecutando el procedimiento de retirada de instalaciones:
  - No se pueden crear reglas de ILM que hagan referencia al sitio que se va a retirar. Tampoco puede editar una regla de ILM existente para hacer referencia al sitio.
  - No se pueden llevar a cabo otros procedimientos de mantenimiento, como la ampliación o la actualización.

Si necesita realizar otro procedimiento de mantenimiento durante un desmantelamiento de un sitio conectado, puede pausar el procedimiento mientras se quitan los nodos de almacenamiento. El botón **Pausa** está habilitado durante la etapa “Descomisionado de Datos Replicados y con Código de Borrado”.

  - Si necesita recuperar algún nodo después de iniciar el procedimiento de retirada del sitio, debe ponerse en contacto con el servicio de soporte de.

Pasos

1. Revise la sección nodos desconectados del paso 5 (resolver conflictos de nodos) para determinar si alguno de los nodos del sistema StorageGRID tiene un estado de conexión desconocido ( ) O administrativamente abajo ( ).

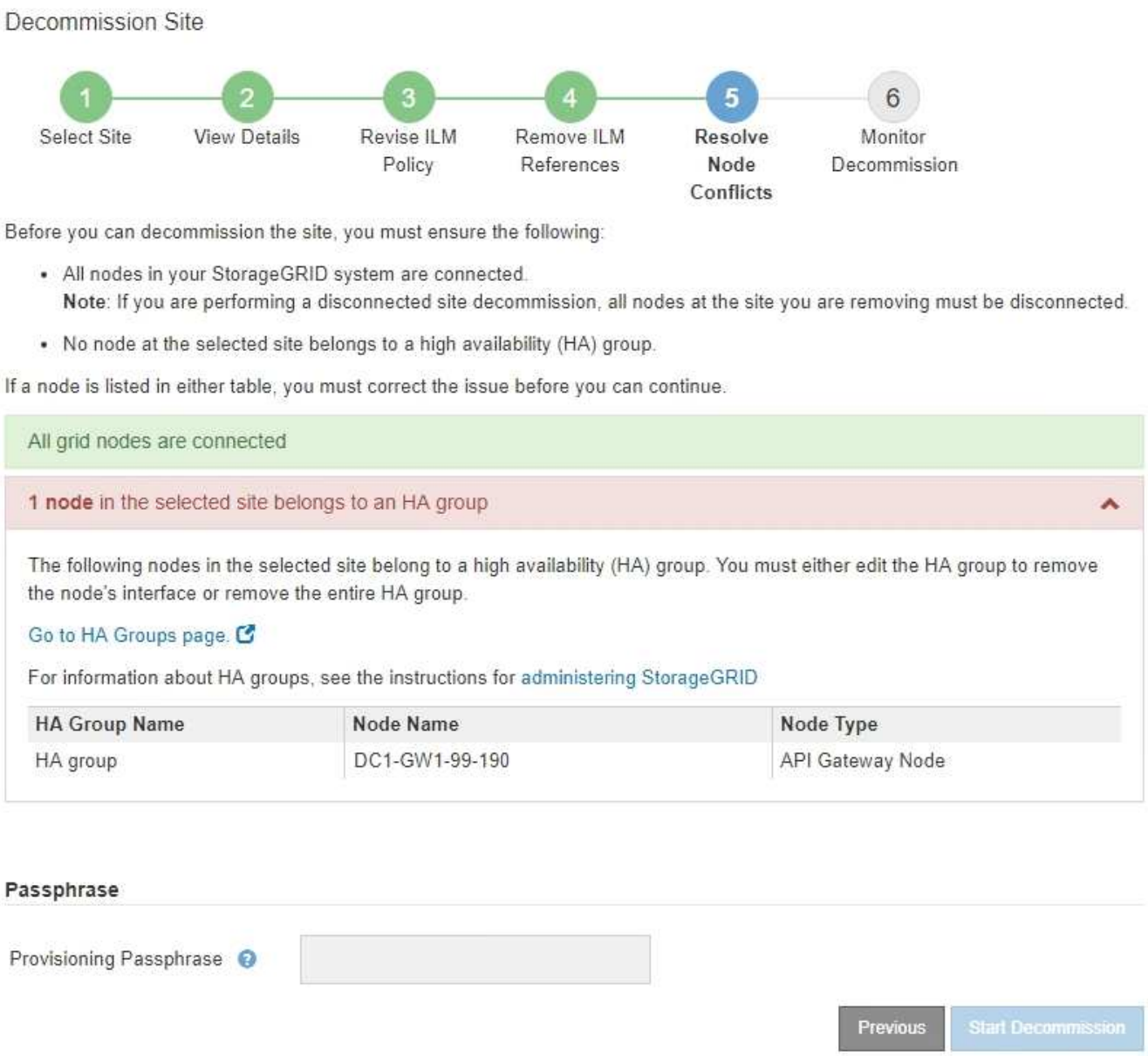


2. Si alguno de los nodos está desconectado, vuelva a ponerlos en línea.

   Consulte "Procedimientos de nodo". Si necesita ayuda, póngase en contacto con el soporte técnico.

3. Cuando todos los nodos desconectados hayan vuelto a estar en línea, revise la sección de grupos de alta disponibilidad del paso 5 (resolver conflictos de nodos).

   En esta tabla se enumeran los nodos del sitio seleccionado que pertenecen a un grupo de alta disponibilidad.

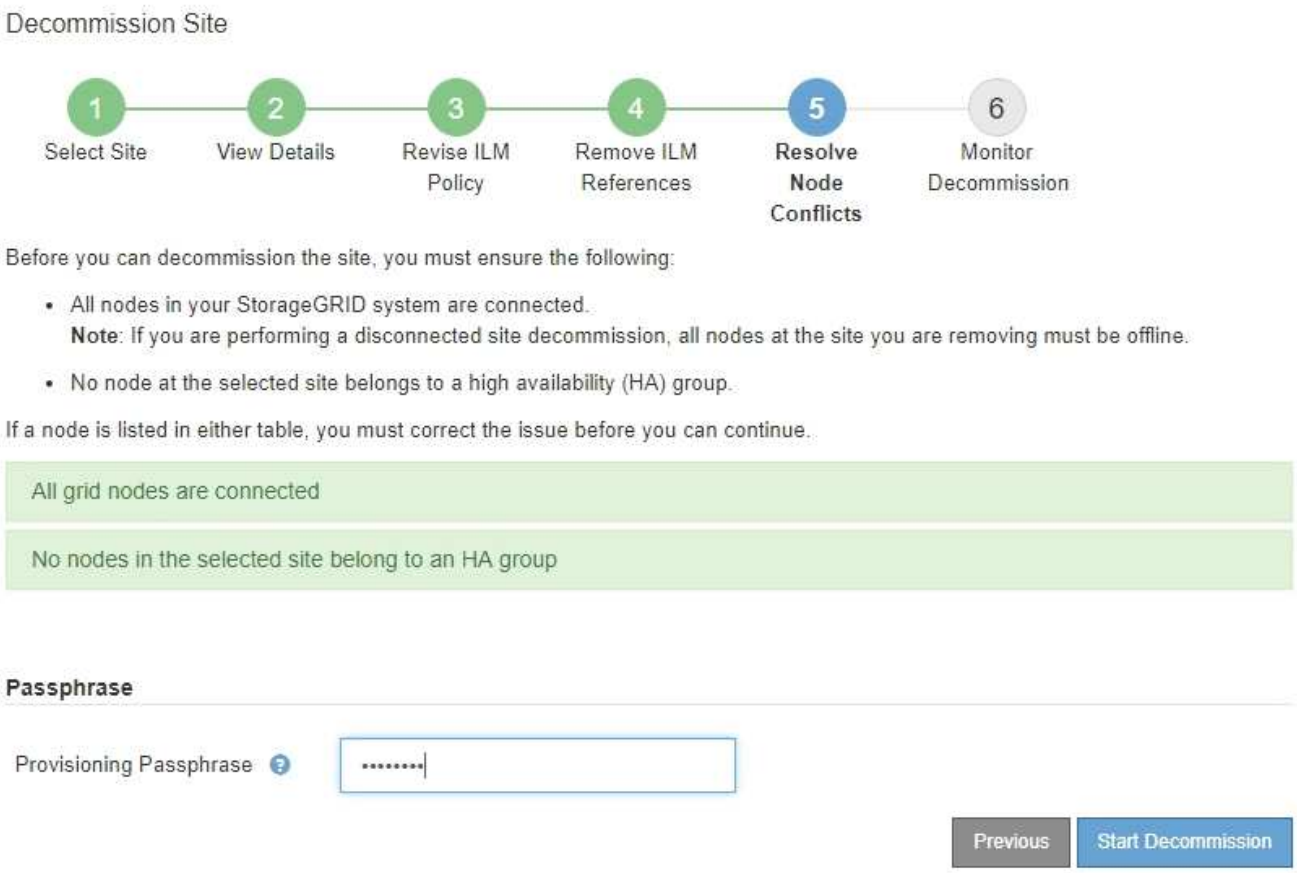


4. Si aparece algún nodo, realice una de las siguientes acciones:
   - Edite cada grupo de alta disponibilidad afectado para quitar la interfaz del nodo.
   - Quite un grupo de alta disponibilidad que solo incluye nodos de este sitio.
     Consulte las instrucciones para administrar StorageGRID.

   Si todos los nodos están conectados y no se utiliza ningún nodo en el sitio seleccionado en un grupo ha, se activa el campo **frase de paso** de aprovisionamiento.

5. Introduzca la clave de acceso de aprovisionamiento.

   El botón **Iniciar misión** se activa.

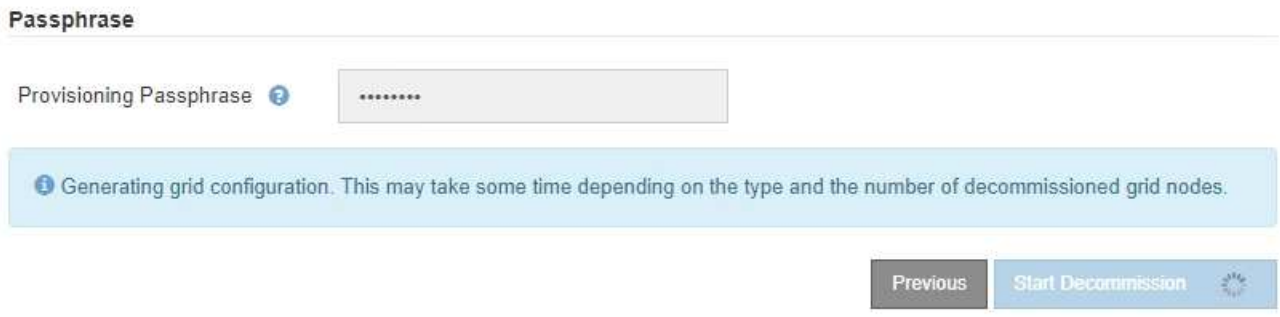


6. Si está listo para iniciar el procedimiento de retirada del sitio, seleccione **Iniciar misión**.

   Una advertencia indica el sitio y los nodos que se van a quitar. Se le recuerda que puede tardar días, semanas o incluso meses en eliminar completamente el sitio.

7. Revise la advertencia. Si está listo para comenzar, seleccione **Aceptar**.

   Aparece un mensaje cuando se genera la nueva configuración de cuadrícula. Este proceso puede tardar algún tiempo, dependiendo del tipo y el número de nodos de cuadrícula que se retiraron.



   Cuando se ha generado la nueva configuración de cuadrícula, aparece el paso 6 (retirada del monitor).

   El botón **anterior** permanece desactivado hasta que se completa la retirada.

Paso 6: Supervisión de la misión

En el paso 6 (Supervisión de misión) del asistente de página Sitio de retirada, puede supervisar el progreso a medida que se quita el sitio.

Acerca de esta tarea

Cuando StorageGRID quita un sitio conectado, quita los nodos en el siguiente orden:

1. Nodos de puerta de enlace
2. Nodos de administración
3. Nodos de almacenamiento

Cuando StorageGRID quita un sitio desconectado, quita los nodos en el siguiente orden:

1. Nodos de puerta de enlace
2. Nodos de almacenamiento
3. Nodos de administración

Es posible que cada nodo de puerta de enlace o nodo de administrador solo requiera unos minutos o una hora; sin embargo, los nodos de almacenamiento pueden tardar días o semanas.

Pasos

1. Tan pronto como se haya generado un nuevo paquete de recuperación, descargue el archivo.

> Descargue el Lo antes posible. del paquete de recuperación para asegurarse de que puede recuperar la red si hay algún problema durante el procedimiento de retirada de servicio.

   a. Seleccione el enlace en el mensaje o seleccione **MANTENIMIENTO** > **Sistema** > **Paquete de recuperación**.

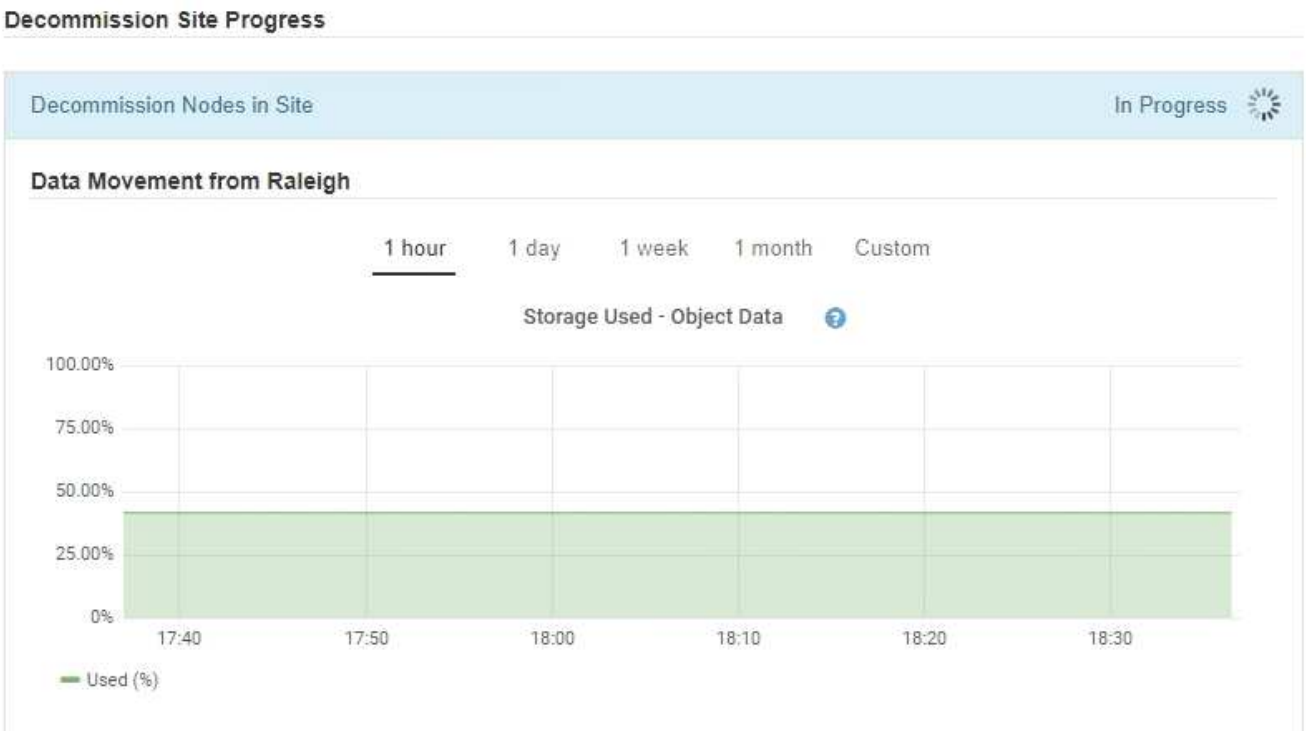
   b. Descargue el `.zip` archivo.

      Consulte las instrucciones para "Descarga del paquete de recuperación".

> El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

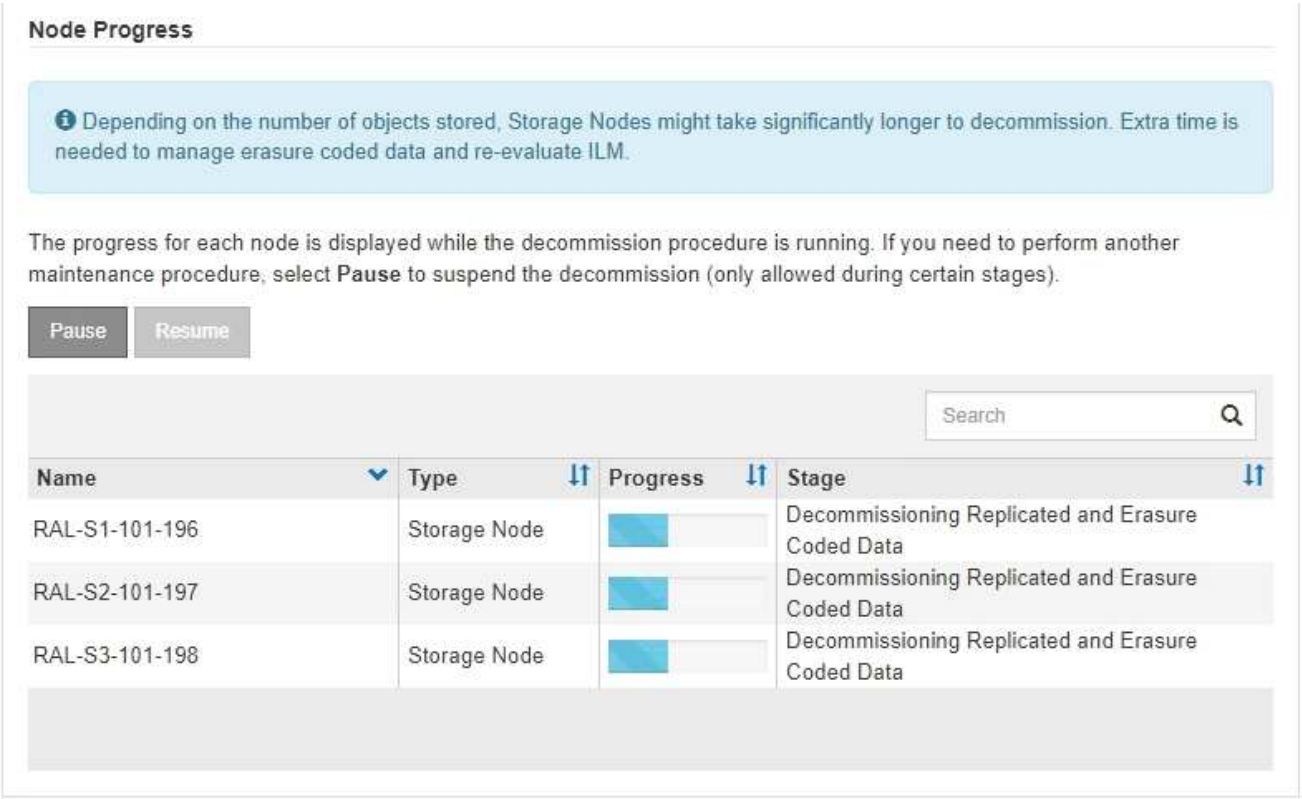
2. Con el gráfico de movimiento de datos, supervise el movimiento de datos de objetos desde este sitio a otros sitios.

El movimiento de datos se inició cuando se activó la nueva política de ILM en el paso 3 (revisar política de ILM). El movimiento de datos se realizará durante todo el procedimiento de retirada de servicio.



3. En la sección progreso de nodos de la página, supervise el progreso del procedimiento de retirada a medida que se quitan los nodos.

   Cuando se elimina un nodo de almacenamiento, cada nodo pasa por una serie de etapas. Aunque la mayoría de estas fases se dan de forma rápida o incluso imperceptible, es posible que tenga que esperar días o incluso semanas para que se completen otras fases, en función de la cantidad de datos necesarios que se vayan a mover. Se necesita tiempo adicional para gestionar datos codificados de borrado y volver a evaluar la ILM.



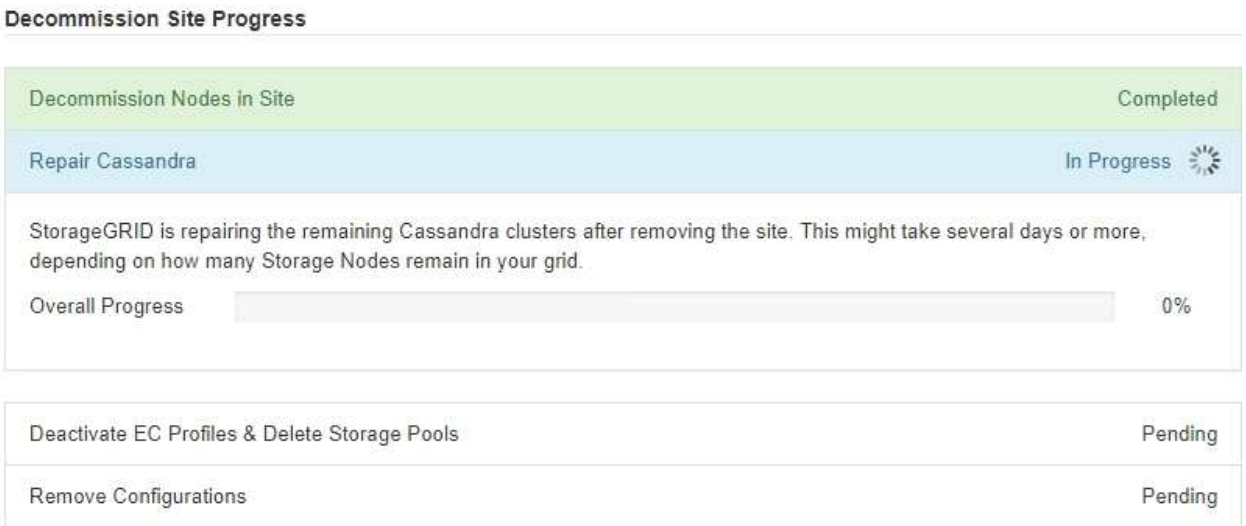
Si va a supervisar el progreso de una retirada de sitios conectados, consulte esta tabla para comprender las etapas de retirada de un nodo de almacenamiento:

Etapa	Duración estimada
Pendiente	Minuto o menos
Espere a que se bloqueen	Minutos
Preparar tarea	Minuto o menos
Marcado de LDR retirado	Minutos
Retirada de datos replicados y con código de borrado	Horas, días o semanas en función de la cantidad de datos **Nota**: Si necesita realizar otras actividades de mantenimiento, puede hacer una pausa en la retirada del sitio durante esta fase.
Estado del conjunto LDR	Minutos
Eliminar colas de auditoría	De minutos a horas, según el número de mensajes y la latencia de la red.
Completo	Minutos

Si va a supervisar el progreso de una retirada de sitios desconectada, consulte esta tabla para comprender las etapas de retirada de un nodo de almacenamiento:

Etapa	Duración estimada
Pendiente	Minuto o menos
Espere a que se bloqueen	Minutos
Preparar tarea	Minuto o menos
Desactive Servicios externos	Minutos
Revocación de certificados	Minutos
Unregister Node	Minutos
Registro de grado de almacenamiento	Minutos
Extracción del grupo de almacenamiento	Minutos
Eliminación de entidades	Minutos
Completo	Minutos

4. Una vez que todos los nodos hayan alcanzado la fase completa, espere a que se completen las operaciones de retirada del sitio restantes.
   - Durante el paso **reparar Cassandra**, StorageGRID realiza las reparaciones necesarias a los clústeres Cassandra que permanecen en la cuadrícula. Estas reparaciones pueden tardar varios días o más, según la cantidad de nodos de almacenamiento que haya en el grid.

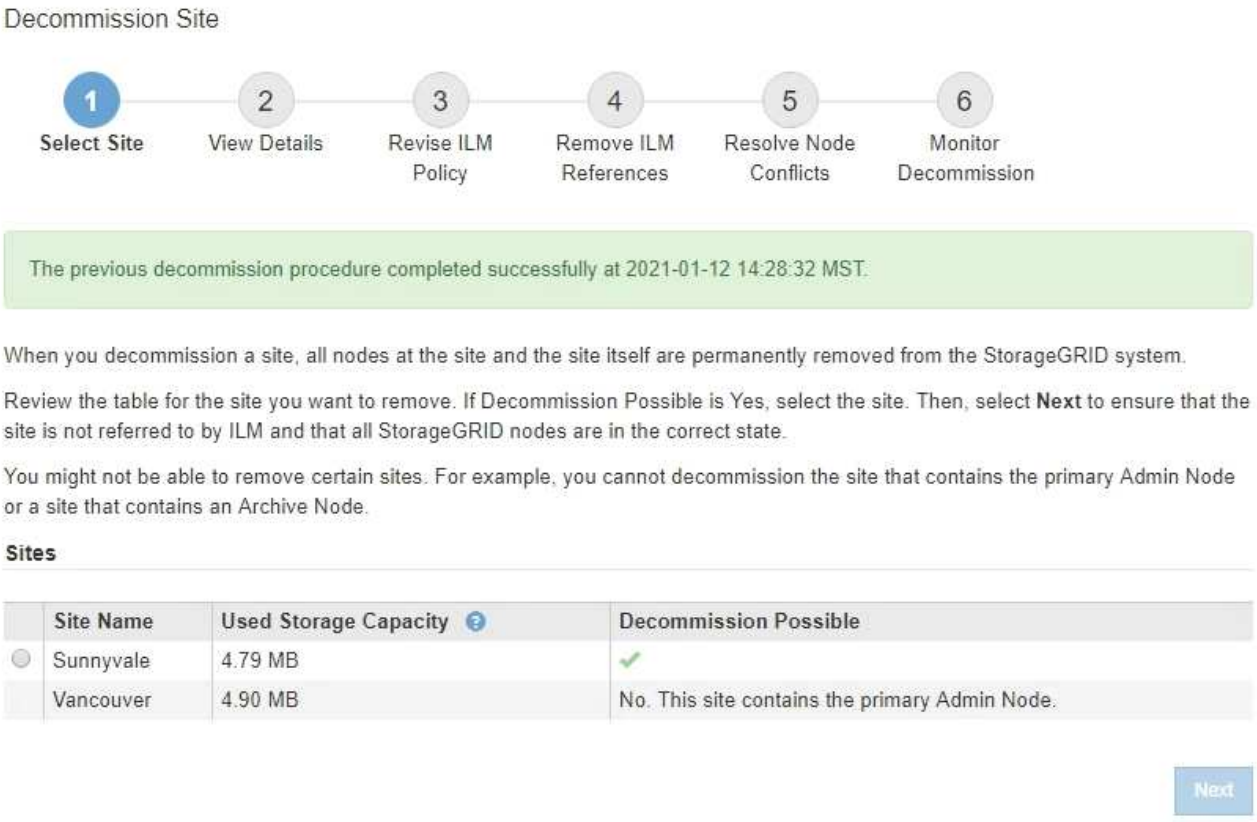


   - Durante el paso **Desactivar perfiles de EC y Eliminar grupos de almacenamiento**, se realizan los siguientes cambios de ILM:
     - Se desactivan los perfiles de código de borrado que hacen referencia al sitio.
     - Los pools de almacenamiento a los que se hace referencia el sitio se eliminan.

El pool de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11,6 y anteriores) también se elimina porque utiliza el sitio Todos los sitios.

- Finalmente, durante el paso **Eliminar configuración**, cualquier referencia restante al sitio y sus nodos se quita del resto de la cuadrícula.

5. Una vez completado el procedimiento de retirada, la página Sitio de retirada muestra un mensaje de éxito y el sitio eliminado ya no se muestra.



Después de terminar

Complete estas tareas después de completar el procedimiento de retirada del sitio:

- Asegúrese de que las unidades de todos los nodos de almacenamiento del sitio donde se decomisionó se limpias. Utilice una herramienta o servicio de limpieza de datos disponible en el mercado para eliminar los

datos de las unidades de forma permanente y segura.

- Si el sitio incluye uno o más nodos de administración y el inicio de sesión único (SSO) está habilitado para el sistema StorageGRID, elimine todas las confianzas de partes que dependan del sitio de los Servicios de Federación de Active Directory (AD FS).
- Una vez que los nodos se han apagado automáticamente como parte del procedimiento de retirada del sitio conectado, quite las máquinas virtuales asociadas.

Cambie el nombre de cuadrícula, sitio o nodo

Renombrar cuadrícula, sitios y nodos: Descripción general

Según sea necesario, puede cambiar los nombres mostrados en Grid Manager para toda la cuadrícula, cada sitio y cada nodo. Puede actualizar los nombres mostrados de forma segura y siempre que lo necesite.

¿Qué es el procedimiento de cambio de nombre?

Cuando se instala StorageGRID inicialmente, se especifica un nombre para la cuadrícula, cada sitio y cada nodo. Estos nombres iniciales se conocen como *nombres del sistema*, y son los nombres mostrados inicialmente en StorageGRID.

Los nombres del sistema son necesarios para las operaciones internas de StorageGRID y no se pueden cambiar. Sin embargo, puede utilizar el procedimiento de cambio de nombre para definir nuevos *nombres de visualización* para la cuadrícula, cada sitio y cada nodo. Estos nombres mostrados aparecen en varias ubicaciones de StorageGRID en lugar de (o en algunos casos, además de) los nombres del sistema subyacentes.

Utilice el procedimiento de cambio de nombre para corregir errores tipográficos, para implementar una convención de nomenclatura diferente o para indicar que se han reubicado un sitio y todos sus nodos. A diferencia de los nombres del sistema, los nombres para mostrar se pueden actualizar siempre que sea necesario y sin afectar a las operaciones de StorageGRID.

¿Dónde aparecen los nombres del sistema y de visualización?

En la siguiente tabla se resume dónde se muestran los nombres del sistema y los nombres mostrados en la interfaz de usuario de StorageGRID y en los archivos StorageGRID.

Ubicación	Nombre del sistema	Nombre para mostrar
Páginas de Grid Manager	Se muestra a menos que se cambie el nombre del elemento	Si se cambia el nombre de un elemento, se muestra en lugar del nombre del sistema en estas ubicaciones: • Consola • Nodos • Páginas de configuración para grupos de alta disponibilidad, extremos del equilibrador de carga, interfaces VLAN, servidores de gestión de claves, contraseñas de grid y control de firewall • Alertas • Definiciones de pools de almacenamiento • Página de consulta de metadatos de objetos • Páginas relacionadas con procedimientos de mantenimiento, incluidas actualización, corrección urgente, actualización de SANtricity OS, retirada, comprobación de expansión, recuperación y existencia de objetos • Páginas de soporte (registros y diagnósticos) • Página Single Sign-On, junto al nombre de host del nodo de administración en la tabla para los detalles del nodo de administración
NODOS > pestaña **Overview** para un nodo	Siempre se muestra	Sólo se muestra si se cambia el nombre del elemento
Páginas heredadas en Grid Manager (por ejemplo, **SUPPORT** > **Grid Topology**)	Se muestra	No se muestra
Node-health API	Siempre devuelto	Devuelto sólo si se cambia el nombre del elemento

Ubicación	Nombre del sistema	Nombre para mostrar

Prompt cuando se utiliza SSH para acceder a un nodo	Se muestra como nombre principal a menos que se haya cambiado el nombre del elemento:
	
	`admin@SYSTEM-NAME: ~ $`
	
	Se incluye entre paréntesis cuando se cambia el nombre del elemento:
	
	`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`
		Se muestra como nombre principal cuando se cambia el nombre del elemento:
		
		`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`

`Passwords.txt` En el paquete de recuperación	Se muestra como `Server Name`	Se muestra como `Display Name`
`/etc/hosts` en todos los nodos Por ejemplo: `10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host`	Siempre se muestra en la segunda columna	Cuando se cambia el nombre del elemento, se muestra en la cuarta columna
`topology-display-names.json`, Incluido con los datos de AutoSupport	No incluido	Vacío a menos que se haya cambiado el nombre de los elementos; de lo contrario, asigna los ID de cuadrícula, sitio y nodo a sus nombres mostrados.

Requisitos de nombre para mostrar

Antes de utilizar este procedimiento, revise los requisitos para los nombres mostrados.

Nombres mostrados de los nodos

Los nombres mostrados de los nodos deben seguir estas reglas:

- Debe ser único en todo el sistema StorageGRID.
- No puede ser el mismo que el nombre del sistema para cualquier otro elemento del sistema StorageGRID.
- Debe contener al menos 1 y no más de 32 caracteres.
- Puede contener números, guiones (-) y letras mayúsculas y minúsculas.
- Puede comenzar o terminar con una letra o un número, pero no puede comenzar ni terminar con un guion.

- No puede ser todos los números.
- No son sensibles a mayúsculas/minúsculas. Por ejemplo: `DC1-ADM` y.. `dc1-adm` se consideran duplicados.

Puede cambiar el nombre de un nodo con un nombre mostrado que anteriormente utilizaba otro nodo, siempre y cuando el cambio de nombre no tenga como resultado un nombre mostrado duplicado o un nombre de sistema.

Nombres mostrados para cuadrícula y sitios

Los nombres mostrados para la cuadrícula y los sitios siguen las mismas reglas con estas excepciones:

- Puede incluir espacios.
- Puede incluir estos caracteres especiales: `= - _ : , . @ !`
- Puede comenzar y terminar con los caracteres especiales, incluidos los guiones.
- Puede ser todos los números o caracteres especiales.

Mostrar las mejores prácticas de nombres

Si tiene pensado cambiar el nombre de varios elementos, documente el esquema de nomenclatura general antes de utilizar este procedimiento. Crea un sistema que garantice que los nombres sean únicos, consistentes y fáciles de entender de un vistazo.

Puede utilizar cualquier convención de nomenclatura que se ajuste a los requisitos de su organización. Considere estas sugerencias básicas de lo que incluir:

- **Indicador del sitio**: Si tiene varios sitios, agregue un código de sitio a cada nombre de nodo.
- **Tipo de nodo**: Los nombres de nodo suelen indicar el tipo del nodo. Puede utilizar abreviaturas como `s`, `adm`, `gw`, y. `arc` (Nodo de almacenamiento, nodo de administración, nodo de puerta de enlace y nodo de archivado).
- **Número de nodo**: Si un sitio contiene más de uno de un tipo de nodo en particular, agregue un número único al nombre de cada nodo.

Piense dos veces antes de agregar detalles específicos a los nombres que probablemente cambien con el tiempo. Por ejemplo, no incluya direcciones IP en los nombres de nodos porque estas direcciones se pueden cambiar. Del mismo modo, la ubicación de los bastidores o los números de modelo de los dispositivos pueden cambiar si mueve el equipo o actualiza el hardware.

Nombres mostrados de ejemplo

Supongamos que su sistema StorageGRID tiene tres centros de datos y tiene nodos de diferentes tipos en cada centro de datos. Los nombres mostrados pueden ser tan simples como los siguientes:

- **Grid**: `StorageGRID Deployment`
- **Primer sitio**: `Data Center 1`
  - `dc1-adm1`
  - `dc1-s1`
  - `dc1-s2`

- dc1-s3
- dc1-gw1

- **Segundo sitio**: `Data Center 2`
  - dc2-adm2
  - dc2-s1
  - dc2-s2
  - dc2-s3
- **Tercer sitio**: `Data Center 3`
  - dc3-s1
  - dc3-s2
  - dc3-s3

Agregar o actualizar nombres mostrados

Puede utilizar este procedimiento para agregar o actualizar los nombres mostrados utilizados para la cuadrícula, las ubicaciones y los nodos. Puede cambiar el nombre de un único elemento, varios elementos o incluso todos los elementos al mismo tiempo. La definición o actualización de un nombre mostrado no afecta de ninguna manera a las operaciones de StorageGRID.

Antes de empezar

- Desde el **nodo de administración principal**, ha iniciado sesión en Grid Manager mediante un "navegador web compatible".

> Puede agregar o actualizar nombres mostrados de un nodo de administración no principal, pero debe iniciar sesión en el nodo de administración principal para descargar un paquete de recuperación.

- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento.
- Comprende los requisitos y las prácticas recomendadas para los nombres mostrados. Consulte "Renombrar cuadrícula, sitios y nodos: Descripción general".

Cómo cambiar el nombre de cuadrícula, sitios o nodos

Puede cambiar el nombre del sistema StorageGRID, de uno o más sitios, o de uno o varios nodos.

Puede utilizar un nombre mostrado utilizado anteriormente por un nodo diferente, siempre y cuando el cambio de nombre no dé como resultado un nombre mostrado duplicado o un nombre del sistema.

Seleccione los elementos para cambiar el nombre

Para comenzar, seleccione los elementos cuyo nombre desea cambiar.

Pasos

1. Selecciona **MANTENIMIENTO** > **Tareas** > **Cambiar nombre de cuadrícula, sitios y nodos**.
2. Para el paso **Seleccionar nombres**, selecciona los elementos a los que quieres cambiar el nombre.

Elemento para cambiar	Instrucción
Nombres de todo (o casi todo) en su sistema	a. Selecciona **Seleccionar todo**. b. Opcionalmente, borre los elementos a los que no desee cambiar el nombre.
Nombre de la cuadrícula	Seleccione la casilla de verificación de la cuadrícula.
Nombre de un sitio y algunos o todos sus nodos	a. Seleccione la casilla de verificación en el encabezado de la tabla para el sitio. b. Opcionalmente, borre los nodos a los que no quiera cambiar el nombre.
Nombre de un sitio	Seleccione la casilla de verificación para el sitio.
El nombre de un nodo	Seleccione la casilla de comprobación del nodo.

3. Seleccione **continuar**.
4. Revise la tabla, que incluye los elementos seleccionados.
   - La columna **Nombre de visualización** muestra el nombre actual de cada elemento. Si el elemento nunca se ha cambiado de nombre, su nombre mostrado es el mismo que su nombre de sistema.
   - La columna **Nombre del sistema** muestra el nombre que ingresó para cada elemento durante la instalación. Los nombres del sistema se utilizan para operaciones internas de StorageGRID y no se pueden cambiar. Por ejemplo, el nombre del sistema para un nodo podría ser su nombre de host.
   - La columna **Type** indica el tipo de elemento: Grid, Site, o el tipo específico de nodo.

Proponer nuevos nombres

Para el paso **Proponer nuevos nombres**, puede introducir un nombre para mostrar para cada elemento individualmente, o puede cambiar el nombre de los elementos a granel.

Cambiar el nombre de los elementos individualmente

Siga estos pasos para introducir un nombre mostrado para cada elemento que desee cambiar de nombre.

Pasos

1. En el campo **Nombre para mostrar**, introduzca un nombre para mostrar propuesto para cada elemento de la lista.

   Consulte "Renombrar cuadrícula, sitios y nodos: Descripción general" para aprender los requisitos de nomenclatura.

2. Para eliminar cualquier elemento que no desee cambiar de nombre, seleccione ✕ En la columna **Remove from list**.

   Si no va a proponer un nuevo nombre para un elemento, debe eliminarlo de la tabla.

3. Cuando haya propuesto nuevos nombres para todos los elementos de la tabla, seleccione **Renombrar**.

   Aparece un mensaje de éxito. Los nuevos nombres mostrados se utilizan ahora en Grid Manager.

Cambiar el nombre de los elementos en bloque

Utilice la herramienta de cambio de nombre masivo si los nombres de elementos comparten una cadena común que desea reemplazar con una cadena diferente.

Pasos

1. Para el paso **Proponer nuevos nombres**, selecciona **Usar herramienta de cambio de nombre masivo**.

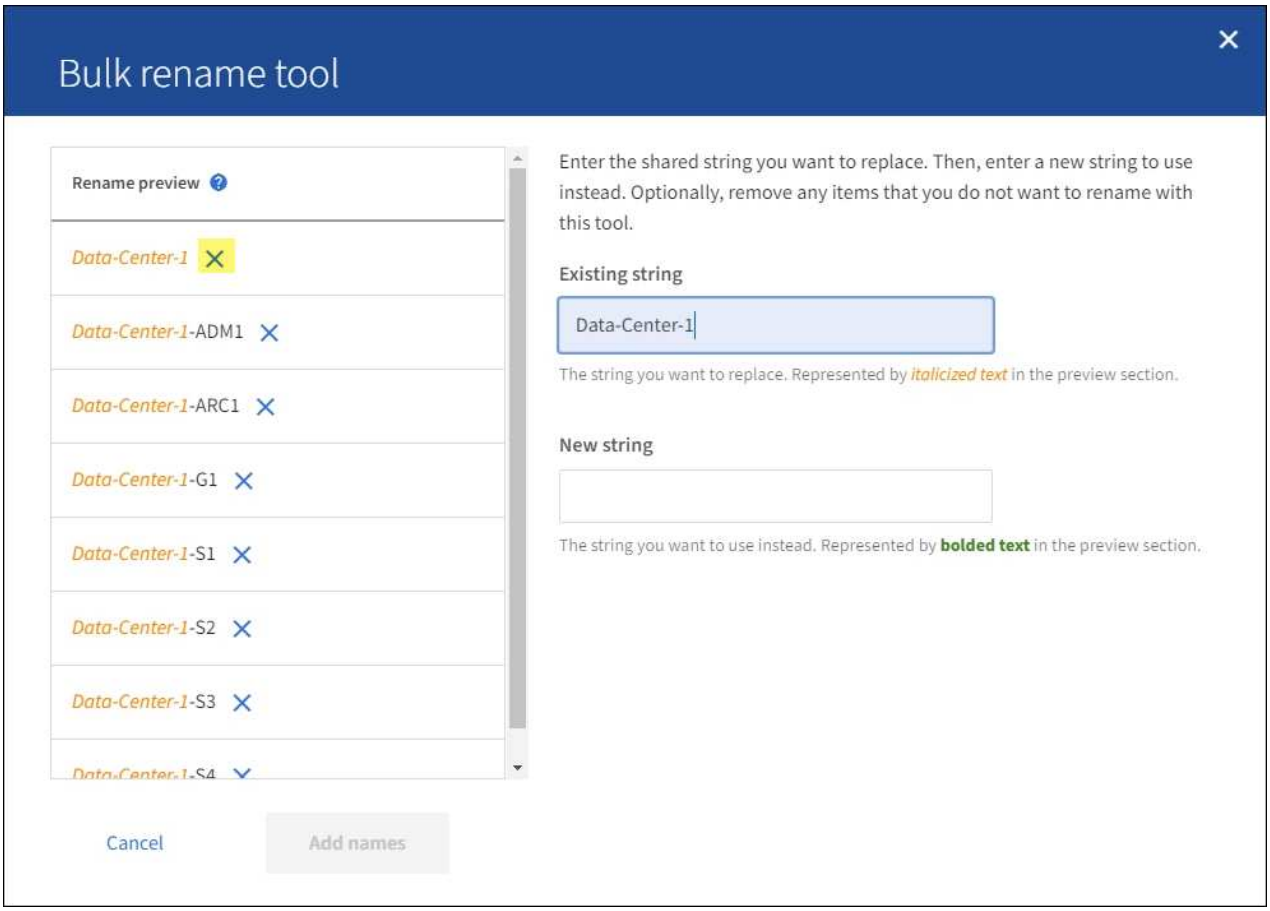
   El **Rename preview** incluye todos los elementos que se mostraron para el paso **Proponer nuevos nombres**. Puede utilizar la vista previa para ver el aspecto que tendrán los nombres mostrados después de reemplazar una cadena compartida.

2. En el campo **cadena existente**, introduzca la cadena compartida que desea reemplazar. Por ejemplo, si la cadena que desea reemplazar es `Data-Center-1`, Introduzca **Data-Center-1**.

   A medida que escribe, el texto se resalta donde se encuentre en los nombres de la izquierda.

3. Seleccione ✕ para eliminar cualquier elemento que no desee cambiar de nombre con esta herramienta.

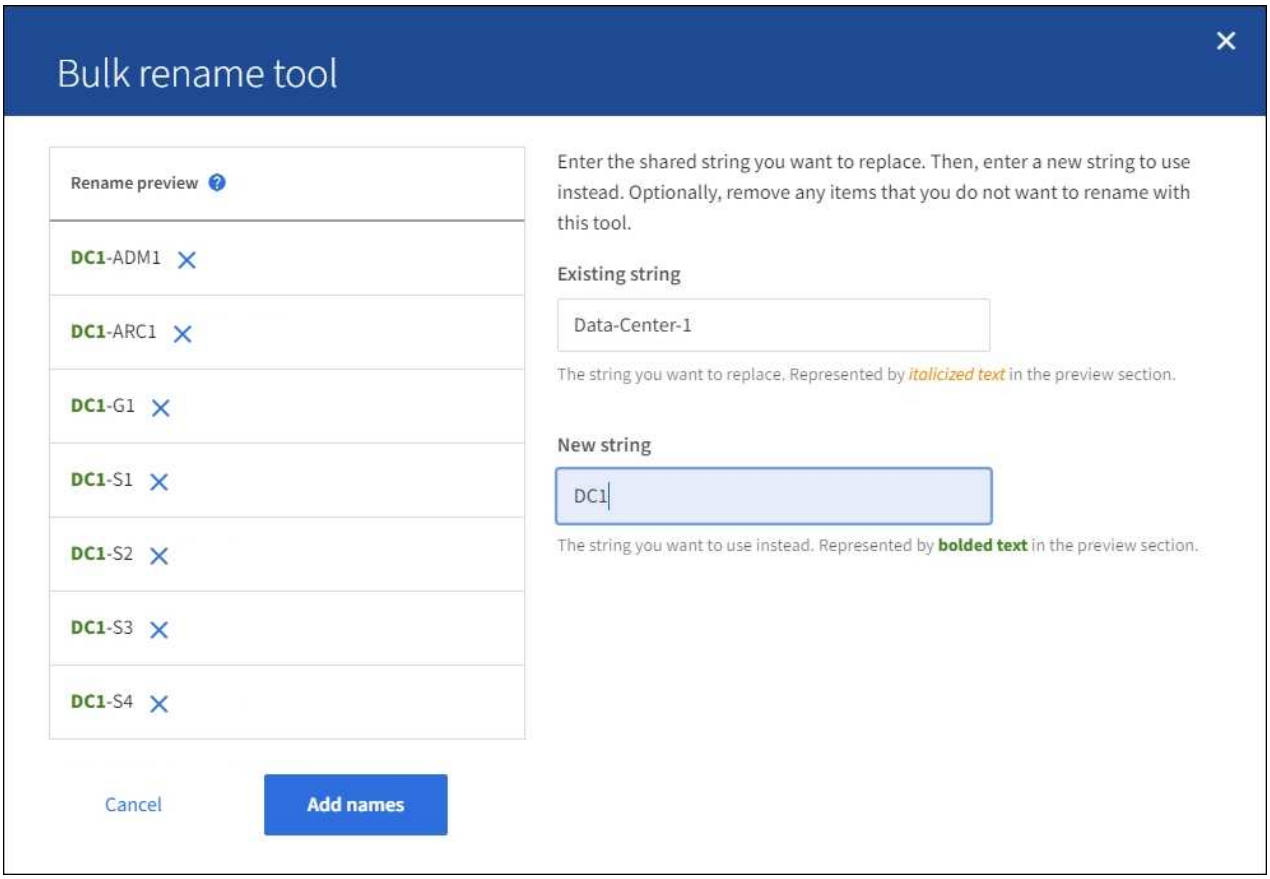
   Por ejemplo, suponga que desea cambiar el nombre de todos los nodos que contienen la cadena `Data-Center-1`, pero no desea cambiar el nombre del `Data-Center-1` sitio en sí. Seleccione ✕ para eliminar el sitio de la vista previa de cambio de nombre.



4. En el campo **New string**, ingresa la cadena de reemplazo que deseas usar en su lugar. Por ejemplo, introduzca **DC1**.

   Consulte "Renombrar cuadrícula, sitios y nodos: Descripción general" para aprender los requisitos de nomenclatura.

   Al introducir la cadena de sustitución, los nombres de la izquierda se actualizan, de modo que puede verificar que los nuevos nombres sean correctos.



5. Cuando esté satisfecho con los nombres mostrados en la vista previa, seleccione **Agregar nombres** para agregar los nombres a la tabla para el paso **Proponer nuevos nombres**.
6. Realice los cambios adicionales necesarios o seleccione ✕ para eliminar cualquier elemento que no desee cambiar de nombre.
7. Cuando esté listo para cambiar el nombre de todos los elementos de la tabla, seleccione **Cambiar nombre**.

   Se muestra un mensaje de éxito. Los nuevos nombres mostrados se utilizan ahora en Grid Manager.

Descargue el paquete de recuperación

Cuando haya terminado de cambiar el nombre de los elementos, descargue y guarde un nuevo paquete de recuperación. Los nuevos nombres de visualización para los elementos a los que ha cambiado el nombre se incluyen en la `Passwords.txt` archivo.

Pasos

1. Introduzca la clave de acceso de aprovisionamiento.
2. Seleccione **Descargar paquete de recuperación**.

   La descarga comienza inmediatamente.

3. Cuando finalice la descarga, abra la `Passwords.txt` archivo para ver el nombre del servidor de todos los nodos y los nombres mostrados de los nodos renombrados.
4. Copie el `sgws-recovery-package-`*`id-revision`*`.zip` archivo en dos ubicaciones seguras, seguras y separadas.

El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

5. Selecciona **Finalizar** para volver al primer paso.

Revierte los nombres mostrados a los nombres del sistema

Puede revertir una cuadrícula, un sitio o un nodo cuyo nombre ha cambiado de nombre al sistema original. Al revertir un elemento a su nombre de sistema, las páginas del Administrador de grid y otras ubicaciones de StorageGRID ya no muestran un **Nombre mostrado** para ese elemento. Sólo se muestra el nombre del sistema del elemento.

Pasos

1. Selecciona **MANTENIMIENTO** > **Tareas** > **Cambiar nombre de cuadrícula, sitios y nodos**.
2. Para el paso **Seleccionar nombres**, selecciona cualquier elemento que quieras volver a los nombres del sistema.
3. Seleccione **continuar**.
4. Para el paso **Proponer nuevos nombres**, revierta los nombres mostrados de nuevo a los nombres del sistema individualmente o en bloque.

Vuelva a los nombres del sistema de forma individual

a. Copie el nombre original del sistema de cada elemento y péguelo en el campo **Nombre para mostrar**, o seleccione ✕ para eliminar cualquier elemento que no desee revertir.

   Para revertir un nombre para mostrar, el nombre del sistema debe aparecer en el campo **Nombre para mostrar**, pero el nombre no distingue entre mayúsculas y minúsculas.

b. Seleccione **Cambiar nombre**.

   Aparece un mensaje de éxito. Los nombres mostrados para estos elementos ya no se utilizan.

Vuelva a los nombres de sistema en bloque

a. Para el paso **Proponer nuevos nombres**, selecciona **Usar herramienta de cambio de nombre masivo**.
b. En el campo **cadena existente**, ingrese la cadena de nombre mostrado que desea reemplazar.
c. En el campo **New string**, ingresa la cadena de nombre del sistema que deseas usar en su lugar.
d. Seleccione **Agregar nombres** para agregar los nombres a la tabla para el paso **Proponer nuevos nombres**.
e. Confirme que cada entrada en el campo **Nombre para mostrar** coincide con el nombre del campo **Nombre del sistema**. Realice los cambios o seleccione ✕ para eliminar cualquier elemento que no desee revertir.

   Para revertir un nombre para mostrar, el nombre del sistema debe aparecer en el campo **Nombre para mostrar**, pero el nombre no distingue entre mayúsculas y minúsculas.

f. Seleccione **Cambiar nombre**.

   Se muestra un mensaje de éxito. Los nombres mostrados para estos elementos ya no se utilizan.

5. Descargue y guarde un nuevo paquete de recuperación.

   Los nombres mostrados de los elementos revertidos ya no se incluyen en la `Passwords.txt` archivo.

Procedimientos de nodo

Procedimientos de nodos: Descripción general

Es posible que deba realizar procedimientos de mantenimiento relacionados con nodos de grid específicos o servicios de nodos.

Procedimientos del Administrador de servidores

Server Manager se ejecuta en todos los nodos de grid para supervisar el inicio y la detención de los servicios y garantizar que estos se unen y salen correctamente del sistema StorageGRID. Server Manager también supervisa los servicios en todos los nodos de grid e intentará reiniciar automáticamente los servicios que informen de los errores.

Para realizar los procedimientos del Administrador del servidor, normalmente necesita acceder a la línea de comandos del nodo.

> Debe acceder a Server Manager solo si el soporte técnico le ha indicado hacerlo.

> Debe cerrar la sesión actual del shell de comandos y cerrar la sesión después de terminar con Server Manager. Introduzca: `exit`

Reinicio del nodo, apagado y procedimientos de encendido

Debe usar estos procedimientos para reiniciar uno o más nodos, para apagar y reiniciar nodos, o para apagar los nodos y volver a encenderlos.

Procedimientos de reasignación de puertos

Puede utilizar los procedimientos de reasignación de puertos para eliminar las reasignaciones de puertos de un nodo, por ejemplo, si desea configurar un punto final de equilibrio de carga mediante un puerto que se haya reasignado anteriormente.

Procedimientos del Administrador de servidores

Ver el estado y la versión de Server Manager

Para cada nodo de cuadrícula, puede ver el estado y la versión actuales de Server Manager que se ejecuta en ese nodo de cuadrícula. También puede obtener el estado actual de todos los servicios que se ejecutan en ese nodo de grid.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de grid:

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

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

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

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

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

2. Ver el estado actual de Server Manager que se ejecuta en el nodo de cuadrícula: **`service servermanager status`**

   Se informa del estado actual de Server Manager que se ejecuta en el nodo de cuadrícula (en ejecución o no). Si el estado del Administrador del servidor es `running`, se muestra la hora a la que se ha estado ejecutando desde la última vez que se inició. Por ejemplo:

   ```
   servermanager running for 1d, 13h, 0m, 30s
   ```

3. Ver la versión actual de Server Manager que se ejecuta en un nodo de cuadrícula: **`service servermanager version`**

   Se muestra la versión actual. Por ejemplo:

   ```
   11.1.0-20180425.1905.39c9493
   ```

4. Cierre la sesión del shell de comandos: **`exit`**

Ver el estado actual de todos los servicios

Puede ver el estado actual de todos los servicios que se ejecutan en un nodo de grid en cualquier momento.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de grid:

   a. Introduzca el siguiente comando: `ssh admin@`*`grid_node_IP`*

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

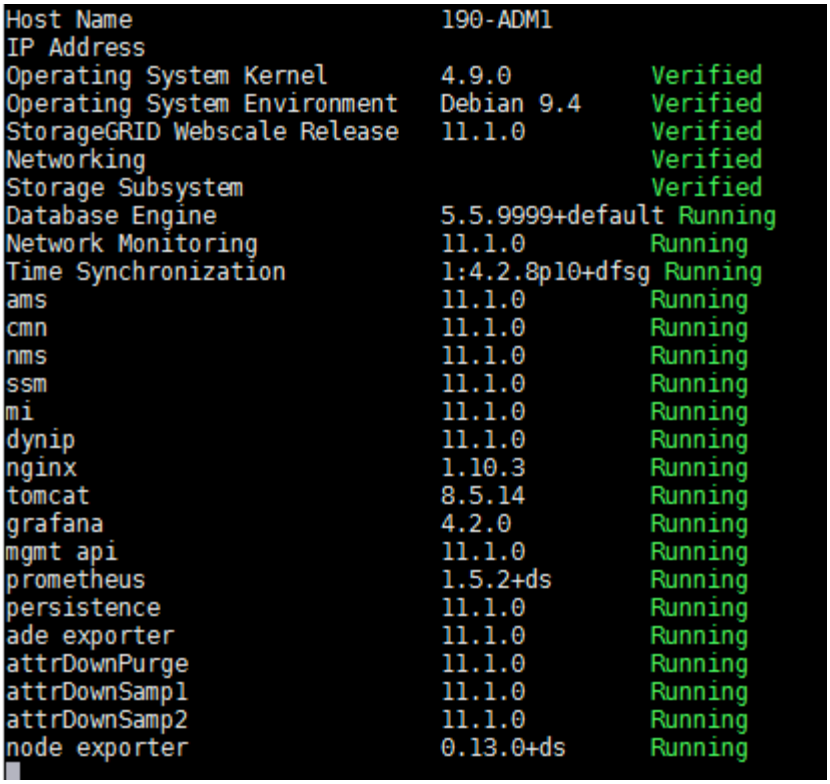
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`

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

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

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

   Por ejemplo, el resultado del nodo de administración principal muestra el estado actual de los servicios AMS, CMN y NMS en ejecución. Este resultado se actualiza inmediatamente si cambia el estado de un servicio.



3. Vuelva a la línea de comandos y pulse **Ctrl**+**C**.
4. Opcionalmente, vea un informe estático para todos los servicios que se ejecutan en el nodo de grid: `/usr/local/servermanager/reader.rb`

   Este informe incluye la misma información que el informe actualizado continuamente, pero no se actualiza si el estado de un servicio cambia.

5. Cierre la sesión del shell de comandos: `exit`

Inicie Server Manager y todos los servicios

Es posible que necesite iniciar Server Manager, que también inicia todos los servicios en el nodo de cuadrícula.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Acerca de esta tarea

Al iniciar Server Manager en un nodo de cuadrícula en el que ya se está ejecutando, se produce un reinicio de Server Manager y de todos los servicios del nodo de cuadrícula.

Pasos

1. Inicie sesión en el nodo de grid:

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

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

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

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

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

2. Iniciar Server Manager: `service servermanager start`
3. Cierre la sesión del shell de comandos: `exit`

Reinicie Server Manager y todos los servicios

Es posible que deba reiniciar el administrador de servidores y todos los servicios que se ejecuten en un nodo de grid.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de grid:

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

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

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

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

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

2. Reinicie Server Manager y todos los servicios del nodo de grid: `service servermanager restart`

   El Administrador del servidor y todos los servicios del nodo de grid se detienen y, a continuación, se reinician.

   > Con el `restart` el comando es el mismo que utiliza el `stop` comando seguido de `start` comando.

3. Cierre la sesión del shell de comandos: `exit`

Detenga Server Manager y todos los servicios

Server Manager está pensado para ejecutarse en todo momento, pero es posible que necesite detener Server Manager y todos los servicios que se ejecutan en un nodo de cuadrícula.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de grid:

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

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

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

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

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

2. Detenga Server Manager y todos los servicios que se ejecutan en el nodo de grid: `service servermanager stop`

   Server Manager y todos los servicios que se ejecutan en el nodo de grid se finalizan correctamente. Los servicios pueden tardar hasta 15 minutos en apagarse.

3. Cierre la sesión del shell de comandos: `exit`

Ver el estado actual del servicio

Puede ver el estado actual de los servicios que se ejecutan en un nodo de grid en cualquier momento.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de grid:

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

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

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

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

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

2. Ver el estado actual de un servicio que se ejecuta en un nodo de cuadrícula: `**service *servicename* status**`
   Se informa del estado actual del servicio solicitado que se ejecuta en el nodo de cuadrícula (en ejecución o no). Por ejemplo:

   ```
   cmn running for 1d, 14h, 21m, 2s
   ```

3. Cierre la sesión del shell de comandos: **`exit`**

Detenga el servicio

Algunos procedimientos de mantenimiento requieren que detenga un solo servicio mientras se ejecutan otros servicios del nodo de grid. Detenga únicamente los servicios individuales cuando se lo indique un procedimiento de mantenimiento.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Acerca de esta tarea

Cuando utilice estos pasos para detener administrativamente un servicio, el Administrador del servidor no reiniciará automáticamente el servicio. Debe iniciar el único servicio manualmente o reiniciar Server Manager.

Si necesita detener el servicio LDR en un nodo de almacenamiento, tenga en cuenta que puede tardar un tiempo en detener el servicio si hay conexiones activas.

Pasos

1. Inicie sesión en el nodo de grid:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Detenga un servicio individual: `service servicename stop`

   Por ejemplo:

   ```
   service ldr stop
   ```

   Los servicios pueden tardar hasta 11 minutos en detenerse.

3. Cierre la sesión del shell de comandos: `exit`

Información relacionada

"Fuerce el servicio para terminar"

Fuerce el servicio para terminar

Si necesita detener un servicio inmediatamente, puede utilizar `force-stop` comando.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de grid:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Fuerce manualmente el servicio para que finalice: `service servicename force-stop`

   Por ejemplo:

   ```
   service ldr force-stop
   ```

   El sistema espera 30 segundos antes de terminar el servicio.

3. Cierre la sesión del shell de comandos: `exit`

Inicie o reinicie el servicio

Es posible que deba iniciar un servicio detenido o que deba detener y reiniciar un servicio.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de grid:

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

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

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

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

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

2. Decida qué comando emitir, en función de si el servicio se está ejecutando actualmente o detenido.

   - Si el servicio está detenido actualmente, utilice `start` comando para iniciar el servicio manualmente: `service servicename start`

     Por ejemplo:

     ```
     service ldr start
     ```

   - Si el servicio se está ejecutando actualmente, utilice `restart` comando para detener el servicio y, a continuación, reiniciarlo: `service servicename restart`

     Por ejemplo:

```
service ldr restart
```

+

> Con el `restart` el comando es el mismo que utiliza el `stop` comando seguido de `start` comando. Puede emitir `restart` incluso si el servicio se detiene actualmente.

3. Cierre la sesión del shell de comandos: `exit`

Utilice un archivo DoNotStart

Si está realizando varios procedimientos de mantenimiento o configuración bajo la dirección del soporte técnico, es posible que se le solicite que utilice un archivo DoNotStart para evitar que los servicios se inicien cuando se inicie o reinicie Server Manager.

> Debe agregar o quitar un archivo DoNotStart sólo si el soporte técnico le ha indicado que lo haga.

Para evitar que se inicie un servicio, coloque un archivo DoNotStart en el directorio del servicio que desea impedir que se inicie. Al iniciar, el Administrador del servidor busca el archivo DoNotStart. Si el archivo está presente, se impide que se inicie el servicio (y cualquier servicio que dependa de él). Cuando se quita el archivo DoNotStart, el servicio detenido anteriormente se iniciará en el siguiente inicio o reinicio de Server Manager. Los servicios no se inician automáticamente cuando se elimina el archivo DoNotStart.

La forma más eficaz de evitar que todos los servicios se reinicien es impedir que se inicie el servicio NTP. Todos los servicios dependen del servicio NTP y no se pueden ejecutar si el servicio NTP no se está ejecutando.

Agregue el archivo DoNotStart para el servicio técnico

Puede impedir que un servicio individual comience agregando un archivo DoNotStart al directorio de ese servicio en un nodo de cuadrícula.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de grid:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Agregar un archivo DoNotStart: `touch /etc/sv/service/DoNotStart`

   donde `service` es el nombre del servicio que se va a impedir que se inicie. Por ejemplo:

```
touch /etc/sv/ldr/DoNotStart
```

Se crea un archivo DoNotStart. No se necesita contenido del archivo.

Cuando se reinicia el Administrador del servidor o el nodo de cuadrícula, el Administrador del servidor se reinicia, pero el servicio no.

3. Cierre la sesión del shell de comandos: `exit`

Quitar el archivo DoNotStart para el servicio técnico

Al quitar un archivo DoNotStart que impide que se inicie un servicio, debe iniciar dicho servicio.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de grid:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Elimine el archivo DoNotStart del directorio de servicios: `rm /etc/sv/service/DoNotStart`

   donde `service` es el nombre del servicio. Por ejemplo:

   ```
   rm /etc/sv/ldr/DoNotStart
   ```

3. Inicie el servicio: `service servicename start`
4. Cierre la sesión del shell de comandos: `exit`

Solucionar problemas de Server Manager

Si surge un problema al utilizar Server Manager, compruebe su archivo de registro.

Los mensajes de error relacionados con Server Manager se capturan en el archivo de registro de Server Manager, que se encuentra en: `/var/local/log/servermanager.log`

Compruebe si hay mensajes de error en este archivo. Si es necesario, Escale el problema al soporte técnico. Es posible que se le solicite reenviar los archivos de registro al soporte técnico.

Servicio con estado de error

Si detecta que un servicio ha introducido un estado de error, intente reiniciar el servicio.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Acerca de esta tarea

Server Manager supervisa los servicios y reinicia los que se hayan detenido inesperadamente. Si un servicio falla, Server Manager intenta reiniciarlo. Si hay tres intentos fallidos para iniciar un servicio en un plazo de cinco minutos, el servicio introduce un estado de error. El Administrador de servidores no intenta volver a iniciar.

Pasos

1. Inicie sesión en el nodo de grid:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Confirmar el estado de error del servicio: `service servicename status`

   Por ejemplo:

   ```
   service ldr status
   ```

   Si el servicio está en estado de error, se devuelve el siguiente mensaje: `servicename in error state`. Por ejemplo:

   ```
   ldr in error state
   ```

   > Si el estado del servicio es `disabled`, consulte las instrucciones para "Quitar un archivo DoNotStart para un servicio".

3. Intente eliminar el estado de error reiniciando el servicio: `service servicename restart`

   Si el servicio no se reinicia, póngase en contacto con el soporte técnico.

4. Cierre la sesión del shell de comandos: `exit`

Procedimientos de reinicio, apagado y encendido

Realice un reinicio gradual

Puede realizar un reinicio gradual para reiniciar varios nodos de grid sin provocar una interrupción del servicio.

Antes de empezar

- Ha iniciado sesión en Grid Manager en el nodo de administración principal y está utilizando un "navegador web compatible".

  Debe iniciar sesión en el nodo de administración principal para realizar este procedimiento.

- Usted tiene la "Permiso de mantenimiento o acceso raíz".

Acerca de esta tarea

Use este procedimiento si necesita reiniciar varios nodos a la vez. Por ejemplo, puede utilizar este procedimiento después de cambiar el modo FIPS para la cuadrícula "Política de seguridad TLS y SSH". Cuando cambia el modo FIPS, debe reiniciar todos los nodos para poner en vigor el cambio.

Si solo necesita reiniciar un nodo, puede "Reinicie el nodo desde la pestaña Tasks".

Cuando StorageGRID reinicia los nodos de grid, emite el `reboot` comando en cada nodo, lo que hace que el nodo se apague y se reinicie. Todos los servicios se reinician automáticamente.

- Reiniciar un nodo VMware reinicia la máquina virtual.
- Reiniciar un nodo Linux reinicia el contenedor.
- Reiniciar un nodo StorageGRID Appliance reinicia la controladora de computación.

El procedimiento de reinicio gradual puede reiniciar varios nodos al mismo tiempo, con las siguientes excepciones:

- No se reiniciarán dos nodos del mismo tipo al mismo tiempo.
- Los nodos de puerta de enlace y los nodos de administración no se reiniciarán al mismo tiempo.
- Los nodos de almacenamiento y los nodos de archivado no se reiniciarán al mismo tiempo.

En su lugar, estos nodos se reinician secuencialmente para garantizar que los grupos de alta disponibilidad, los datos de objetos y los servicios de nodos cruciales siempre estén disponibles.

Al reiniciar el nodo de administración principal, el explorador pierde temporalmente el acceso a Grid Manager, por lo que ya no puede supervisar el procedimiento. Por este motivo, el nodo de administración principal se reinicia en último lugar.

Realice un reinicio gradual

Debe seleccionar los nodos que desea reiniciar, revisar las selecciones, iniciar el procedimiento de reinicio y supervisar el progreso.

Seleccione los nodos

Como primer paso, acceda a la página Rolling reboot y seleccione los nodos que desea reiniciar.

Pasos

1. Selecciona **MANTENIMIENTO** > **Tareas** > **Reiniciar rodando**.
2. Revise el estado de conexión y los iconos de alerta en la columna **Nombre del nodo**.

> No se puede reiniciar un nodo si está desconectado de la cuadrícula. Las casillas de comprobación están deshabilitadas para los nodos con estos iconos: o.

3. Si algún nodo tiene alertas activas, revise la lista de alertas en la columna **Resumen de alertas**.

> Para ver todas las alertas actuales de un nodo, también puede seleccionar la **Pestaña Nodos › Overview**.

4. Opcionalmente, realice las acciones recomendadas para resolver las alertas actuales.
5. Opcionalmente, si todos los nodos están conectados y desea reiniciarlos todos, seleccione la casilla de verificación en el encabezado de la tabla y seleccione **Seleccionar todo**. De lo contrario, seleccione cada nodo que desee reiniciar.

   Puede utilizar las opciones de filtro de la tabla para ver los subconjuntos de nodos. Por ejemplo, puede ver y seleccionar solo nodos de almacenamiento o todos los nodos de un determinado sitio.

6. Selecciona **Revisar selección**.

Revisar selección

En este paso, puede determinar cuánto tiempo puede tardar el procedimiento de reinicio total y confirmar que ha seleccionado los nodos correctos.

1. En la página de selección Review, revise Summary, que indica cuántos nodos se reiniciarán y el tiempo total estimado para que se reinicien todos los nodos.
2. Opcionalmente, para eliminar un nodo específico de la lista de reinicio, seleccione **Eliminar**.
3. Opcionalmente, para agregar más nodos, seleccione **Paso anterior**, seleccione los nodos adicionales y seleccione **Selección de revisión**.
4. Cuando esté listo para iniciar el procedimiento de reinicio progresivo para todos los nodos seleccionados, seleccione **Reiniciar nodos**.
5. Si seleccionó reiniciar el nodo de administración principal, lea el mensaje de información y seleccione **Sí**.

> El nodo de administración principal será el último nodo en reiniciarse. Mientras este nodo se está reiniciando, se perderá la conexión de su navegador. Cuando el nodo de administración principal vuelva a estar disponible, debe volver a cargar la página de reinicio progresivo.

Supervisar un reinicio sucesivo

Mientras se ejecuta el procedimiento de reinicio sucesivo, puede supervisarlo desde el nodo de administración principal.

Pasos

1. Revise el progreso general de la operación, que incluye la siguiente información:
   - Número de nodos reiniciados

- Número de nodos en proceso de reinicio
- Número de nodos que quedan por reiniciar

2. Revise la tabla para cada tipo de nodo.

   Las tablas proporcionan una barra de progreso de la operación en cada nodo y muestran la etapa de reinicio de ese nodo, que puede ser una de las siguientes:

   - Esperando reinicio
   - Deteniendo servicios
   - Reiniciando el sistema
   - Iniciando servicios
   - Se completó el reinicio

Detenga el procedimiento de reinicio progresivo

Puede detener el procedimiento de reinicio gradual desde el nodo de administración principal. Cuando detenga el procedimiento, cualquier nodo que tenga el estado de detención de servicios, reinicio del sistema o inicio de servicios completará la operación de reinicio. Sin embargo, ya no se realizará el seguimiento de estos nodos como parte del procedimiento.

Pasos

1. Selecciona **MANTENIMIENTO** > **Tareas** > **Reiniciar rodando**.
2. En el paso **Monitor reboot**, selecciona **Stop reboot**.

Reinicie el nodo de cuadrícula desde la pestaña Tareas

Se puede reiniciar un nodo de cuadrícula individual desde la pestaña Tasks de la página Nodes.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento.
- Si va a reiniciar el nodo de administración principal o cualquier nodo de almacenamiento, ha revisado las siguientes consideraciones:
  - Al reiniciar el nodo de administración principal, el explorador pierde temporalmente el acceso a Grid Manager.
  - Si reinicia dos o más nodos de almacenamiento en un sitio determinado, es posible que no pueda acceder a ciertos objetos durante el reinicio. Este problema puede ocurrir si alguna regla de ILM utiliza la opción de ingesta **Dual commit** (o una regla especifica **Balanced** y no es posible crear inmediatamente todas las copias requeridas). En este caso, StorageGRID confirmará objetos recién ingeridos en dos nodos de almacenamiento en el mismo sitio y evaluará ILM más adelante.
  - Para garantizar que puede acceder a todos los objetos mientras se reinicia un nodo de almacenamiento, deje de procesar objetos en un sitio durante aproximadamente una hora antes de reiniciar el nodo.

Acerca de esta tarea

Cuando StorageGRID reinicia un nodo de grid, emite el `reboot` comando en el nodo, lo que provoca que el nodo se apague y se reinicie. Todos los servicios se reinician automáticamente.

- Reiniciar un nodo VMware reinicia la máquina virtual.
- Reiniciar un nodo Linux reinicia el contenedor.
- Reiniciar un nodo StorageGRID Appliance reinicia la controladora de computación.

> Si necesita reiniciar más de un nodo, puede usar el "procedimiento de reinicio progresivo".

Pasos

1. Selecciona **NODOS**.
2. Seleccione el nodo de cuadrícula que desea reiniciar.
3. Seleccione la ficha **tareas**.
4. Seleccione **Reiniciar**.

   Se muestra un cuadro de diálogo de confirmación. Si va a reiniciar el nodo de administración principal, el cuadro de diálogo de confirmación le recuerda que la conexión del explorador con el Administrador de grid se perderá temporalmente cuando se detengan los servicios.

5. Introduzca la contraseña de aprovisionamiento y seleccione **Aceptar**.
6. Espere a que se reinicie el nodo.

   El apagado de los servicios puede llevar cierto tiempo.

   Cuando el nodo se está reiniciando, aparece el icono gris (administrativamente inactivo) para el nodo en la página Nodos. Cuando todos los servicios se hayan iniciado de nuevo y el nodo se haya conectado correctamente a la cuadrícula, la página Nodos debe mostrar su estado normal (no hay iconos a la izquierda del nombre del nodo), lo que indica que no hay ninguna alerta activa y que el nodo está conectado a la cuadrícula.

Reinicie el nodo de cuadrícula desde el shell de comandos

Si necesita supervisar la operación de reinicio más de cerca o si no puede acceder a Grid Manager, puede iniciar sesión en el nodo de cuadrícula y ejecutar el comando de reinicio del Administrador del servidor desde el shell de comandos.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de grid:

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

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

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

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

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

2. Si lo desea, detenga los servicios: `service servermanager stop`

   Detener los servicios es un paso opcional pero recomendado. Los servicios pueden tardar hasta 15 minutos en apagarse y es posible que desee iniciar sesión en el sistema de forma remota para supervisar el proceso de apagado antes de reiniciar el nodo en el siguiente paso.

3. Reinicie el nodo de cuadrícula: `reboot`
4. Cierre la sesión del shell de comandos: `exit`

Apague el nodo de grid

Puede apagar un nodo de grid desde el shell de comandos del nodo.

Antes de empezar

- Usted tiene la `Passwords.txt` archivo.

Acerca de esta tarea

Antes de realizar este procedimiento, revise estas consideraciones:

- En general, no debe apagar más de un nodo a la vez para evitar interrupciones.
- No apague un nodo durante un procedimiento de mantenimiento a menos que la documentación o el soporte técnico lo indiquen explícitamente.
- El proceso de apagado se basa en la ubicación en la que se instala el nodo, de la siguiente manera:
  - Apagar un nodo de VMware apaga la máquina virtual.
  - Apagar un nodo Linux apaga el contenedor.
  - Apagar un nodo de un dispositivo StorageGRID apaga la controladora de computación.
- Si tiene previsto apagar más de un nodo de almacenamiento en un sitio, detenga la incorporación de objetos en el sitio durante una hora aproximadamente antes de apagar los nodos.

  Si alguna regla de ILM utiliza la opción de ingesta **Dual commit** (o si una regla usa la opción **Balanced** y no se pueden crear inmediatamente todas las copias requeridas), StorageGRID confirma inmediatamente cualquier objeto recién ingerido en dos nodos de almacenamiento en el mismo sitio y evalúa ILM más tarde. Si se apaga más de un nodo de almacenamiento en un sitio, es posible que no pueda acceder a los objetos recién procesados durante la interrupción del apagado. También es posible que se produzca un error en las operaciones de escritura si hay demasiados nodos de almacenamiento disponibles en el sitio. Consulte "Gestión de objetos con ILM".

Pasos

1. Inicie sesión en el nodo de grid:

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

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

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

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

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

2. Detenga todos los servicios: `service servermanager stop`

Los servicios pueden tardar hasta 15 minutos en apagarse, y es posible que desee iniciar sesión en el sistema de forma remota para supervisar el proceso de apagado.

3. Si el nodo se está ejecutando en una máquina virtual de VMware o si es un nodo del dispositivo, utilice el comando shutdown: `shutdown -h now`

   Realice este paso independientemente del resultado del `service servermanager stop` comando.

   > Después de emitir el `shutdown -h now` debe apagar y encender el dispositivo para reiniciar el nodo.

   Para el dispositivo, este comando apaga la controladora pero el dispositivo sigue encendido. Debe completar el siguiente paso.

4. Si va a apagar un nodo del dispositivo, siga los pasos del dispositivo.

   SGF6112

   a. Apague el aparato.
   b. Espere a que se apague el LED de alimentación azul.

   SG6000

   a. Espere a que se apague el LED verde de caché activa en la parte posterior de las controladoras de almacenamiento.

      Este LED está encendido cuando es necesario escribir en las unidades los datos en caché. Debe esperar a que este LED se apague antes de apagarse.

   b. Apague el aparato y espere a que se apague el LED de alimentación azul.

   SG5700

   a. Espere a que se apague el LED verde de caché activa en la parte posterior de la controladora de almacenamiento.

      Este LED está encendido cuando es necesario escribir en las unidades los datos en caché. Debe esperar a que este LED se apague antes de apagarse.

   b. Apague el aparato y espere a que todos los LED y la actividad de visualización de siete segmentos se detengan.

   SG100 o SG1000

   a. Apague el aparato.
   b. Espere a que se apague el LED de alimentación azul.

Apague el host

Antes de apagar un host, debe detener los servicios de todos los nodos de grid de ese host.

Pasos

1. Inicie sesión en el nodo de grid:

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

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

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

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

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

2. Detenga todos los servicios que se ejecutan en el nodo: `service servermanager stop`

   Los servicios pueden tardar hasta 15 minutos en apagarse, y es posible que desee iniciar sesión en el sistema de forma remota para supervisar el proceso de apagado.

3. Repita los pasos 1 y 2 con cada nodo del host.
4. Si tiene un host Linux:

   a. Inicie sesión en el sistema operativo del host.

   b. Detenga el nodo: `storagegrid node stop`

   c. Apague el sistema operativo host.

5. Si el nodo se está ejecutando en una máquina virtual de VMware o si es un nodo del dispositivo, utilice el comando shutdown: `shutdown -h now`

   Realice este paso independientemente del resultado del `service servermanager stop` comando.

   > Después de emitir el `shutdown -h now` debe apagar y encender el dispositivo para reiniciar el nodo.

   Para el dispositivo, este comando apaga la controladora pero el dispositivo sigue encendido. Debe completar el siguiente paso.

6. Si va a apagar un nodo del dispositivo, siga los pasos del dispositivo.

SGF6112

a. Apague el aparato.

b. Espere a que se apague el LED de alimentación azul.

SG6000

a. Espere a que se apague el LED verde de caché activa en la parte posterior de las controladoras de almacenamiento.

   Este LED está encendido cuando es necesario escribir en las unidades los datos en caché. Debe esperar a que este LED se apague antes de apagarse.

b. Apague el aparato y espere a que se apague el LED de alimentación azul.

SG5700

a. Espere a que se apague el LED verde de caché activa en la parte posterior de la controladora de almacenamiento.

   Este LED está encendido cuando es necesario escribir en las unidades los datos en caché. Debe esperar a que este LED se apague antes de apagarse.

b. Apague el aparato y espere a que todos los LED y la actividad de visualización de siete segmentos se detengan.

SG100 o SG1000

a. Apague el aparato.

b. Espere a que se apague el LED de alimentación azul.

7. Cierre la sesión del shell de comandos: `exit`

Información relacionada

"Dispositivos de almacenamiento SGF6112"

"Dispositivos de almacenamiento SG6000"

"Dispositivos de almacenamiento SG5700"

"Servicios de aplicaciones SG100 y SG1000"

Apague y encienda todos los nodos de grid

Puede que tenga que apagar todo el sistema StorageGRID, por ejemplo, si va a mover un centro de datos. Estos pasos proporcionan una descripción general de alto nivel de la secuencia recomendada para realizar un apagado controlado e inicio.

Cuando se apagan todos los nodos en un sitio o un grid, no se puede acceder a los objetos procesados mientras los nodos de almacenamiento están sin conexión.

Detenga los servicios y apague los nodos de grid

Antes de poder apagar un sistema StorageGRID, debe detener todos los servicios que se ejecutan en cada

nodo de grid y, a continuación, apagar todas las máquinas virtuales de VMware, los motores de contenedor y los dispositivos StorageGRID.

Acerca de esta tarea

Detenga primero los servicios en los nodos de administración y la puerta de enlace y, a continuación, detenga los servicios en los nodos de almacenamiento.

Este enfoque permite usar el nodo de administración principal para supervisar el estado de los demás nodos de grid durante el mayor tiempo posible.

> Si un solo host incluye más de un nodo de cuadrícula, no apague el host hasta que haya detenido todos los nodos de ese host. Si el host incluye el nodo de administrador principal, apague ese host en último lugar.

> Si es necesario, puede "Migre los nodos de un host Linux a otro" para realizar tareas de mantenimiento del host sin afectar a la funcionalidad o disponibilidad del grid.

Pasos

1. Detenga que todas las aplicaciones cliente no accedan a la cuadrícula.
2. Iniciar sesión en cada nodo de puerta de enlace:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.
3. detenga todos los servicios que se ejecutan en el nodo: `service servermanager stop`

   Los servicios pueden tardar hasta 15 minutos en apagarse, y es posible que desee iniciar sesión en el sistema de forma remota para supervisar el proceso de apagado.
4. Repita los dos pasos anteriores para detener los servicios en todos los nodos de almacenamiento, nodos de archivado y nodos de administración no primarios.

   Puede detener los servicios en estos nodos en cualquier orden.

   > Si emite el `service servermanager stop` Para detener los servicios en un nodo de almacenamiento de dispositivo, debe apagar y encender el dispositivo para reiniciar el nodo.
5. Para el nodo de administración principal, repita los pasos a. inicie sesión en el nodo y.. detener todos los servicios del nodo.
6. Para los nodos que se ejecutan en hosts Linux:
   a. Inicie sesión en el sistema operativo del host.
   b. Detenga el nodo: `storagegrid node stop`
   c. Apague el sistema operativo host.

7. Para los nodos que se ejecutan en máquinas virtuales de VMware y para los nodos de almacenamiento de dispositivos, ejecute el comando shutdown: `shutdown -h now`

   Realice este paso independientemente del resultado del `service servermanager stop` comando.

   Para el dispositivo, este comando apaga la controladora de computación, pero el dispositivo sigue encendido. Debe completar el siguiente paso.

8. Si tiene nodos de dispositivo, siga los pasos para su dispositivo.

   SG100 o SG1000

   a. Apague el aparato.

   b. Espere a que se apague el LED de alimentación azul.

   SGF6112

   a. Apague el aparato.

   b. Espere a que se apague el LED de alimentación azul.

   SG6000

   a. Espere a que se apague el LED verde de caché activa en la parte posterior de las controladoras de almacenamiento.

      Este LED está encendido cuando es necesario escribir en las unidades los datos en caché. Debe esperar a que este LED se apague antes de apagarse.

   b. Apague el aparato y espere a que se apague el LED de alimentación azul.

   SG5700

   a. Espere a que se apague el LED verde de caché activa en la parte posterior de la controladora de almacenamiento.

      Este LED está encendido cuando es necesario escribir en las unidades los datos en caché. Debe esperar a que este LED se apague antes de apagarse.

   b. Apague el aparato y espere a que todos los LED y la actividad de visualización de siete segmentos se detengan.

9. Si es necesario, cierre la sesión del shell del comando: `exit`

   El grid de StorageGRID se ha apagado.

Inicie nodos de grid

> Si toda la cuadrícula se ha apagado durante más de 15 días, debe ponerse en contacto con el soporte técnico antes de iniciar cualquier nodo de grid. No intente los procedimientos de recuperación que reconstruyen los datos de Cassandra. Si lo hace, se puede producir la pérdida de datos.

Si es posible, encienda los nodos de la cuadrícula en este orden:

- Aplique primero la alimentación a los nodos de administración.
- Aplique alimentación a los nodos de puerta de enlace en último lugar.

> Si un host incluye varios nodos de grid, los nodos vuelven a estar en línea automáticamente cuando se enciende el host.

Pasos

1. Encienda los hosts del nodo de administrador principal y los nodos de administrador que no son primarios.

   > No podrá iniciar sesión en los nodos de administrador hasta que se hayan reiniciado los nodos de almacenamiento.

2. Encienda los hosts para todos los nodos de archivado y los nodos de almacenamiento.

   Puede encender estos nodos en cualquier orden.

3. Encienda los hosts de todos los nodos de la puerta de enlace.
4. Inicie sesión en Grid Manager.
5. Seleccione **NODES** y supervise el estado de los nodos de la cuadrícula. Compruebe que no hay iconos de alerta junto a los nombres de los nodos.

Información relacionada

- "Dispositivos de almacenamiento SGF6112"
- "Servicios de aplicaciones SG100 y SG1000"
- "Dispositivos de almacenamiento SG6000"
- "Dispositivos de almacenamiento SG5700"

Procedimientos de reasignación de puertos

Eliminar reasignaciones de puertos

Si desea configurar un extremo para el servicio Load Balancer y desea utilizar un puerto que ya se ha configurado como el puerto asignado a un remap de puertos, primero debe eliminar el remap de puertos existente o el extremo no será efectivo. Debe ejecutar un script en cada nodo de administración y nodo de puerta de enlace que tenga puertos reasignados en conflicto para quitar todas las reasignaciones de puertos del nodo.

Acerca de esta tarea

Este procedimiento quita todas las reasignaciones de puertos. Si necesita conservar parte de los remapas, póngase en contacto con el soporte técnico.

Para obtener más información sobre la configuración de puntos finales del equilibrador de carga, consulte "Configuración de los extremos del equilibrador de carga".

> Si la reasignación de puertos proporciona acceso de cliente, vuelva a configurar el cliente para que utilice un puerto diferente como punto final de equilibrio de carga para evitar la pérdida del servicio. De lo contrario, la eliminación de la asignación de puertos provocará la pérdida del acceso del cliente y se deberá programar según corresponda.

Este procedimiento no funciona en un sistema StorageGRID implementado como contenedor en hosts con configuración básica. Consulte las instrucciones para "quitar mapas de puertos en hosts sin sistema operativo".

Pasos

1. Inicie sesión en el nodo.
   a. Introduzca el siguiente comando: `ssh -p 8022 admin@node_IP`

      El puerto 8022 es el puerto SSH del sistema operativo base, mientras que el puerto 22 es el puerto SSH del motor del contenedor que ejecuta StorageGRID.

   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Ejecute el siguiente script: `remove-port-remap.sh`
3. Reinicie el nodo: `reboot`
4. Cierre la sesión del shell de comandos: `exit`
5. Repita estos pasos en cada nodo de administrador y nodo de puerta de enlace que tenga puertos reasignados en conflicto.

Quite las reasignaciones de puertos en hosts sin sistema operativo

Si desea configurar un extremo para el servicio Load Balancer y desea utilizar un puerto que ya se ha configurado como el puerto asignado a un remap de puertos, primero debe eliminar el remap de puertos existente o el extremo no será efectivo.

Acerca de esta tarea

Si está ejecutando StorageGRID en hosts con configuración básica, siga este procedimiento en lugar del procedimiento general para quitar reasignaciones de puertos. Debe editar el archivo de configuración de nodos para cada nodo de administración y nodo de puerta de enlace que tenga puertos reasignados en conflicto para quitar todas las reasignaciones de puertos del nodo y reiniciar el nodo.

Este procedimiento quita todas las reasignaciones de puertos. Si necesita conservar parte de los remapas, póngase en contacto con el soporte técnico.

Para obtener información sobre la configuración de puntos finales del equilibrador de carga, consulte las instrucciones para administrar StorageGRID.

Este procedimiento puede provocar la pérdida temporal del servicio cuando se reinician los nodos.

Pasos

1. Inicie sesión en el host que admite el nodo. Inicie sesión como raíz o con una cuenta que tenga permiso sudo.

2. Ejecute el siguiente comando para deshabilitar temporalmente el nodo: `sudo storagegrid node stop node-name`
3. Mediante un editor de texto como vim o pico, edite el archivo de configuración del nodo.

   Puede encontrar el archivo de configuración del nodo en `/etc/storagegrid/nodes/node-name.conf`.

4. Busque la sección del archivo de configuración del nodo que contiene las reasignaciones de puertos.

   Consulte las dos últimas líneas en el siguiente ejemplo.

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = Interface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = Interface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = Interface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443
```

5. Edite las entradas PORT_REMAPP y PORT_REMAPP_INBOUND para eliminar los remapas de puertos.

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. Ejecute el siguiente comando para validar los cambios en el archivo de configuración del nodo para el nodo: `sudo storagegrid node validate node-name`

Solucione todos los errores o advertencias antes de continuar con el siguiente paso.

7. Ejecute el siguiente comando para reiniciar el nodo sin reasignaciones de puerto: `sudo storagegrid node start node-name`
8. Inicie sesión en el nodo como administrador con la contraseña que aparece en el `Passwords.txt` archivo.
9. Compruebe que los servicios se inician correctamente.
   a. Ver una lista de los estados de todos los servicios del servidor:`sudo storagegrid-status`

      El estado se actualiza automáticamente.

   b. Espere a que todos los servicios tengan el estado en ejecución o verificado.
   c. Salir de la pantalla de estado:`Ctrl+C`
10. Repita estos pasos en cada nodo de administrador y nodo de puerta de enlace que tenga puertos reasignados en conflicto.

Procedimientos de red

Actualice las subredes de la red de cuadrícula

StorageGRID mantiene una lista de las subredes de red que se utilizan para comunicarse entre los nodos de grid en la red de cuadrícula (eth0). Estas entradas incluyen las subredes utilizadas para la red de cuadrícula por cada sitio del sistema StorageGRID, así como las subredes utilizadas para NTP, DNS, LDAP u otros servidores externos a los que se acceda a través de la puerta de enlace de red de cuadrícula. Al agregar nodos de cuadrícula o un sitio nuevo en una expansión, es posible que deba actualizar o agregar subredes a la red de cuadrícula.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento.
- Tiene las direcciones de red, en notación CIDR, de las subredes que desea configurar.

Acerca de esta tarea

Si está realizando una actividad de expansión que incluye agregar una nueva subred, debe agregar una nueva subred a la lista de subred de Red de Grid antes de iniciar el procedimiento de expansión. De lo contrario, tendrá que cancelar la expansión, agregar la nueva subred e iniciar la expansión de nuevo.

Agregue una subred

Pasos

1. Seleccione **MANTENIMIENTO** > **Red** > **Red de red**.
2. Seleccione **Agregar otra subred** para agregar una nueva subred en la notación CIDR.

   Por ejemplo, introduzca `10.96.104.0/22`.

3. Introduzca la contraseña de aprovisionamiento y seleccione **Guardar**.
4. Espere hasta que se apliquen los cambios y, a continuación, descargue un nuevo paquete de recuperación.
   a. Seleccione **MANTENIMIENTO** > **sistema** > **paquete de recuperación**.
   b. Introduzca la **frase de paso de aprovisionamiento**.

> El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID. También se utiliza para recuperar el nodo de administración principal.

Las subredes que ha especificado se configuran automáticamente para el sistema StorageGRID.

Editar una subred

Pasos

1. Seleccione **MANTENIMIENTO** > **Red** > **Red de red**.
2. Seleccione la subred que desea editar y realice los cambios necesarios.
3. Introduzca la frase de contraseña de Provisionamiento y seleccione **Guardar**.
4. Seleccione **Sí** en el cuadro de diálogo de confirmación.
5. Espere hasta que se apliquen los cambios y, a continuación, descargue un nuevo paquete de recuperación.
   a. Seleccione **MANTENIMIENTO** > **sistema** > **paquete de recuperación**.
   b. Introduzca la **frase de paso de aprovisionamiento**.

Eliminar una subred

Pasos

1. Seleccione **MANTENIMIENTO** > **Red** > **Red de red**.
2. Seleccione el icono de eliminar ✕ junto a la subred.
3. Introduzca la frase de contraseña de Provisionamiento y seleccione **Guardar**.
4. Seleccione **Sí** en el cuadro de diálogo de confirmación.
5. Espere hasta que se apliquen los cambios y, a continuación, descargue un nuevo paquete de recuperación.
   a. Seleccione **MANTENIMIENTO** > **sistema** > **paquete de recuperación**.
   b. Introduzca la **frase de paso de aprovisionamiento**.

Configurar las direcciones IP

Configurar direcciones IP: Descripción general

Puede realizar la configuración de red configurando direcciones IP para nodos de grid mediante la herramienta Cambiar IP.

Debe utilizar la herramienta Change IP para realizar la mayoría de los cambios en la configuración de red que se estableció inicialmente durante la implementación de grid. Los cambios manuales que utilizan comandos y

archivos de red estándar de Linux pueden no propagarse a todos los servicios de StorageGRID y podrían no persistir en todas las actualizaciones, reinicios o procedimientos de recuperación de nodos.

> El procedimiento de cambio de IP puede ser un procedimiento disruptivo. Es posible que algunas partes de la cuadrícula no estén disponibles hasta que se aplique la nueva configuración.

> Si sólo va a realizar cambios en la lista de subredes de red de cuadrícula, utilice el administrador de cuadrícula para agregar o cambiar la configuración de red. De lo contrario, utilice la herramienta Cambiar IP si no se puede acceder a Grid Manager debido a un problema de configuración de red o si está realizando un cambio de enrutamiento de red de cuadrícula y otros cambios de red al mismo tiempo.

> Si desea cambiar la dirección IP de red de cuadrícula para todos los nodos de la cuadrícula, utilice "procedimiento especial para cambios en toda la red".

Interfaces Ethernet

La dirección IP asignada a eth0 siempre es la dirección IP de red de cuadrícula del nodo. La dirección IP asignada a eth1 siempre es la dirección IP de red de administrador del nodo de grid. La dirección IP asignada a eth2 es siempre la dirección IP de red de cliente del nodo grid.

Tenga en cuenta que en algunas plataformas, como dispositivos StorageGRID, eth0, eth1 y eth2 pueden ser interfaces de agregado compuestas de puentes subordinados o enlaces de interfaces físicas o VLAN. En estas plataformas, la pestaña **SSM** > **Resources** puede mostrar la dirección IP de red de Grid, Admin y Client Network asignada a otras interfaces además de eth0, eth1 o eth2.

DHCP

DHCP solo puede configurarse durante la fase de implementación. No puede configurar DHCP durante la configuración. Debe usar los procedimientos de cambio de direcciones IP si desea cambiar las direcciones IP, las máscaras de subred y las puertas de enlace predeterminadas para un nodo de grid. Si se usa la herramienta Change IP, las direcciones DHCP se volverán estáticas.

Grupos de alta disponibilidad

- Si una interfaz de red de cliente está contenida en un grupo de alta disponibilidad, no puede cambiar la dirección IP de la red de cliente de esa interfaz a una dirección que esté fuera de la subred configurada para el grupo de alta disponibilidad.
- No puede cambiar la dirección IP de la red del cliente al valor de una dirección IP virtual existente asignada a un grupo HA configurado en la interfaz de red del cliente.
- Si una interfaz de red de Grid está contenida en un grupo de alta disponibilidad, no puede cambiar la dirección IP de red de Grid de esa interfaz por una dirección que esté fuera de la subred configurada para el grupo de alta disponibilidad.
- No puede cambiar la dirección IP de red de grid al valor de una dirección IP virtual existente asignada a un grupo HA configurado en la interfaz de red de grid.

Cambie la configuración de red de los nodos

Puede cambiar la configuración de red de uno o varios nodos con la herramienta Cambiar IP. Puede cambiar la configuración de la red de cuadrícula o agregar, cambiar o

quitar las redes de administrador o de cliente.

Antes de empezar

Usted tiene la `Passwords.txt` archivo.

Acerca de esta tarea

Linux: Si va a agregar un nodo de cuadrícula a la red de administración o a la red de cliente por primera vez, y no ha configurado previamente ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET en el archivo de configuración de nodo, debe hacerlo ahora.

Consulte las instrucciones de instalación de StorageGRID para su sistema operativo Linux:

- "Instalar StorageGRID en Red Hat Enterprise Linux"
- "Instalar StorageGRID en Ubuntu o Debian"

Electrodomésticos: En los dispositivos StorageGRID, si el Cliente o la Red de administración no se configuraron en el Instalador de dispositivos StorageGRID durante la instalación inicial, la red no se puede agregar utilizando solo la herramienta Cambiar IP. En primer lugar, usted debe "coloque el aparato en modo de mantenimiento", Configure los vínculos, devuelva el dispositivo al modo de funcionamiento normal y, a continuación, utilice la herramienta Cambiar IP para modificar la configuración de la red. Consulte "procedimiento para configurar enlaces de red".

Es posible cambiar el valor de la dirección IP, la máscara de subred, la puerta de enlace o MTU para uno o más nodos de cualquier red.

También puede agregar o quitar un nodo de una red cliente o de una red administrativa:

- Puede añadir un nodo a una red cliente o a una red de administrador si añade una dirección IP/máscara de subred en esa red al nodo.
- Puede quitar un nodo de una red cliente o de una red de administrador si elimina la dirección IP/máscara de subred del nodo en esa red.

  Los nodos no se pueden eliminar de la red de grid.

Los intercambios de direcciones IP no están permitidos. Si debe intercambiar direcciones IP entre nodos de cuadrícula, debe utilizar una dirección IP intermedia temporal.

Si está habilitado el inicio de sesión único (SSO) para el sistema StorageGRID y va a cambiar la dirección IP de un nodo de administración, tenga en cuenta que cualquier confianza de la parte que dependa configurada mediante la dirección IP del nodo de administración (en lugar de su nombre de dominio completo, como se recomienda) pasará a ser no válida. Ya no podrá iniciar sesión en el nodo. Inmediatamente después de cambiar la dirección IP, debe actualizar o volver a configurar la confianza del interlocutor que confía en el nodo en los Servicios de Federación de Active Directory (AD FS) con la nueva dirección IP. Consulte las instrucciones para "Configuración de SSO".

Todos los cambios realizados en la red mediante la herramienta Cambiar IP se propagan al firmware del instalador para los dispositivos StorageGRID. De este modo, si se vuelve a instalar el software StorageGRID en un dispositivo o si se pone un dispositivo en modo de mantenimiento, la configuración de red será correcta.

Pasos

1. Inicie sesión en el nodo de administración principal:

   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`

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

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

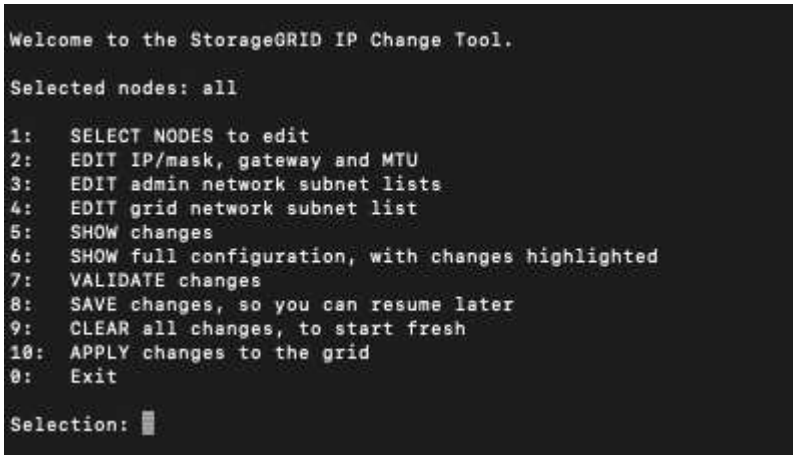
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Inicie la herramienta Cambiar IP introduciendo el siguiente comando: `change-ip`

3. Introduzca la clave de acceso de aprovisionamiento en el aviso de.

   Aparece el menú principal.



4. Si lo desea, seleccione **1** para elegir los nodos que desea actualizar. A continuación, seleccione una de las siguientes opciones:

   - **1**: Un solo nodo — seleccione por nombre
   - **2**: Un solo nodo — seleccione por sitio y luego por nombre
   - **3**: Un solo nodo — seleccione por IP actual
   - **4**: Todos los nodos de un sitio
   - **5**: Todos los nodos de la red

     Nota: Si desea actualizar todos los nodos, deje que "All" permanezca seleccionado.

   Después de hacer su selección, aparece el menú principal, con el campo **nodos seleccionados** actualizado para reflejar su elección. Todas las acciones posteriores se realizan solo en los nodos que se muestran.

5. En el menú principal, seleccione la opción **2** para editar la información de IP/máscara, puerta de enlace y MTU para los nodos seleccionados.

   a. Seleccione la red en la que desea realizar los cambios:

      - **1**: Red de red
      - **2**: Red de administración

- **3**: Red cliente
- **4**: Todas las redes

Después de realizar su selección, la petición de datos muestra el nombre del nodo, el nombre de red (Grid, Admin o Client), el tipo de datos (IP/mask, pasarela o MTU) y valor actual.

Si se edita la dirección IP, la longitud del prefijo, la puerta de enlace o la MTU de una interfaz configurada para DHCP, la interfaz se cambiará a estática. Cuando se selecciona para cambiar una interfaz configurada por DHCP, se muestra una advertencia para informarle de que la interfaz cambiará a estática.

Las interfaces se han configurado como `fixed` no se puede editar.

b. Para establecer un nuevo valor, introdúzcalo en el formato que se muestra para el valor actual.

c. Para dejar sin modificar el valor actual, pulse **Intro**.

d. Si el tipo de datos es `IP/mask`, Puede eliminar la red de administración o de cliente del nodo introduciendo **d** o **0.0.0.0/0**.

e. Después de editar todos los nodos que desea cambiar, introduzca **q** para volver al menú principal.

Los cambios se mantienen hasta que se borran o se aplican.

6. Revise los cambios seleccionando una de las siguientes opciones:
   - **5**: Muestra las ediciones en la salida que está aislada para mostrar sólo el elemento cambiado. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones), como se muestra en la salida de ejemplo:

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Grid    MTU     [               1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
username-x Admin   MTU     [               1400 ]: 0
Press Enter to continue
```

   - **6**: Muestra las ediciones en salida que muestran la configuración completa. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones).

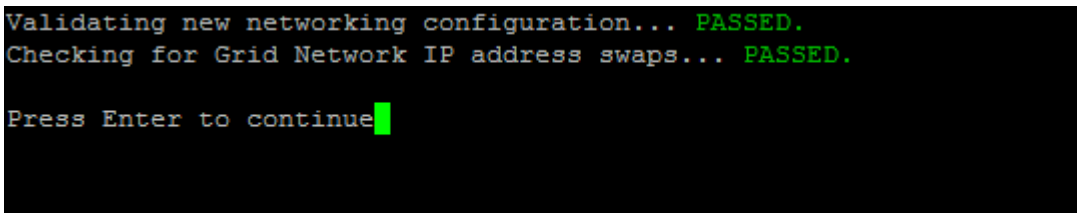
Algunas interfaces de línea de comandos pueden mostrar adiciones y eliminaciones utilizando formato de tachado. La visualización adecuada depende del cliente de terminal que admita las secuencias de escape de VT100 necesarias.

7. Seleccione la opción **7** para validar todos los cambios.

   Esta validación garantiza que no se violen las reglas para las redes Grid, Admin y Client, como no utilizar subredes superpuestas.

   En este ejemplo, la validación devolvió errores.

   En este ejemplo, se ha aprobado la validación.



8. Una vez aprobada la validación, elija una de las siguientes opciones:
   - **8**: Guardar los cambios no aplicados.

     Esta opción le permite salir de la herramienta Cambiar IP e iniciarla de nuevo más tarde, sin perder ningún cambio no aplicado.

   - **10**: Aplique la nueva configuración de red.
9. Si ha seleccionado la opción **10**, elija una de las siguientes opciones:
   - **Aplicar**: Aplique los cambios inmediatamente y reinicie automáticamente cada nodo si es necesario.

     Si la nueva configuración de red no requiere ningún cambio físico de red, puede seleccionar **aplicar** para aplicar los cambios inmediatamente. Los nodos se reiniciarán automáticamente si es necesario. Se mostrarán los nodos que se deban reiniciar.

   - **Fase**: Aplique los cambios la próxima vez que se reinicien manualmente los nodos.

     Si necesita realizar cambios físicos o virtuales en la configuración de red para que funcione la nueva configuración de red, debe utilizar la opción **Stage**, apagar los nodos afectados, realizar los cambios físicos de red necesarios y reiniciar los nodos afectados. Si selecciona **aplicar** sin realizar primero estos cambios de red, los cambios normalmente fallarán.

     Si utiliza la opción **Stage**, debe reiniciar el nodo Lo antes posible. después de la configuración provisional para minimizar las interrupciones.

- **CANCELAR**: No realice ningún cambio de red en este momento.

  Si no sabía que los cambios propuestos requieren que se reinicien los nodos, puede aplazar los cambios para minimizar el impacto del usuario. Si selecciona **cancelar**, volverá al menú principal y mantendrá los cambios para que los pueda aplicar más tarde.

  Al seleccionar **aplicar** o **fase**, se genera un nuevo archivo de configuración de red, se realiza el aprovisionamiento y los nodos se actualizan con nueva información de trabajo.

  Durante el aprovisionamiento, la salida muestra el estado a medida que se aplican las actualizaciones.

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

Después de aplicar o almacenar en zona intermedia los cambios, se genera un nuevo paquete de recuperación como resultado del cambio de configuración de cuadrícula.

10. Si ha seleccionado **fase**, siga estos pasos después de finalizar el aprovisionamiento:

    a. Realice los cambios necesarios en la red virtual o física.

       Cambios físicos en la red: Realice los cambios físicos necesarios en la red, apagando el nodo de forma segura si es necesario.

    Linux: Si agrega el nodo a una red de administración o a una red de cliente por primera vez, asegúrese de que ha agregado la interfaz como se describe en "Linux: Añadir interfaces al nodo existente".

    a. Reinicie los nodos afectados.

11. Seleccione **0** para salir de la herramienta Cambiar IP una vez que hayan finalizado los cambios.
12. Descargue un nuevo paquete de recuperación desde Grid Manager.
    a. Seleccione **MANTENIMIENTO** > **sistema** > **paquete de recuperación**.
    b. Introduzca la clave de acceso de aprovisionamiento.

Agregar o cambiar listas de subredes en la red de administración

Puede agregar, eliminar o cambiar las subredes en la Lista de subredes de red de administración de uno o más nodos.

Antes de empezar

- Usted tiene la `Passwords.txt` archivo.

Puede agregar, eliminar o cambiar subredes a todos los nodos de la lista de subredes de la red de administración.

Pasos

1. Inicie sesión en el nodo de administración principal:

a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`

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

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

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

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

2. Inicie la herramienta Cambiar IP introduciendo el siguiente comando: `change-ip`
3. Introduzca la clave de acceso de aprovisionamiento en el aviso de.

   Aparece el menú principal.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

4. De manera opcional, limite las redes/nodos a los que se realizan las operaciones. Elija una de las siguientes opciones:
   - Seleccione los nodos que desea editar eligiendo **1**, si desea filtrar en nodos específicos en los que realizar la operación. Seleccione una de las siguientes opciones:
     - **1**: Un solo nodo (seleccione por nombre)
     - **2**: Un solo nodo (seleccione por sitio y, a continuación, por nombre)
     - **3**: Un solo nodo (seleccione por IP actual)
     - **4**: Todos los nodos de un sitio
     - **5**: Todos los nodos de la red
     - **0**: Vuelva
   - Permitir que todos permanezcan seleccionados.
     Una vez realizada la selección, aparece la pantalla del menú principal. El campo nodos seleccionados refleja su nueva selección y ahora todas las operaciones seleccionadas sólo se realizarán en este elemento.
5. En el menú principal, seleccione la opción para editar subredes para la red de administración (opción **3**).
6. Elija una de las siguientes opciones:
   - Para añadir una subred, introduzca este comando: `add CIDR`
   - Para eliminar una subred, introduzca este comando: `del CIDR`
   - Defina la lista de subredes introduciendo este comando: `set CIDR`

Para todos los comandos, es posible introducir varias direcciones con este formato: `add CIDR, CIDR`

Ejemplo: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

Puede reducir la cantidad de escritura necesaria con la flecha hacia arriba para recuperar los valores previamente escritos en la petición de datos de entrada actual y, a continuación, editarlos si es necesario.

La entrada de ejemplo siguiente muestra cómo agregar subredes a la lista de subredes de la red de administración:

```
Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
  10.0.0.0/8
  172.19.0.0/16
  172.21.0.0/16
  172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16
```

7. Cuando esté listo, introduzca **q** para volver a la pantalla del menú principal. Los cambios se mantienen hasta que se borran o se aplican.

Si seleccionó cualquiera de los modos de selección de nodos “Todos” en el paso 2, presione **Intro** (sin **q**) para llegar al siguiente nodo de la lista.

8. Elija una de las siguientes opciones:

   - Seleccione la opción **5** para mostrar las ediciones en la salida que está aislada para mostrar sólo el elemento cambiado. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones), como se muestra en la siguiente salida de ejemplo:

```
================================================================================
Site: Data Center 1
================================================================================
DC1-ADM1-105-154 Admin  Subnets                        add 172.17.0.0/16
                                                       del 172.16.0.0/16
                                [       172.14.0.0/16 ]
                                [       172.15.0.0/16 ]
                                [       172.17.0.0/16 ]
                                [       172.19.0.0/16 ]
                                [       172.20.0.0/16 ]
                                [       172.21.0.0/16 ]
Press Enter to continue
```

   - Seleccione la opción **6** para mostrar las ediciones en la salida que muestran la configuración completa. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones).
     Nota: algunos emuladores de terminal pueden mostrar adiciones y eliminaciones utilizando formato de

tachado.

Cuando intenta cambiar la lista de subredes, se muestra el siguiente mensaje:

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that aren't
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
aren't reachable using default StorageGRID routing, but are reachable
using a different interface and gateway. Making and applying changes
to the subnet list will make all automatically applied subnets
persistent. If you don't want that to happen, delete the unwanted
subnets before applying changes. If you know that all /32 subnets in
the list were added intentionally, you can ignore this caution.
```

Si no asignó específicamente las subredes del servidor NTP y DNS a una red, StorageGRID crea una ruta de host (/32) para la conexión automáticamente. Si, por ejemplo, prefiere tener una ruta /16 o /24 para la conexión saliente a un servidor DNS o NTP, debe eliminar la ruta /32 creada automáticamente y agregar las rutas que desee. Si no elimina la ruta de host creada automáticamente, se mantendrá después de aplicar cualquier cambio a la lista de subredes.

> Aunque puede utilizar estas rutas de host detectadas automáticamente, en general debe configurar manualmente las rutas DNS y NTP para garantizar la conectividad.

9. Seleccione la opción **7** para validar todos los cambios organizados.

   Esta validación garantiza que se sigan las reglas para las redes Grid, Admin y Client, como el uso de subredes superpuestas.

10. Opcionalmente, seleccione la opción **8** para guardar todos los cambios organizados y volver más tarde para continuar realizando cambios.

    Esta opción le permite salir de la herramienta Cambiar IP e iniciarla de nuevo más tarde, sin perder ningún cambio no aplicado.

11. Debe realizar una de las siguientes acciones:
    - Seleccione la opción **9** si desea borrar todos los cambios sin guardar ni aplicar la nueva configuración de red.
    - Seleccione la opción **10** si está listo para aplicar cambios y para aprovisionar la nueva configuración de red. Durante el aprovisionamiento, la salida muestra el estado a medida que se aplican las actualizaciones, tal y como se muestra en la siguiente salida de ejemplo:

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

12. Descargue un nuevo paquete de recuperación desde Grid Manager.
    a. Seleccione **MANTENIMIENTO** > **sistema** > **paquete de recuperación**.
    b. Introduzca la clave de acceso de aprovisionamiento.

Agregar o cambiar listas de subred en Grid Network

Puede utilizar la herramienta Cambiar IP para agregar o cambiar subredes en la red de cuadrícula.

Antes de empezar

- Usted tiene la `Passwords.txt` archivo.

Puede agregar, eliminar o cambiar subredes en la Lista de subredes de red de cuadrícula. Los cambios afectarán el enrutamiento de todos los nodos de la cuadrícula.

> Si sólo va a realizar cambios en la lista de subredes de red de cuadrícula, utilice el administrador de cuadrícula para agregar o cambiar la configuración de red. De lo contrario, utilice la herramienta Cambiar IP si no se puede acceder a Grid Manager debido a un problema de configuración de red o si está realizando un cambio de enrutamiento de red de cuadrícula y otros cambios de red al mismo tiempo.

Pasos

1. Inicie sesión en el nodo de administración principal:
    a. Introduzca el siguiente comando: `ssh admin@`*`primary_Admin_Node_IP`*
    b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
    c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
    d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Inicie la herramienta Cambiar IP introduciendo el siguiente comando: `change-ip`
3. Introduzca la clave de acceso de aprovisionamiento en el aviso de.

    Aparece el menú principal.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

4. En el menú principal, seleccione la opción para editar subredes para la red de cuadrícula (opción **4**).

   Los cambios en la lista de subredes de red de cuadrícula se realizan en toda la cuadrícula.

5. Elija una de las siguientes opciones:

   - Para añadir una subred, introduzca este comando: `add CIDR`
   - Para eliminar una subred, introduzca este comando: `del CIDR`
   - Defina la lista de subredes introduciendo este comando: `set CIDR`

   Para todos los comandos, es posible introducir varias direcciones con este formato: `add CIDR, CIDR`

   Ejemplo: `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

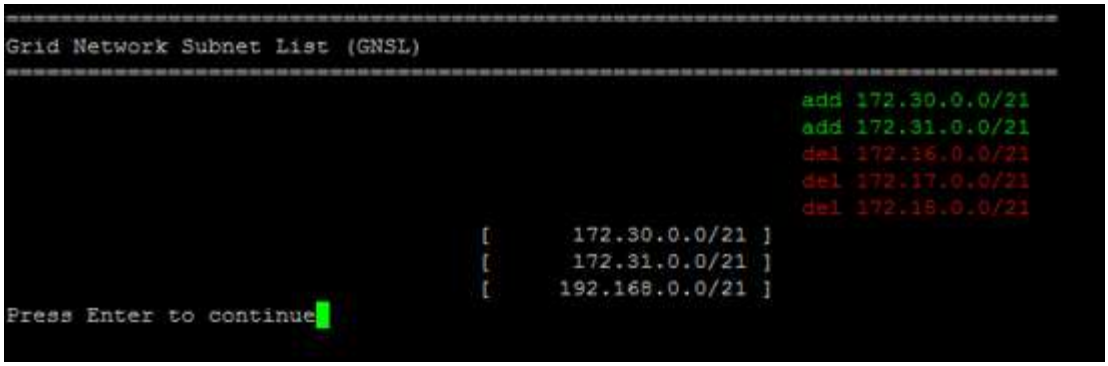
   Puede reducir la cantidad de escritura necesaria con la flecha hacia arriba para recuperar los valores previamente escritos en la petición de datos de entrada actual y, a continuación, editarlos si es necesario.

   La entrada de ejemplo siguiente muestra la configuración de subredes para la Lista de subredes de redes de cuadrícula:

```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
  172.16.0.0/21
  172.17.0.0/21
  172.18.0.0/21
  192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

6. Cuando esté listo, introduzca **q** para volver a la pantalla del menú principal. Los cambios se mantienen hasta que se borran o se aplican.
7. Elija una de las siguientes opciones:

   - Seleccione la opción **5** para mostrar las ediciones en la salida que está aislada para mostrar sólo el elemento cambiado. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones), como se muestra en la siguiente salida de ejemplo:



- Seleccione la opción **6** para mostrar las ediciones en la salida que muestran la configuración completa. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones).

> Algunas interfaces de línea de comandos pueden mostrar adiciones y eliminaciones utilizando formato de tachado.

8. Seleccione la opción **7** para validar todos los cambios organizados.

   Esta validación garantiza que se sigan las reglas para las redes Grid, Admin y Client, como el uso de subredes superpuestas.

9. Opcionalmente, seleccione la opción **8** para guardar todos los cambios organizados y volver más tarde para continuar realizando cambios.

   Esta opción le permite salir de la herramienta Cambiar IP e iniciarla de nuevo más tarde, sin perder ningún cambio no aplicado.

10. Debe realizar una de las siguientes acciones:
    - Seleccione la opción **9** si desea borrar todos los cambios sin guardar ni aplicar la nueva configuración de red.
    - Seleccione la opción **10** si está listo para aplicar cambios y para aprovisionar la nueva configuración de red. Durante el aprovisionamiento, la salida muestra el estado a medida que se aplican las actualizaciones, tal y como se muestra en la siguiente salida de ejemplo:

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

11. Si ha seleccionado la opción **10** al realizar cambios en la red de cuadrícula, seleccione una de las siguientes opciones:
    - **Aplicar**: Aplique los cambios inmediatamente y reinicie automáticamente cada nodo si es necesario.

      Si la nueva configuración de red funcionará simultáneamente con la configuración de red antigua sin ningún cambio externo, puede utilizar la opción **aplicar** para un cambio de configuración completamente automatizado.

- **Fase**: Aplique los cambios la próxima vez que se reinicien los nodos.

  Si necesita realizar cambios físicos o virtuales en la configuración de red para que funcione la nueva configuración de red, debe utilizar la opción **Stage**, apagar los nodos afectados, realizar los cambios físicos de red necesarios y reiniciar los nodos afectados.

  > Si utiliza la opción **stage**, reinicie el nodo lo antes posible después de la puesta en escena para minimizar las interrupciones.

- **CANCELAR**: No realice ningún cambio de red en este momento.

  Si no sabía que los cambios propuestos requieren que se reinicien los nodos, puede aplazar los cambios para minimizar el impacto del usuario. Si selecciona **cancelar**, volverá al menú principal y mantendrá los cambios para que los pueda aplicar más tarde.

Después de aplicar o almacenar en zona intermedia los cambios, se genera un nuevo paquete de recuperación como resultado del cambio de configuración de cuadrícula.

12. Si la configuración se detiene debido a errores, están disponibles las siguientes opciones:
    - Para finalizar el procedimiento de cambio de IP y volver al menú principal, introduzca **A**.
    - Para volver a intentar la operación que falló, introduzca **r**.
    - Para continuar con la siguiente operación, introduzca **c**.

      La operación fallida se puede volver a intentar más tarde seleccionando la opción **10** (aplicar cambios) en el menú principal. El procedimiento de cambio de IP no se completará hasta que todas las operaciones se hayan completado correctamente.

    - Si tuvo que intervenir manualmente (para reiniciar un nodo, por ejemplo) y está seguro de que la acción que la herramienta considera que ha fallado se ha completado correctamente, introduzca **f** para marcarlo como correcto y pasar a la siguiente operación.
13. Descargue un nuevo paquete de recuperación desde Grid Manager.
    a. Seleccione **MANTENIMIENTO** > **sistema** > **paquete de recuperación**.
    b. Introduzca la clave de acceso de aprovisionamiento.

    > El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID.

Cambie las direcciones IP para todos los nodos de la cuadrícula

Si necesita cambiar la dirección IP de red de cuadrícula para todos los nodos de la cuadrícula, debe seguir este procedimiento especial. No se puede realizar un cambio de IP de red de red de red de toda la red mediante el procedimiento para cambiar nodos individuales.

Antes de empezar

- Usted tiene la `Passwords.txt` archivo.

Para asegurarse de que la cuadrícula se inicia correctamente, debe realizar todos los cambios al mismo tiempo.

Este procedimiento se aplica sólo a la red de cuadrícula. No puede utilizar este procedimiento para cambiar las direcciones IP en las redes de administración o cliente.

Si desea cambiar las direcciones IP y MTU para los nodos en un solo sitio, siga el "Cambie la configuración de red de los nodos" instrucciones.

Pasos

1. Planifique con antelación los cambios que necesite hacer fuera de la herramienta Cambiar IP, como los cambios en DNS o NTP, y los cambios en la configuración de inicio de sesión único (SSO), si se utiliza.

   Si no podrá acceder a los servidores NTP existentes a la cuadrícula en las nuevas direcciones IP, añada los nuevos servidores NTP antes de realizar el procedimiento de cambio ip.

   Si no se podrá acceder a los servidores DNS existentes a la cuadrícula en las nuevas direcciones IP, agregue los nuevos servidores DNS antes de realizar el procedimiento Change-ip.

   Si SSO está habilitado para el sistema StorageGRID y todas las confianzas de partes que dependan se configuraron utilizando direcciones IP de nodos de administración (en lugar de nombres de dominio completos, según se recomienda), esté preparado para actualizar o reconfigurar estas confianzas de partes que se basan en los Servicios de Federación de Active Directory (AD FS). Inmediatamente después de cambiar las direcciones IP. Consulte "Configurar el inicio de sesión único".

   De ser necesario, añada la nueva subred para las nuevas direcciones IP.

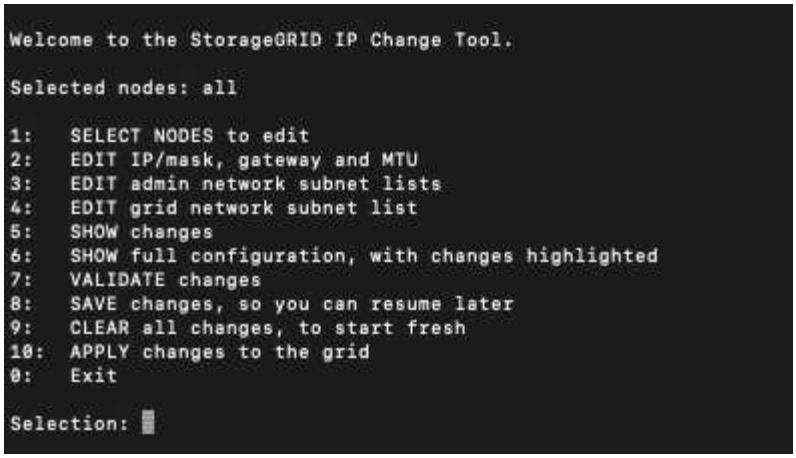
2. Inicie sesión en el nodo de administración principal:

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

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

3. Inicie la herramienta Cambiar IP introduciendo el siguiente comando: `change-ip`
4. Introduzca la clave de acceso de aprovisionamiento en el aviso de.

   Aparece el menú principal. De forma predeterminada, la `Selected nodes` el campo está establecido en `all`.



5. En el menú principal, seleccione **2** para editar la información de IP/máscara de subred, puerta de enlace y MTU para todos los nodos.

   a. Seleccione **1** para realizar cambios en la red de cuadrícula.

      Después de realizar la selección, el símbolo del sistema muestra los nombres de los nodos, el nombre de red de cuadrícula, el tipo de datos (IP/máscara, puerta de enlace o MTU), y los valores actuales.

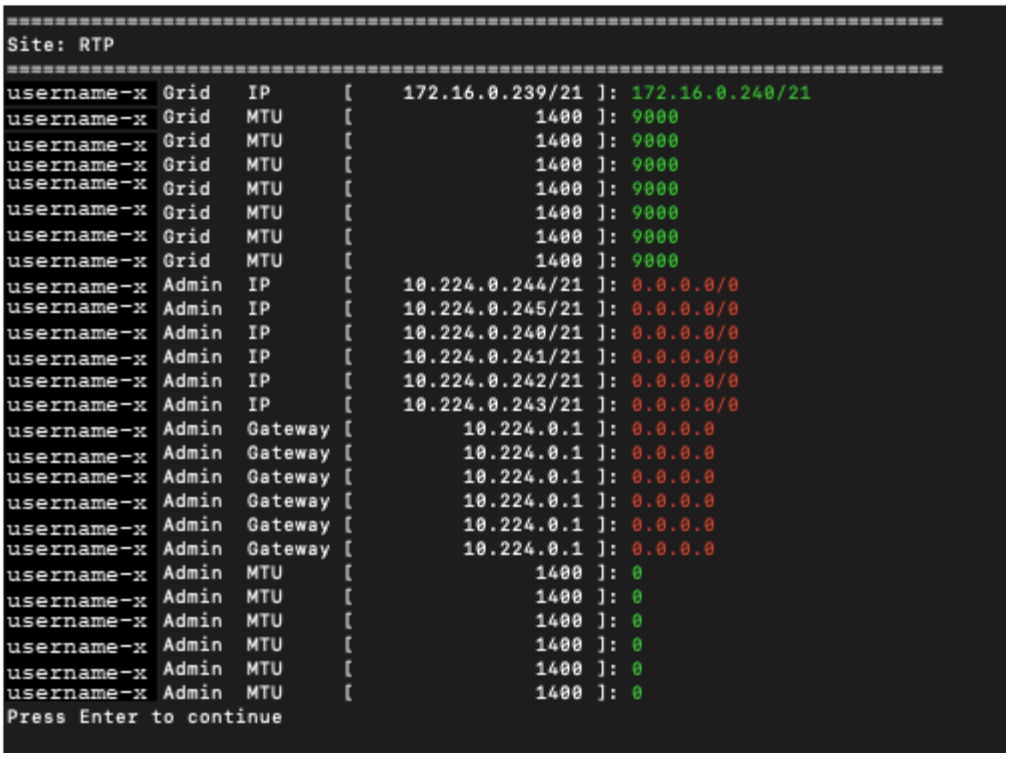
      Si se edita la dirección IP, la longitud del prefijo, la puerta de enlace o la MTU de una interfaz configurada para DHCP, la interfaz se cambiará a estática. Se muestra una advertencia antes de cada interfaz configurada por DHCP.

   Las interfaces se han configurado como `fixed` no se puede editar.

   a. Para establecer un nuevo valor, introdúzcalo en el formato que se muestra para el valor actual.
   b. Después de editar todos los nodos que desea cambiar, introduzca **q** para volver al menú principal.

      Los cambios se mantienen hasta que se borran o se aplican.

6. Revise los cambios seleccionando una de las siguientes opciones:
   - **5**: Muestra las ediciones en la salida que está aislada para mostrar sólo el elemento cambiado. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones), como se muestra en la salida de ejemplo:



- **6**: Muestra las ediciones en salida que muestran la configuración completa. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones).

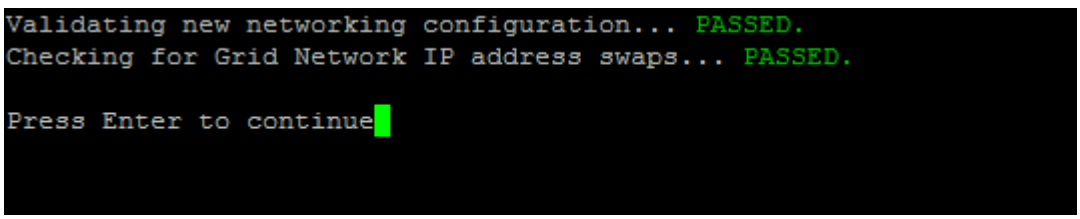
> Algunas interfaces de línea de comandos pueden mostrar adiciones y eliminaciones utilizando formato de tachado. La visualización adecuada depende del cliente de terminal que admita las secuencias de escape de VT100 necesarias.

7. Seleccione la opción **7** para validar todos los cambios.

   Esta validación garantiza que no se violen las reglas para la red de grid, como no utilizar subredes superpuestas.

   En este ejemplo, la validación devolvió errores.

   En este ejemplo, se ha aprobado la validación.



8. Después de la validación, seleccione **10** para aplicar la nueva configuración de red.
9. Seleccione **Stage** para aplicar los cambios la próxima vez que se reinicien los nodos.

> Debe seleccionar **fase**. No realice un reinicio gradual, ya sea manualmente o seleccionando **Aplicar** en lugar de **STAGE**; la cuadrícula no se iniciará correctamente.

10. Una vez que haya finalizado el cambio, seleccione **0** para salir de la herramienta Cambiar IP.
11. Apague todos los nodos de forma simultánea.

> Todo el grid debe cerrarse, de modo que todos los nodos estén inactivos al mismo tiempo.

12. Realice los cambios necesarios en la red virtual o física.
13. Verifique que todos los nodos de grid estén inactivos.
14. Encienda todos los nodos.
15. Después de que la cuadrícula se inicie correctamente:
    a. Si añadió servidores NTP nuevos, elimine los valores anteriores del servidor NTP.
    b. Si añadió nuevos servidores DNS, elimine los antiguos valores de servidor DNS.
16. Descargue el nuevo paquete de recuperación desde Grid Manager.
    a. Seleccione **MANTENIMIENTO** > **sistema** > **paquete de recuperación**.
    b. Introduzca la clave de acceso de aprovisionamiento.

Información relacionada

- "Agregar o cambiar listas de subred en Grid Network"
- "Apague el nodo de grid"

Añada interfaces al nodo existente

Linux: Añada interfaces de administrador o de cliente a un nodo existente

Siga estos pasos para añadir una interfaz en la red de administración o la red de cliente a un nodo Linux después de que se haya instalado.

Si no configuró ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET en el archivo de configuración del nodo en el host Linux durante la instalación, utilice este procedimiento para añadir la interfaz. Para obtener más información sobre el archivo de configuración de nodos, consulte las instrucciones del sistema operativo Linux:

- "Instalar StorageGRID en Red Hat Enterprise Linux"
- "Instalar StorageGRID en Ubuntu o Debian"

Realiza este procedimiento en el servidor Linux que aloja el nodo que necesita la nueva asignación de red, no dentro del nodo. Este procedimiento solo añade la interfaz al nodo; se produce un error de validación si intenta especificar cualquier otro parámetro de red.

Para proporcionar información de direccionamiento, debe utilizar la herramienta Cambiar IP. Consulte "Cambie la configuración de red de los nodos".

Pasos

1. Inicie sesión en el servidor Linux que aloja el nodo.
2. Edite el archivo de configuración del nodo: `/etc/storagegrid/nodes/node-name.conf`.

   No especifique ningún otro parámetro de red o se producirá un error de validación.

   a. Agregue una entrada para el nuevo destino de red. Por ejemplo:

      `CLIENT_NETWORK_TARGET = bond0.3206`

   b. Opcional: Agregue una entrada para la dirección MAC. Por ejemplo:

      `CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c`

3. Ejecute el comando node validate:

   `sudo storagegrid node validate node-name`

4. Resolver todos los errores de validación.
5. Ejecute el comando node reload:

   `sudo storagegrid node reload node-name`

Linux: Añada tronco o interfaces de acceso a un nodo

Puede añadir tronco o interfaces de acceso adicionales a un nodo Linux después de instalarlo. Las interfaces que agregue se muestran en la página interfaces de VLAN y la página ha groups.

Antes de empezar

- Tiene acceso a las instrucciones para instalar StorageGRID en su plataforma Linux.
  - "Instalar StorageGRID en Red Hat Enterprise Linux"
  - "Instalar StorageGRID en Ubuntu o Debian"
- Usted tiene la `Passwords.txt` archivo.
- Ya tienes "permisos de acceso específicos".

No intente agregar interfaces a un nodo mientras haya una actualización de software, un procedimiento de recuperación o un procedimiento de expansión activo.

Acerca de esta tarea

Estos pasos permiten añadir una o varias interfaces adicionales a un nodo Linux después de instalar el nodo. Por ejemplo, es posible que desee agregar una interfaz troncal a un nodo de administración o puerta de enlace, de modo que pueda utilizar interfaces VLAN para separar el tráfico que pertenece a diferentes aplicaciones o inquilinos. O bien, es posible que desee añadir una interfaz de acceso para utilizarla en un grupo de alta disponibilidad (ha).

Si añade una interfaz troncal, debe configurar una interfaz VLAN en StorageGRID. Si agrega una interfaz de acceso, puede añadir la interfaz directamente a un grupo de alta disponibilidad; no es necesario configurar una interfaz de VLAN.

El nodo no está disponible durante un breve periodo de tiempo cuando se añaden interfaces. Debe realizar este procedimiento en un nodo por vez.

Pasos

1. Inicie sesión en el servidor Linux que aloja el nodo.
2. Mediante un editor de texto como vim o pico, edite el archivo de configuración del nodo:

   `/etc/storagegrid/nodes/node-name.conf`

3. Agregue una entrada al archivo para especificar el nombre y, opcionalmente, la descripción de cada interfaz adicional que desee agregar al nodo. Utilice este formato.

   `INTERFACE_TARGET_nnnn=value`

   Para *nnnn*, especifique un número único para cada uno `INTERFACE_TARGET` entrada que está agregando.

   En *value*, especifique el nombre de la interfaz física en el host de configuración básica. A continuación, de manera opcional, añada una coma y proporcione una descripción de la interfaz, que se muestra en la página interfaces VLAN y en la página grupos de alta disponibilidad.

   Por ejemplo:

   `INTERFACE_TARGET_0001=ens256, Trunk`

   > No especifique ningún otro parámetro de red o se producirá un error de validación.

4. Ejecute el siguiente comando para validar los cambios en el archivo de configuración del nodo:

   `sudo storagegrid node validate node-name`

   Solucione todos los errores o advertencias antes de continuar con el siguiente paso.

5. Ejecute el siguiente comando para actualizar la configuración del nodo:

   `sudo storagegrid node reload node-name`

Después de terminar

- Si ha añadido una o varias interfaces de línea externa, vaya a. "Configure las interfaces VLAN" Para configurar una o varias interfaces VLAN para cada nueva interfaz principal.
- Si ha añadido una o varias interfaces de acceso, vaya a. "configuración de grupos de alta disponibilidad" Y añadir las nuevas interfaces directamente a los grupos de alta disponibilidad.

VMware: Añada tronco o interfaces de acceso a un nodo

Puede añadir un enlace troncal o una interfaz de acceso a un nodo de máquina virtual una vez que se ha instalado el nodo. Las interfaces que agregue se muestran en la página interfaces de VLAN y la página ha groups.

Antes de empezar

- Tiene acceso a las instrucciones para "Instalación de StorageGRID en su plataforma VMware".

- Tiene máquinas virtuales VMware Node de administrador y Gateway Node.
- Tiene una subred de red que no se utiliza como Grid, Admin o Client Network.
- Usted tiene la `Passwords.txt` archivo.
- Ya tienes "permisos de acceso específicos".

> No intente agregar interfaces a un nodo mientras haya una actualización de software, un procedimiento de recuperación o un procedimiento de expansión activo.

Acerca de esta tarea

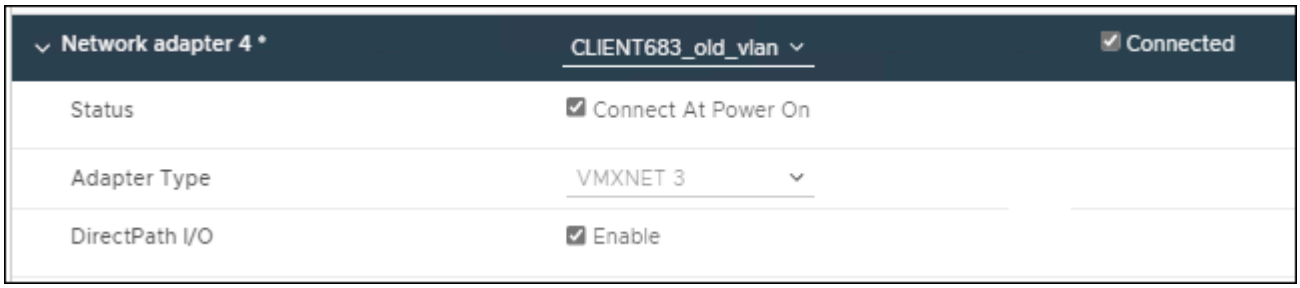
Siga estos pasos para añadir una o varias interfaces adicionales a un nodo de VMware después de instalar el nodo. Por ejemplo, es posible que desee agregar una interfaz troncal a un nodo de administración o puerta de enlace, de modo que pueda utilizar interfaces VLAN para separar el tráfico que pertenece a diferentes aplicaciones o inquilinos. O bien, puede que desee añadir una interfaz de acceso para utilizarla en un grupo de alta disponibilidad.

Si añade una interfaz troncal, debe configurar una interfaz VLAN en StorageGRID. Si agrega una interfaz de acceso, puede añadir la interfaz directamente a un grupo de alta disponibilidad; no es necesario configurar una interfaz de VLAN.

Es posible que el nodo no esté disponible durante un breve periodo de tiempo cuando se añaden interfaces.

Pasos

1. En vCenter, añada un nuevo adaptador de red (tipo VMXNEL3) a una máquina virtual de nodo de administración y nodo de puerta de enlace. Seleccione las casillas de verificación **Connected** y **Connect at Power On**.



2. Use SSH para iniciar sesión en el nodo de administrador o en el nodo de puerta de enlace.
3. Uso `ip link show` para confirmar que se ha detectado la nueva interfaz de red ens256.

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

Después de terminar

- Si ha añadido una o varias interfaces de línea externa, vaya a. "Configure las interfaces VLAN" Para configurar una o varias interfaces VLAN para cada nueva interfaz principal.
- Si ha añadido una o varias interfaces de acceso, vaya a. "configuración de grupos de alta disponibilidad" Y añadir las nuevas interfaces directamente a los grupos de alta disponibilidad.

Configurar servidores DNS

Puede agregar, actualizar y eliminar servidores DNS, de manera que pueda utilizar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP.

Para utilizar nombres de dominio completos (FQDN) en lugar de direcciones IP al especificar nombres de host para destinos externos, especifique la dirección IP de cada servidor DNS que utilizará. Estas entradas se utilizan para AutoSupport, correos electrónicos de alerta, notificaciones SNMP, extremos de servicios de plataforma, pools de almacenamiento en la nube, y mucho más.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Tiene las direcciones IP de los servidores DNS que se van a configurar.

Acerca de esta tarea

Para garantizar que el funcionamiento sea correcto, especifique dos o tres servidores DNS. Si especifica más de tres, es posible que solo se utilicen tres debido a las limitaciones conocidas del sistema operativo en algunas plataformas. Si tiene restricciones de enrutamiento en su entorno, puede "Personalice la lista de servidores DNS" Para nodos individuales (normalmente todos los nodos en un sitio) para usar un conjunto diferente de hasta tres servidores DNS.

Si es posible, utilice servidores DNS a los que cada sitio puede acceder localmente para asegurarse de que un sitio islandn pueda resolver los FQDN para destinos externos.

Añada un servidor DNS

Siga estos pasos para agregar un servidor DNS.

Pasos

1. Seleccione **MANTENIMIENTO** > **Red** > **Servidores DNS**.
2. Seleccione **Agregar otro servidor** para agregar un servidor DNS.
3. Seleccione **Guardar**.

Modificar un servidor DNS

Siga estos pasos para modificar un servidor DNS.

Pasos

1. Seleccione **MANTENIMIENTO** > **Red** > **Servidores DNS**.
2. Seleccione la dirección IP del nombre del servidor que desea editar y realice los cambios necesarios.
3. Seleccione **Guardar**.

Eliminar un servidor DNS

Siga estos pasos para eliminar una dirección IP de un servidor DNS.

Pasos

1. Seleccione **MANTENIMIENTO** > **Red** > **Servidores DNS**.
2. Seleccione el icono de eliminar Junto a la dirección IP.
3. Seleccione **Guardar**.

Modifique la configuración de DNS para un solo nodo de grid

En lugar de configurar el DNS globalmente para toda la implementación, puede ejecutar un script para configurar DNS de manera diferente para cada nodo de grid.

En general, debe utilizar la opción **MANTENIMIENTO** > **Red** > **Servidores DNS** en Grid Manager para configurar los servidores DNS. Utilice la siguiente secuencia de comandos sólo si necesita usar servidores DNS diferentes para nodos de cuadrícula diferentes.

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

   e. Añada la clave privada SSH al agente SSH. Introduzca: `ssh-add`
   f. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.

2. Inicie sesión en el nodo que desea actualizar con una configuración DNS personalizada: `ssh node_IP_address`
3. Ejecute el script de configuración de DNS: `setup_resolv.rb`.

   El script responde con la lista de comandos admitidos.

```
Tool to modify external name servers

available commands:
  add search <domain>
              add a specified domain to search list
              e.g.> add search netapp.com
  remove search <domain>
              remove a specified domain from list
              e.g.> remove search netapp.com
  add nameserver <ip>
              add a specified IP address to the name server list
              e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
              remove a specified IP address from list
              e.g.> remove nameserver 192.0.2.65
  remove nameserver all
              remove all nameservers from list
  save        write configuration to disk and quit
  abort       quit without saving changes
  help        display this help message


Current list of name servers:
    192.0.2.64
Name servers inherited from global DNS configuration:
    192.0.2.126
    192.0.2.127
Current list of search entries:
    netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
             [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

4. Añada la dirección IPv4 de un servidor que proporcione servicio de nombres de dominio para la red: `add <nameserver IP_address>`
5. Repita el `add nameserver` comando para agregar servidores de nombres.
6. Siga las instrucciones que se le indiquen para otros comandos.

7. Guarde los cambios y salga de la aplicación: `save`
8. cierre el shell de comandos en el servidor: `exit`
9. Para cada nodo de cuadrícula, repita los pasos desde inicie sesión en el nodo por cierre del shell de comandos.
10. Cuando ya no necesite un acceso sin contraseñas a otros servidores, quite la clave privada del agente SSH. Introduzca: `ssh-add -D`

Gestione servidores NTP

Puede añadir, actualizar o quitar servidores de protocolo de tiempo de redes (NTP) para garantizar que los datos se sincronicen de forma precisa entre los nodos de grid del sistema StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento.
- Tiene las direcciones IPv4 de los servidores NTP para configurar.

Cómo utiliza StorageGRID NTP

El sistema StorageGRID utiliza el protocolo de hora de redes (NTP) para sincronizar la hora entre todos los nodos de grid de la cuadrícula.

Se asigna el rol NTP principal en cada sitio, al menos dos nodos del sistema StorageGRID. Se sincronizan con un mínimo sugerido de cuatro, y un máximo de seis, fuentes de tiempo externas y entre sí. Todos los nodos del sistema StorageGRID que no son un nodo NTP principal actúan como cliente NTP y se sincronizan con estos nodos NTP principales.

Los servidores NTP externos se conectan a los nodos a los que se asignaron anteriormente roles NTP primarios. Por este motivo, se recomienda especificar al menos dos nodos con roles NTP principales.

Directrices del servidor NTP

Siga estas directrices para protegerse contra problemas de tiempo:

- Los servidores NTP externos se conectan a los nodos a los que se asignaron anteriormente roles NTP primarios. Por este motivo, se recomienda especificar al menos dos nodos con roles NTP principales.
- Asegúrese de que al menos dos nodos en cada sitio puedan acceder al menos a cuatro orígenes NTP externos. Si solo un nodo de un sitio puede acceder a los orígenes NTP, se producirán problemas de tiempo si ese nodo falla. Además, designar dos nodos por sitio como orígenes NTP primarios garantiza una sincronización precisa si un sitio está aislado del resto de la cuadrícula.
- Los servidores NTP externos especificados deben usar el protocolo NTP. Debe especificar las referencias del servidor NTP de estratum 3 o superior para evitar problemas con la desviación del tiempo.

> Al especificar el origen NTP externo para una instalación de StorageGRID en el nivel de producción, no use el servicio Windows Time (W32Time) en una versión de Windows anterior a Windows Server 2016. El servicio de hora en versiones anteriores de Windows no es lo suficientemente preciso y no es compatible con Microsoft para su uso en entornos de alta precisión, incluido StorageGRID. Para obtener más información, consulte "Límite de soporte para configurar el servicio de tiempo de Windows para entornos de alta precisión".

Configure los servidores NTP

Siga estos pasos para agregar, actualizar o eliminar servidores NTP.

Pasos

1. Seleccione **MANTENIMIENTO** > **Red** > **Servidores NTP**.
2. En la sección Servidores, agregue, actualice o elimine entradas del servidor NTP, según sea necesario.

   Debe incluir al menos cuatro servidores NTP y puede especificar hasta seis servidores.

3. Introduzca la contraseña de aprovisionamiento para su sistema StorageGRID y, a continuación, seleccione **Guardar**.

   La página está deshabilitada hasta que se completen las actualizaciones de configuración.

   > Si todos los servidores NTP no superan la prueba de conexión después de guardar los nuevos servidores NTP, no continúe. Póngase en contacto con el soporte técnico.

Resuelva problemas del servidor NTP

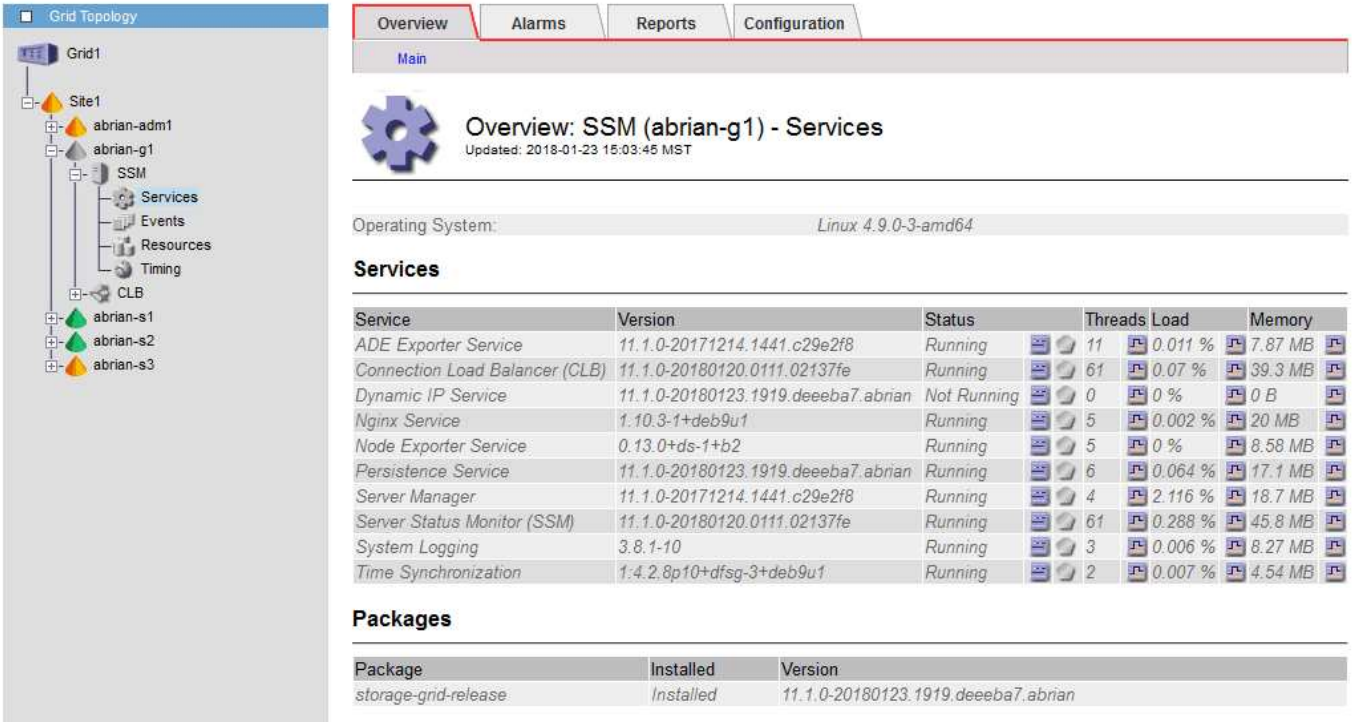
Si tiene problemas con la estabilidad o disponibilidad de los servidores NTP especificados originalmente durante la instalación, puede actualizar la lista de orígenes NTP externos que utiliza el sistema StorageGRID agregando servidores adicionales o actualizando o quitando servidores existentes.

Restaure la conectividad de red para nodos aislados

En determinadas circunstancias, como los cambios de dirección IP en todo el sitio o en la cuadrícula, es posible que uno o más grupos de nodos no puedan ponerse en contacto con el resto de la cuadrícula.

Acerca de esta tarea

En Grid Manager (**SUPPORT** > **Tools** > **Grid topolog**), si un nodo es gris, o si un nodo es azul con muchos de sus servicios que muestran un estado distinto de la ejecución, debe comprobar el aislamiento de nodo.



Entre las consecuencias de tener nodos aislados se incluyen las siguientes:

- Si se aíslan varios nodos, es posible que no pueda iniciar sesión o acceder a Grid Manager.
- Si se aíslan varios nodos, es posible que los valores de cuota y uso de almacenamiento que se muestran en la consola del administrador de inquilinos estén desactualizados. Los totales se actualizarán cuando se restaure la conectividad de red.

Para resolver el problema de aislamiento, se ejecuta una utilidad de línea de comandos en cada nodo aislado o en un nodo de un grupo (todos los nodos de una subred que no contiene el nodo de administración principal) que está aislado de la cuadrícula. La utilidad proporciona a los nodos la dirección IP de un nodo no aislado en la cuadrícula, lo que permite que el nodo aislado o grupo de nodos vuelva a ponerse en contacto con toda la cuadrícula.

Si el sistema de nombres de dominio de multidifusión (mDNS) está desactivado en las redes, es posible que la utilidad de línea de comandos tenga que ejecutarse en cada nodo aislado.

Pasos

1. Acceda al nodo y compruebe `/var/local/log/dynip.log` para mensajes de aislamiento.

   Por ejemplo:

   ```
   [2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
   no contact with other nodes.
   If this warning persists, manual action might be required.
   ```

   Si utiliza la consola de VMware, contendrá un mensaje que podría aislar el nodo.

   En las implementaciones de Linux, aparecerán mensajes de aislamiento en la `/var/log/storagegrid/node/<nodename>.log` archivos.

2. Si los mensajes de aislamiento son recurrentes y persistentes, ejecute el siguiente comando:

   `add_node_ip.py <address>`

   donde `<address>` Es la dirección IP de un nodo remoto conectado al grid.

   ```
   # /usr/sbin/add_node_ip.py  10.224.4.210

   Retrieving local host information
   Validating remote node at address 10.224.4.210
   Sending node IP hint for 10.224.4.210 to local node
   Local node found on remote node. Update complete.
   ```

3. Verifique lo siguiente para cada nodo que estaba aislado previamente:
   - Los servicios del nodo han comenzado.
   - El estado del servicio Dynamic IP es Running después de ejecutar el `storagegrid-status` comando.
   - En el árbol de topología de cuadrícula, el nodo ya no aparece desconectado del resto de la cuadrícula.

> Si ejecuta el `add_node_ip.py` el comando no resuelve el problema; podrían existir otros problemas de red que deban resolverse.

Procedimientos de host y middleware

Linux: Migre el nodo de grid a un nuevo host

Puede migrar uno o varios nodos StorageGRID de un host Linux (el *host de origen*) a otro host Linux (el *host de destino*) a fin de realizar el mantenimiento del host sin que la funcionalidad o la disponibilidad del grid se vean afectadas.

Por ejemplo, es posible que desee migrar un nodo para realizar la aplicación de parches y el reinicio del sistema operativo.

Antes de empezar

- Ha planificado su implementación de StorageGRID para incluir el soporte para la migración.
  - "Requisitos de migración de contenedores de nodos para Red Hat Enterprise Linux"
  - "Requisitos de migración de contenedores de nodos para Ubuntu o Debian"
- El host de destino ya está preparado para el uso de StorageGRID.
- El almacenamiento compartido se utiliza para todos los volúmenes de almacenamiento por nodo
- Las interfaces de red tienen nombres consistentes entre los hosts.

En una implementación de producción, no ejecute más de un nodo de almacenamiento en un único host. El uso de un host dedicado para cada nodo de almacenamiento proporciona un dominio de fallo aislado.

Existen otros tipos de nodos, como los nodos de administrador o los nodos de pasarela, que se pueden implementar en el mismo host. Sin embargo, si tiene varios nodos del mismo tipo (dos nodos de Gateway, por ejemplo), no instale todas las instancias en el mismo host.

Exportar nodo desde el host de origen

Como primer paso, cierre el nodo de la cuadrícula y expórtelo desde el host de Linux de origen.

Ejecute los siguientes comandos en el *source host*.

Pasos

1. Obtenga el estado de todos los nodos que actualmente se ejecutan en el host de origen.

   ```
   sudo storagegrid node status all
   ```

   Resultado de ejemplo:

   ```
   Name Config-State Run-State
   DC1-ADM1 Configured Running
   DC1-ARC1 Configured Running
   DC1-GW1 Configured Running
   DC1-S1 Configured Running
   DC1-S2 Configured Running
   DC1-S3 Configured Running
   ```

2. Identifique el nombre del nodo que desea migrar y pararlo si su estado de ejecución está en ejecución.

   ```
   sudo storagegrid node stop DC1-S3
   ```

   Resultado de ejemplo:

   ```
   Stopping node DC1-S3
   Waiting up to 630 seconds for node shutdown
   ```

3. Exporte el nodo desde el host de origen.

   ```
   sudo storagegrid node export DC1-S3
   ```

   Resultado de ejemplo:

   ```
   Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.
   Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you
   want to import it again.
   ```

4. Tome nota de la `import` comando sugerido en el resultado.

   Este comando se ejecutará en el host de destino en el paso siguiente.

Importar nodo en host de destino

Después de exportar el nodo desde el host de origen, debe importar y validar el nodo en el host de destino. La validación confirma que el nodo tiene acceso a los mismos dispositivos de interfaz de red y de almacenamiento basado en bloques que los que tenía en el host de origen.

Ejecute los siguientes comandos en el *host de destino*.

Pasos

1. Importe el nodo en el host de destino.

   ```
   sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
   ```

   Resultado de ejemplo:

   ```
   Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.
   You should run 'storagegrid node validate DC1-S3'
   ```

2. Valide la configuración del nodo en el host nuevo.

   ```
   sudo storagegrid node validate DC1-S3
   ```

   Resultado de ejemplo:

   ```
   Confirming existence of node DC1-S3... PASSED
   Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node
   DC1-S3... PASSED
   Checking for duplication of unique values... PASSED
   ```

3. Si se produce algún error de validación, haga una dirección antes de iniciar el nodo migrado.

   Para obtener información sobre la solución de problemas, consulte las instrucciones de instalación de StorageGRID para el sistema operativo Linux.

   - "Instalar StorageGRID en Red Hat Enterprise Linux"
   - "Instalar StorageGRID en Ubuntu o Debian"

Inicie el nodo migrado

Después de validar el nodo migrado, inicie el nodo ejecutando un comando en el *host de destino*.

Pasos

1. Inicie el nodo en el host nuevo.

   ```
   sudo storagegrid node start DC1-S3
   ```

2. Inicie sesión en Grid Manager y compruebe que el estado del nodo es verde sin alerta.

   Comprobar que el estado del nodo sea verde garantiza que el nodo migrado se haya reiniciado completamente y se vuelva a unir al grid. Si el estado no es verde, no migre ningún nodo adicional para que no tenga más de un nodo fuera de servicio.

3. Si no puede acceder a Grid Manager, espere 10 minutos y, a continuación, ejecute el siguiente comando:

   ```
   sudo storagegrid node status _node-name
   ```

   Confirme que el nodo migrado tiene un estado Run-State de Running.

Mantenimiento de nodos de archivado para middleware TSM

Los nodos de archivado pueden configurarse para dar como objetivo una cinta mediante un servidor de middleware de TSM o el cloud a través de la API S3. Una vez completada la configuración, no se puede cambiar el destino de un nodo de archivado.

Si el servidor que aloja el nodo de archivado falla, sustituya el servidor y siga el procedimiento de recuperación adecuado.

Fallo en dispositivos de almacenamiento de archivado

Si determina que hay un error en el dispositivo de almacenamiento de archivado al que está accediendo el nodo de archivado a través de Tivoli Storage Manager (TSM), desconecte el nodo de archivado para limitar el número de alarmas mostradas en el sistema StorageGRID. Entonces, puede utilizar las herramientas administrativas del servidor de TSM o del dispositivo de almacenamiento, o ambas, para diagnosticar y resolver el problema.

Desconecte el componente de destino

Antes de llevar a cabo cualquier mantenimiento del servidor de middleware TSM que pudiera hacer que no esté disponible para el nodo de archivado, desconecte el componente de destino para limitar el número de alarmas que se activan si el servidor de middleware TSM deja de estar disponible.

Antes de empezar

Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione **nodo de archivo** > **ARC** > **objetivo** > **Configuración** > **Principal**.
3. Cambie el valor de Estado de Tivoli Storage Manager a **sin conexión** y haga clic en **aplicar cambios**.
4. Una vez finalizado el mantenimiento, cambie el valor de estado de Tivoli Storage Manager a **Online** y haga clic en **aplicar cambios**.

Herramientas administrativas de Tivoli Storage Manager

La herramienta dsmadmc es la consola administrativa del servidor de middleware TSM que está instalado en el nodo de archivado. Puede acceder a la herramienta escribiendo `dsmadmc` en la línea de comandos del servidor. Inicie sesión en la consola administrativa con el mismo nombre de usuario administrativo y contraseña configurados para el servicio ARC.

La `tsmquery.rb` se creó una secuencia de comandos para generar información de estado de dsmadmc de forma más legible. Este script se puede ejecutar introduciendo el siguiente comando en la línea de comandos del nodo de archivado: `/usr/local/arc/tsmquery.rb status`

Para obtener más información acerca del dsmadmc de la consola administrativa de TSM, consulte *Tivoli Storage Manager for Linux: Administrator's Reference*.

Objeto no disponible de forma permanente

Cuando el nodo de archivado solicita un objeto desde el servidor de Tivoli Storage Manager (TSM) y la recuperación falla, el nodo de archivado vuelve a intentar la solicitud después de un intervalo de 10 segundos. Si el objeto no está disponible de forma permanente (por ejemplo, debido a que el objeto está dañado en cinta), la API de TSM no tiene forma de indicarlo en el nodo de archivado, por lo que el nodo de archivado continúa reintentando la solicitud.

Cuando se produce esta situación, se activa una alarma y el valor continúa aumentando. Para ver la alarma, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione **nodo de archivo** > **ARC** > **recuperar** > **fallos de solicitud**.

Si el objeto no está disponible permanentemente, debe identificar el objeto y, a continuación, cancelar manualmente la solicitud del nodo de archivado como se describe en el procedimiento, Determinar si los objetos no están disponibles de forma permanente.

Una recuperación también puede fallar si el objeto no está disponible temporalmente. En este caso, las posteriores solicitudes de recuperación deberían tener éxito en algún momento.

Si el sistema StorageGRID está configurado para utilizar una regla de ILM que crea una única copia de objeto y esa copia no se puede recuperar, el objeto se pierde y no se puede recuperar. Sin embargo, debe seguir el procedimiento para determinar si el objeto no está disponible permanentemente para limpiar el sistema StorageGRID, cancelar la solicitud del nodo de archivado y depurar los metadatos del objeto perdido.

Determinar si los objetos no están disponibles de forma permanente

Puede determinar si los objetos no están disponibles de forma permanente realizando una solicitud mediante la consola administrativa de TSM.

Antes de empezar

- Ya tienes "permisos de acceso específicos".
- Usted tiene la `Passwords.txt` archivo.
- Tiene la dirección IP de un nodo de administración.

Acerca de esta tarea

Este ejemplo se proporciona para su información. Este procedimiento no puede ayudarle a identificar todas las condiciones de fallo que podrían dar lugar a objetos o volúmenes de cinta no disponibles. Para obtener información acerca de la administración de TSM, consulte la documentación de TSM Server.

Pasos

1. Inicie sesión en un nodo de administrador:
   a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
2. Identifique el objeto o objetos que no ha podido recuperar el nodo de archivado:

a. Vaya al directorio que contiene los archivos del registro de auditoría: `cd /var/local/log`

   El archivo de registro de auditoría activo se denomina audit.log. Una vez al día, el activo `audit.log` el archivo se guardará y se guardará un nuevo `audit.log` se ha iniciado el archivo. El nombre del archivo guardado indica cuándo se guardó, en el formato `yyyy-mm-dd.txt`. Después de un día, el archivo guardado se comprime y cambia su nombre, en el formato `yyyy-mm-dd.txt.gz`, que conserva la fecha original.

b. Busque en el archivo de registro de auditoría correspondiente los mensajes que indican que no se puede recuperar un objeto archivado. Por ejemplo, introduzca: `grep ARCE audit.log | less -n`

   Cuando un objeto no se puede recuperar de un nodo de archivado, el mensaje de auditoría de ARCE (fin de recuperación de objeto de archivado) muestra ARUN (middleware de archivo no disponible) o GERR (error general) en el campo Resultado. La siguiente línea de ejemplo del registro de auditoría muestra que EL mensaje ARCE terminó con el resultado ARUN para CBID 498D8A1F681F05B3.

```
[AUDT:[CBID(UI64):0x498D8A1F681F05B3][VLID(UI64):□20091127][RSLT(FC32
):ARUN][AVER(UI32):7]
[ATIM(UI64):1350613602969243][ATYP(FC32):ARCE][ANID(UI32):13959984][A
MID(FC32):ARCI]
[ATID(UI64):4560349751312520631]]
```

   Para obtener más información, consulte las instrucciones para comprender los mensajes de auditoría.

c. Registre el CBID de cada objeto que tenga un fallo en la solicitud.

   También es posible que desee registrar la siguiente información adicional utilizada por TSM para identificar los objetos guardados por el nodo de archivado:

   - **Nombre del espacio de archivos**: Equivalente al ID del nodo de archivado. Para encontrar el ID de nodo de archivado, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione **nodo de archivo** > **ARC** > **objetivo** > **Descripción general**.
   - **Nombre de alto nivel**: Equivalente al ID de volumen asignado al objeto por el nodo de archivado. El ID del volumen tiene el formato de una fecha (por ejemplo, `20091127`), y se registra como el VLID del objeto en el archivo de mensajes de auditoría.
   - **Nombre de nivel bajo**: Equivalente al CBID asignado a un objeto por el sistema StorageGRID.

d. Cierre la sesión del shell de comandos: `exit`

3. Compruebe el servidor TSM para ver si los objetos identificados en el paso 2 no están disponibles de forma permanente:

   a. Inicie sesión en la consola administrativa del servidor TSM: `dsmadmc`

      Utilice el nombre de usuario administrativo y la contraseña configurados para el servicio ARC. Introduzca el nombre de usuario y la contraseña en Grid Manager. (Para ver el nombre de usuario, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione **nodo de archivo** > **ARC** > **objetivo** > **Configuración**.)

   b. Determine si el objeto no está disponible de forma permanente.

      Por ejemplo, puede buscar en el registro de actividades de TSM un error de integridad de datos para

ese objeto. En el ejemplo siguiente se muestra una búsqueda del registro de actividad del último día de un objeto con CBID `498D8A1F681F05B3`.

```
> query actlog begindate=-1 search=276C14E94082CC69
12/21/2008 05:39:15 ANR0548W Retrieve or restore
failed for session 9139359 for node DEV-ARC-20 (Bycast ARC)
processing file space /19130020 4 for file /20081002/
498D8A1F681F05B3 stored as Archive - data
integrity error detected. (SESSION: 9139359)
>
```

En función de la naturaleza del error, es posible que el CBID no se registre en el registro de actividades de TSM. Es posible que sea necesario buscar el registro para otros errores de TSM alrededor del momento en que se produce el fallo de la solicitud.

c. Si una cinta completa no está disponible de forma permanente, identifique los CBID de todos los objetos almacenados en ese volumen: `query content TSM_Volume_Name`

donde `TSM_Volume_Name` Es el nombre de TSM para la cinta no disponible. A continuación se muestra un ejemplo del resultado de este comando:

```
 > query content TSM-Volume-Name
Node Name     Type Filespace  FSID Client's Name for File Name
------------- ---- ---------- ---- --------------------------
DEV-ARC-20    Arch /19130020  216  /20081201/ C1D172940E6C7E12
DEV-ARC-20    Arch /19130020  216  /20081201/ F1D7FBC2B4B0779E
```

La `Client's Name for File Name` Es el mismo que el ID de volumen del nodo de archivado (o TSM «nombre de nivel superior») seguido del CBID del objeto (o «nombre de nivel inferior» de TSM). Es decir, la `Client's Name for File Name` toma la forma `/Archive Node volume ID /CBID`. En la primera línea del resultado de ejemplo, la `Client's Name for File Name` es `/20081201/ C1D172940E6C7E12`.

Recuerde también que el `Filespace` Es el ID de nodo del nodo de archivado.

Necesitará el CBID de cada objeto almacenado en el volumen y el ID de nodo del nodo de archivado para cancelar la solicitud de recuperación.

4. Para cada objeto que no esté disponible de forma permanente, cancele la solicitud de recuperación y emita un comando para informar al sistema StorageGRID de que la copia de objeto se ha perdido:

> Use la Consola de ADE con precaución. Si la consola se utiliza incorrectamente, es posible interrumpir las operaciones del sistema y dañar los datos. Introduzca los comandos detenidamente y utilice únicamente los comandos documentados en este procedimiento.

a. Si aún no ha iniciado sesión en el nodo de archivado, inicie sesión de la siguiente manera:

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

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

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

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

b. Acceder a la consola ADE del servicio ARC: `telnet localhost 1409`

c. Cancelar la solicitud del objeto: `/proc/BRTR/cancel -c CBID`

donde `CBID` Es el identificador del objeto que no se puede recuperar del TSM.

Si las únicas copias del objeto están en cinta, la solicitud de recuperación masiva se cancela con un mensaje que indica que 1 solicitudes canceladas. Si existen copias del objeto en otro lugar del sistema, la recuperación del objeto se procesa mediante un módulo diferente, por lo que la respuesta al mensaje es “0 solicitudes canceladas”.

d. Emita un comando para notificar al sistema StorageGRID que se ha perdido una copia de objeto y que se debe realizar una copia adicional: `/proc/CMSI/Object_Lost CBID node_ID`

donde `CBID` Es el identificador del objeto que no se puede recuperar del servidor TSM, y. `node_ID` Es el ID de nodo del nodo de archivado en el que se produjo un error en la recuperación.

Debe introducir un comando independiente para cada copia de objeto perdida: No se admite la introducción de un rango de CBID.

En la mayoría de los casos, el sistema StorageGRID empieza inmediatamente a realizar copias adicionales de datos de objetos para garantizar que se sigue la política de ILM del sistema.

Sin embargo, si la regla de ILM para el objeto especifica que se debe hacer una sola copia y que ahora se ha perdido esa copia, el objeto no se puede recuperar. En este caso, ejecute el `Object_Lost` El comando purga los metadatos del objeto perdido desde el sistema StorageGRID.

Cuando la `Object_Lost` el comando se completa correctamente y se muestra el siguiente mensaje:

```
CLOC_LOST_ANS returned result 'SUCS'
```

+

> La `/proc/CMSI/Object_Lost` El comando sólo es válido para los objetos perdidos que se almacenan en nodos de archivado.

a. Salga de la Consola de ADE: `exit`

b. Cierre la sesión del nodo de archivado: `exit`

5. Restablezca el valor de los fallos de solicitud en el sistema StorageGRID:

a. Vaya a **nodo de archivo** > **ARC** > **recuperar** > **Configuración** y seleccione **Restablecer recuento de fallos de solicitud**.

b. Haga clic en **aplicar cambios**.

Información relacionada

"Administre StorageGRID"

"Revisar los registros de auditoría"

VMware: Configure la máquina virtual para el reinicio automático

Si la máquina virtual no se reinicia después de reiniciar el hipervisor de VMware vSphere, es posible que deba configurar la máquina virtual para el reinicio automático.

Debe realizar este procedimiento si observa que una máquina virtual no se reinicia mientras recupera un nodo de cuadrícula o realiza otro procedimiento de mantenimiento.

Pasos

1. En el árbol de VMware vSphere Client, seleccione la máquina virtual que no se ha iniciado.
2. Haga clic con el botón derecho del ratón en la máquina virtual y seleccione **encendido**.
3. Configure VMware vSphere Hypervisor para reiniciar la máquina virtual de forma automática en el futuro.

Recupere o sustituya nodos

Procedimientos de recuperación de nodos de grid: Descripción general

Si falla un nodo de cuadrícula, puede recuperarlo reemplazando el servidor físico o virtual que ha fallado, reinstalando el software StorageGRID y restaurando los datos recuperables.

Los nodos de grid pueden fallar si un error de hardware, virtualización, sistema operativo o software hace que el nodo no se pueda utilizar o no sea fiable. Existen muchos tipos de errores que pueden desencadenar la necesidad de recuperar un nodo de grid.

Los pasos para recuperar un nodo de cuadrícula varían dependiendo de la plataforma en la que se encuentre el nodo de cuadrícula y del tipo de nodo de cuadrícula. Cada tipo de nodo de cuadrícula tiene un procedimiento de recuperación específico, que se debe seguir exactamente.

Generalmente, intenta conservar los datos del nodo de cuadrícula con errores siempre que sea posible, reparar o reemplazar el nodo con error, utilizar el administrador de grid para configurar el nodo de sustitución y restaurar los datos del nodo.

> Si se produce un error en todo un sitio de StorageGRID, póngase en contacto con el soporte técnico. El soporte técnico trabajará con usted para desarrollar y ejecutar un plan de recuperación de sitios que maximice la cantidad de datos que se recuperan y, asimismo, cumpla sus objetivos empresariales. Consulte "Cómo el soporte técnico recupera un sitio".

Advertencias y consideraciones sobre los procesos de recuperación de nodos de grid

Si un nodo de grid falla, debe recuperarlo Lo antes posible.. Antes de empezar, debe revisar todas las advertencias y consideraciones de la recuperación de nodos.

> StorageGRID es un sistema distribuido compuesto por varios nodos que funcionan entre sí. No utilice instantáneas de disco para restaurar nodos de grid. En su lugar, consulte los procedimientos de recuperación y mantenimiento de cada tipo de nodo.

Entre los motivos para recuperar un Lo antes posible. de nodo de Grid con errores se incluyen los siguientes:

- Un nodo de grid fallido puede reducir la redundancia de los datos del sistema y del objeto, lo que le deja vulnerable al riesgo de pérdida permanente de datos si falla otro nodo.
- Un nodo de grid fallido puede afectar la eficiencia de las operaciones diarias de-a-.
- Un nodo de grid con errores puede reducir su capacidad para supervisar las operaciones del sistema.
- Un nodo de grid fallido puede provocar un error interno de 500 servidores si se aplican reglas estrictas de ILM.
- Si un nodo de grid no se recupera con la rapidez, es posible que aumenten los tiempos de recuperación. Por ejemplo, se podrían desarrollar colas que se deben borrar antes de que se complete la recuperación.

Siga siempre el procedimiento de recuperación para el tipo específico de nodo de cuadrícula que se va a recuperar. Los procedimientos de recuperación varían en función de los nodos de administración principales o no primarios, los nodos de puerta de enlace, los nodos de archivado, los nodos de dispositivos y los nodos de almacenamiento.

Condiciones previas para la recuperación de nodos de grid

Al recuperar nodos de grid, se da por sentado las siguientes condiciones:

- Se reemplazó y configuró el hardware físico o virtual que falló.
- La versión del instalador de dispositivos StorageGRID del dispositivo de sustitución coincide con la versión de software de su sistema StorageGRID, como se describe en "Comprobar y actualizar la versión de StorageGRID Appliance Installer".
- Si recupera un nodo de grid que no es el nodo de administrador principal, hay conectividad entre el nodo de grid que se está recuperando y el nodo de administrador principal.

El orden de recuperación de nodos si se produce un error en un servidor que aloja más de un nodo de grid

Si falla un servidor que aloja más de un nodo de grid, puede recuperar los nodos en cualquier orden. Sin embargo, si el servidor con el fallo aloja el nodo de administración principal, primero debe recuperar dicho nodo. Si se recupera el nodo de administrador principal, primero se impide que las recuperaciones de otros nodos se detenguen a medida que esperan para ponerse en contacto con el nodo de administración principal.

Direcciones IP para nodos recuperados

No intente recuperar un nodo usando una dirección IP que esté actualmente asignada a cualquier otro nodo. Cuando se implementa el nodo nuevo, use la dirección IP actual del nodo con errores o una dirección IP sin usar.

Si utiliza una dirección IP nueva para implementar el nodo nuevo y después recuperar el nodo, la dirección IP nueva se seguirá usando para el nodo recuperado. Si desea revertir a la dirección IP original, utilice la herramienta Change IP una vez completada la recuperación.

Recopile los materiales necesarios para la recuperación de los nodos de grid

Antes de realizar procedimientos de mantenimiento, debe asegurarse de tener los materiales necesarios para recuperar un nodo de cuadrícula con errores.

Elemento	Notas
Archivo de instalación de StorageGRID	Si necesita recuperar un nodo de cuadrícula, debe hacerlo Descargue los archivos de instalación de StorageGRID para su plataforma. **Nota:** No es necesario descargar archivos si está recuperando volúmenes de almacenamiento fallidos en un nodo de almacenamiento.

Elemento	Notas
Portátil de servicio	El portátil de servicio debe tener lo siguiente: • Puerto de red • Cliente SSH (por ejemplo, PuTTY) • "Navegador web compatible"
Paquete de recuperación `.zip` archivo	Obtenga una copia del paquete de recuperación más reciente `.zip` archivo: `sgws-recovery-package-id-revision.zip` El contenido del `.zip` los archivos se actualizan cada vez que se modifica el sistema. Se le indica que guarde la versión más reciente del paquete de recuperación en una ubicación segura después de realizar dichos cambios. Utilice la copia más reciente para recuperarse de fallos de la cuadrícula. Si el nodo de administración principal funciona normalmente, puede descargar el paquete de recuperación desde el Administrador de grid. Seleccione **MANTENIMIENTO** > **sistema** > **paquete de recuperación**. Si no puede acceder a Grid Manager, puede encontrar copias cifradas del paquete de recuperación en algunos nodos de almacenamiento que contienen el servicio ADC. En cada nodo de almacenamiento, examine esta ubicación del paquete de recuperación: `/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg` Utilice el paquete de recuperación con el número de revisión más alto.
`Passwords.txt` archivo	Contiene las contraseñas que se necesitan para acceder a los nodos de grid en la línea de comandos. Incluido en el paquete de recuperación.
Clave de acceso de aprovisionamiento	La frase de contraseña se crea y documenta cuando se instala el sistema StorageGRID por primera vez. La clave de acceso de aprovisionamiento no está en la `Passwords.txt` archivo.
La documentación actual de su plataforma	Visite el sitio web del proveedor de la plataforma para obtener documentación. Para conocer las versiones compatibles actuales de la plataforma, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Descargue y extraiga los archivos de instalación de StorageGRID

Descargue el software y extraiga los archivos, a menos que lo esté "Recuperar volúmenes de almacenamiento con fallos en un nodo de almacenamiento".

Debe utilizar la versión de StorageGRID que se esté ejecutando actualmente en la cuadrícula.

Pasos

1. Determine qué versión del software está instalada actualmente. En la parte superior de Grid Manager, seleccione el icono de ayuda y seleccione **Acerca de**.
2. Vaya a la "Página de descargas de NetApp para StorageGRID".
3. Seleccione la versión de StorageGRID que se está ejecutando actualmente en la cuadrícula.

   Las versiones de software StorageGRID tienen el siguiente formato: `11.x.y`.

4. Inicie sesión con el nombre de usuario y la contraseña de su cuenta de NetApp.
5. Lea el Contrato de licencia de usuario final, seleccione la casilla de verificación y, a continuación, seleccione * Aceptar y continuar *.
6. En la columna **instalar StorageGRID** de la página de descarga, seleccione `.tgz` o. `.zip` archivar para su plataforma.

   La versión que se muestra en el archivo de archivo de instalación debe coincidir con la versión del software que está instalado actualmente.

   Utilice la `.zip` Archivo si está ejecutando Windows.

Plataforma	Archivo de instalación

Red Hat Enterprise Linux	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`

Ubuntu o Debian o dispositivos	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`

VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`

7. Descargue y extraiga el archivo de archivo.
8. Siga el paso adecuado para que su plataforma pueda elegir los archivos que necesite, en función de su plataforma y los nodos de grid que necesita recuperar.

   Las rutas enumeradas en el paso de cada plataforma son relativas al directorio de nivel superior instalado por el archivo de archivado.

9. Si se está recuperando un "Sistema Red Hat Enterprise Linux", seleccione los archivos adecuados.

Ruta y nombre de archivo	Descripción
	Archivo de texto que describe todos los archivos contenidos en el archivo de descarga de StorageGRID.

Ruta y nombre de archivo	Descripción
	Una licencia gratuita que no proporciona ningún derecho de soporte para el producto.
	Paquete DE RPM para instalar las imágenes de los nodos StorageGRID en los hosts RHEL.
	Paquete DE RPM para instalar el servicio de host StorageGRID en los hosts de RHEL.
Herramienta de secuencia de comandos de la implementación	Descripción
	Script Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Una secuencia de comandos Python que se utiliza para automatizar la configuración de los dispositivos StorageGRID.
	Ejemplo de archivo de configuración para utilizar con `configure-storagegrid.py` guión.
	Ejemplo de secuencia de comandos Python que puede utilizar para iniciar sesión en la API de gestión de grid cuando está activado el inicio de sesión único. También puede utilizar este script para ping federate.
	Un archivo de configuración en blanco para usar con el `configure-storagegrid.py` guión.
	Ejemplo de rol y libro de estrategia de Ansible para configurar hosts de RHEL para la puesta en marcha del contenedor StorageGRID. Puede personalizar el rol o el libro de estrategia según sea necesario.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de grid cuando se activa el inicio de sesión único (SSO) mediante Active Directory o ping federate.
	Un guion de ayuda llamado por el compañero `storagegrid-ssoauth-azure.py` Script de Python para realizar interacciones SSO con Azure.

Ruta y nombre de archivo	Descripción
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno StorageGRID que no sea de producción para probar la compatibilidad de la actualización.

1. Si se está recuperando un "Sistema Ubuntu o Debian", seleccione los archivos adecuados.

Ruta y nombre de archivo	Descripción
	Archivo de texto que describe todos los archivos contenidos en el archivo de descarga de StorageGRID.
	Un archivo de licencia de NetApp que no es de producción y que se puede usar para pruebas e implementaciones conceptuales.
	PAQUETE DEB para instalar las imágenes del nodo StorageGRID en hosts de Ubuntu o Debian.
	Suma de comprobación MD5 para el archivo `/debs/storagegrid-webscale-images-version-SHA.deb`.
	PAQUETE DEB para instalar el servicio de host de StorageGRID en hosts de Ubuntu o Debian.
Herramienta de secuencia de comandos de la implementación	Descripción
	Script Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Una secuencia de comandos Python que se utiliza para automatizar la configuración de los dispositivos StorageGRID.
	Ejemplo de secuencia de comandos Python que puede utilizar para iniciar sesión en la API de gestión de grid cuando está activado el inicio de sesión único. También puede utilizar este script para ping federate.

Ruta y nombre de archivo	Descripción
	Ejemplo de archivo de configuración para utilizar con `configure-storagegrid.py` guión.
	Un archivo de configuración en blanco para usar con el `configure-storagegrid.py` guión.
	Ejemplo de rol de Ansible y libro de aplicaciones para configurar hosts Ubuntu o Debian para la implementación del contenedor StorageGRID. Puede personalizar el rol o el libro de estrategia según sea necesario.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de grid cuando se activa el inicio de sesión único (SSO) mediante Active Directory o ping federate.
	Un guion de ayuda llamado por el compañero `storagegrid-ssoauth-azure.py` Script de Python para realizar interacciones SSO con Azure.
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno StorageGRID que no sea de producción para probar la compatibilidad de la actualización.

1. Si se está recuperando un "Sistema VMware", seleccione los archivos adecuados.

Ruta y nombre de archivo	Descripción
	Archivo de texto que describe todos los archivos contenidos en el archivo de descarga de StorageGRID.
	Una licencia gratuita que no proporciona ningún derecho de soporte para el producto.
	El archivo de disco de máquina virtual que se usa como plantilla para crear máquinas virtuales del nodo de grid.

Ruta y nombre de archivo	Descripción
	El archivo de plantilla Abrir formato de virtualización (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar el nodo de administración principal.
	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de administración no primarios.
	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de archivado.
	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de puerta de enlace.
	El archivo de plantilla (`.ovf`) y el archivo de manifiesto (`.mf`) Para implementar nodos de almacenamiento basados en máquinas virtuales.
Herramienta de secuencia de comandos de la implementación	Descripción
	Una secuencia de comandos de shell Bash que se utiliza para automatizar la implementación de nodos de cuadrícula virtual.
	Ejemplo de archivo de configuración para utilizar con `deploy-vsphere-ovftool.sh` guión.
	Script Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Una secuencia de comandos Python que se utiliza para automatizar la configuración de los dispositivos StorageGRID.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de grid cuando se activa el inicio de sesión único (SSO). También puede utilizar este script para ping federate.
	Ejemplo de archivo de configuración para utilizar con `configure-storagegrid.py` guión.

Ruta y nombre de archivo	Descripción
	Un archivo de configuración en blanco para usar con el `configure-storagegrid.py` guión.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de grid cuando se activa el inicio de sesión único (SSO) mediante Active Directory o ping federate.
	Un guion de ayuda llamado por el compañero `storagegrid-ssoauth-azure.py` Script de Python para realizar interacciones SSO con Azure.
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno StorageGRID que no sea de producción para probar la compatibilidad de la actualización.

1. Si va a recuperar un sistema basado en dispositivos de StorageGRID, seleccione los archivos adecuados.

Ruta y nombre de archivo	Descripción
	DEB el paquete para instalar las imágenes de nodo StorageGRID en sus dispositivos.
	Suma de comprobación MD5 para el archivo `/debs/storagegridwebscale-images-version-SHA.deb`.

Para la instalación del dispositivo, estos archivos sólo son necesarios si necesita evitar el tráfico de red. El dispositivo puede descargar los archivos necesarios del nodo de administración principal.

Seleccione el procedimiento de recuperación nodo

Debe seleccionar el procedimiento de recuperación correcto para el tipo de nodo que ha fallado.

Nodo de grid	Procedimiento de recuperación
Más de un nodo de almacenamiento	Póngase en contacto con el soporte técnico. Si se produjo un error en más de un nodo de almacenamiento, el soporte técnico debe facilitar la recuperación para evitar incoherencias de la base de datos que podrían provocar la pérdida de datos. Es posible que sea necesario un procedimiento de recuperación del sitio. "Cómo el soporte técnico recupera un sitio"
Un solo nodo de almacenamiento	El procedimiento de recuperación del nodo de almacenamiento depende del tipo y de la duración del error. "Recupere el sistema de errores de nodo de almacenamiento"
Nodo de administración	El procedimiento Admin Node depende de si se necesita recuperar el nodo de administrador principal o un nodo de administrador que no sea primario. "Recupere desde fallos de nodo de administrador"
Nodo de puerta de enlace	"Recuperarse de fallos de nodo de puerta de enlace".
Nodo de archivado	"Recupere desde errores de nodo de archivado".

Si falla un servidor que aloja más de un nodo de grid, puede recuperar los nodos en cualquier orden. Sin embargo, si el servidor con el fallo aloja el nodo de administración principal, primero debe recuperar dicho nodo. Si se recupera el nodo de administrador principal, primero se impide que las recuperaciones de otros nodos se detenguen a medida que esperan para ponerse en contacto con el nodo de administración principal.

Recupere el sistema de errores de nodo de almacenamiento

Recuperación de fallos en nodos de almacenamiento: Información general

El procedimiento para recuperar un nodo de almacenamiento con errores depende del tipo de error y del tipo de nodo de almacenamiento que se ha producido un error.

Utilice esta tabla para seleccionar el procedimiento de recuperación de un nodo de almacenamiento con errores.

Problema	Acción	Notas
• Se produjo un error en más de un nodo de almacenamiento. • Un segundo nodo de almacenamiento ha fallado menos de 15 días después de un fallo o una recuperación en un nodo de almacenamiento. Esto incluye el caso en el que un nodo de almacenamiento falla mientras se recupera otro nodo de almacenamiento aún está en curso.	Póngase en contacto con el soporte técnico.	Recuperar más de un nodo de almacenamiento (o varios de un nodo de almacenamiento en un plazo de 15 días) puede afectar a la integridad de la base de datos Cassandra, lo que puede provocar la pérdida de datos. El soporte técnico puede determinar cuándo es seguro iniciar la recuperación de un segundo nodo de almacenamiento. **Nota**: Si más de un nodo de almacenamiento que contiene el servicio ADC falla en un sitio, perderá cualquier solicitud de servicio de plataforma pendiente para ese sitio.
Hay un error en más de un nodo de almacenamiento en un sitio o se ha producido un error en todo el sitio.	Póngase en contacto con el soporte técnico. Puede que sea necesario realizar un procedimiento de recuperación del sitio.	El soporte técnico evaluará su situación y desarrollará un plan de recuperación. Consulte "Cómo el soporte técnico recupera un sitio".
Un nodo de almacenamiento se ha desconectado durante más de 15 días.	"Recupere el nodo de almacenamiento en más de 15 días"	Este procedimiento es necesario para garantizar la integridad de la base de datos de Cassandra.
Se produjo un error en un nodo de almacenamiento del dispositivo.	"Recupere el nodo de almacenamiento del dispositivo"	El procedimiento de recuperación de los nodos de almacenamiento del dispositivo es el mismo para todos los errores.
Se produjo un error en uno o más volúmenes de almacenamiento, pero la unidad del sistema está intacta	" Recupérese de un fallo en el volumen de almacenamiento, donde la unidad del sistema está intacta"	Este procedimiento se usa para nodos de almacenamiento basados en software.
La unidad del sistema falló.	"Recupere datos de un fallo de unidad del sistema"	El procedimiento de sustitución del nodo depende de la plataforma de puesta en marcha y de si también ha fallado algún volumen de almacenamiento.

Algunos procedimientos de recuperación de StorageGRID usan Reaper para gestionar las reparaciones de Cassandra. Las reparaciones se realizan automáticamente tan pronto como se hayan iniciado los servicios relacionados o necesarios. Es posible que note la salida de un script que menciona “reaper” o “Cassandra repair”. Si ve un mensaje de error que indica que la reparación ha fallado, ejecute el comando indicado en el mensaje de error.

Recupere el nodo de almacenamiento en más de 15 días

Si un solo nodo de almacenamiento ha estado desconectado y no está conectado a otros nodos de almacenamiento durante más de 15 días, debe reconstruir Cassandra en el nodo.

Antes de empezar

- Comprobó que un decomisionado del nodo de almacenamiento no está en curso o que ha pausado el procedimiento para decomisionar el nodo. (En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **misión**.)
- Ha comprobado que una expansión no está en curso. (En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **expansión**.)

Acerca de esta tarea

Los nodos de almacenamiento tienen una base de datos Cassandra que incluye metadatos de objetos. Si un nodo de almacenamiento no pudo comunicarse con otros nodos de almacenamiento durante más de 15 días, StorageGRID asume que la base de datos Cassandra del nodo está obsoleta. El nodo de almacenamiento no puede volver a unirse al grid hasta que Cassandra se haya recompilado con información de otros nodos de almacenamiento.

Use este procedimiento para reconstruir Cassandra solo si un solo nodo de almacenamiento está inactivo. Póngase en contacto con el soporte técnico si hay más nodos de almacenamiento sin conexión o si Cassandra se ha reconstruido en otro nodo de almacenamiento en los últimos 15 días; por ejemplo, Cassandra se puede haber reconstruido como parte de los procedimientos para recuperar volúmenes de almacenamiento con fallos o para recuperar un nodo de almacenamiento con errores.

Si más de un nodo de almacenamiento presenta errores (o está sin conexión), póngase en contacto con el soporte técnico. No realice el siguiente procedimiento de recuperación. Podrían perderse datos.

Si este es el segundo fallo del nodo de almacenamiento en menos de 15 días después de un fallo o una recuperación en el nodo de almacenamiento, póngase en contacto con el soporte técnico. No realice el siguiente procedimiento de recuperación. Podrían perderse datos.

Si se produce un error en más de un nodo de almacenamiento de un sitio, es posible que se requiera un procedimiento de recuperación del sitio. Consulte "Cómo el soporte técnico recupera un sitio".

Pasos

1. Si es necesario, encienda el nodo de almacenamiento que se debe recuperar.
2. Inicie sesión en el nodo de grid:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

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

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

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

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

> Si no puede iniciar sesión en el nodo de grid, es posible que el disco del sistema no esté intacto. Vaya al procedimiento para "recuperación del fallo de la unidad del sistema".

3. Realice las siguientes comprobaciones en el nodo de almacenamiento:

a. Emita este comando: `nodetool status`

La salida debería ser `Connection refused`

b. En Grid Manager, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.

c. Seleccione ***Site*** > **Storage Node** > **SSM** > **Services**. Compruebe que aparece el servicio Cassandra `Not Running`.

d. Selecciona **Nodo de almacenamiento** > **SSM** > **Recursos**. Compruebe que no haya estado de error en la sección Volumes.

e. Emita este comando: `grep -i Cassandra /var/local/log/servermanager.log`

Debería ver el siguiente mensaje en el resultado:

```
Cassandra not started because it has been offline for more than 15 day
grace period - rebuild Cassandra
```

4. Emita este comando y supervise el resultado del script: `check-cassandra-rebuild`

- Si se está ejecutando el servicio Cassandra según el volumen 0, se le pedirá que lo detenga. Introduzca: **Y**

> Si el servicio Cassandra ya está detenido, no se le preguntará. El servicio Cassandra se ha detenido solo para el volumen 0.

- Revise las advertencias del script. Si no se aplica ninguno de ellos, confirme que desea reconstruir Cassandra. Introduzca: **Y**

> Algunos procedimientos de recuperación de StorageGRID usan Reaper para gestionar las reparaciones de Cassandra. Las reparaciones se realizan automáticamente tan pronto como se hayan iniciado los servicios relacionados o necesarios. Es posible que note la salida de un script que menciona “reaper” o “Cassandra repair”. Si ve un mensaje de error que indica que la reparación ha fallado, ejecute el comando indicado en el mensaje de error.

5. Una vez finalizada la reconstrucción, realice las siguientes comprobaciones:

a. En Grid Manager, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.

b. Seleccione ***Site*** > **Recuerdo de almacenamiento** > **SSM** > **Servicios**.

c. Confirme que todos los servicios están en ejecución.

d. Selecciona **DDS** > **Almacén de datos**.

e. Confirme que el **Estado del almacén de datos** es “Activo” y que el **Estado del almacén de datos** es “Normal”.

Recupere el nodo de almacenamiento del dispositivo

Advertencias para recuperar nodos de almacenamiento del dispositivo

El procedimiento para recuperar un nodo de almacenamiento en dispositivos StorageGRID con fallos es el mismo tanto si se está recuperando de la pérdida de la unidad del sistema como de la pérdida de volúmenes de almacenamiento únicamente.

Si más de un nodo de almacenamiento presenta errores (o está sin conexión), póngase en contacto con el soporte técnico. No realice el siguiente procedimiento de recuperación. Podrían perderse datos.

Si este es el segundo fallo del nodo de almacenamiento en menos de 15 días después de un fallo o una recuperación en el nodo de almacenamiento, póngase en contacto con el soporte técnico. La reconstrucción de Cassandra en dos o más nodos de almacenamiento en 15 días puede provocar la pérdida de datos.

Si se produce un error en más de un nodo de almacenamiento de un sitio, es posible que se requiera un procedimiento de recuperación del sitio. Consulte "Cómo el soporte técnico recupera un sitio".

Si las reglas de ILM se configuran para almacenar una sola copia replicada y existe una en un volumen de almacenamiento donde se produjo un error, no podrá recuperar el objeto.

Si encuentra una alarma Services: Status - Cassandra (SVST) durante la recuperación, consulte "Recuperar volúmenes de almacenamiento con fallos y reconstruir la base de datos de Cassandra". Una vez reconstruida Cassandra, las alarmas se deberían borrar. Si las alarmas no se borran, póngase en contacto con el soporte técnico.

Para conocer procedimientos de mantenimiento del hardware, como instrucciones para reemplazar una controladora o reinstalar SANtricity OS, consulte la "instrucciones de mantenimiento para su dispositivo de almacenamiento".

Prepare el nodo de almacenamiento del dispositivo para su reinstalación

Al recuperar un nodo de almacenamiento del dispositivo, primero debe preparar el dispositivo para la reinstalación del software StorageGRID.

Pasos

1. Inicie sesión en el nodo de almacenamiento con errores:

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

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

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

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

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

2. Prepare el nodo de almacenamiento del dispositivo para la instalación del software StorageGRID. `sgareinstall`
3. Cuando se le solicite continuar, introduzca: `y`

   El dispositivo se reinicia y la sesión SSH finaliza. Normalmente tarda unos 5 minutos en estar disponible el instalador de dispositivos de StorageGRID; aunque en algunos casos es posible que deba esperar hasta 30 minutos.

   > No intente acelerar el reinicio apagando o reiniciando el aparato. Puede interrumpir las actualizaciones automáticas de BIOS, BMC u otras actualizaciones de firmware.

   El nodo de almacenamiento del dispositivo StorageGRID se restablece y ya no se puede acceder a los datos en el nodo de almacenamiento. Las direcciones IP configuradas durante el proceso de instalación original deben permanecer intactas; sin embargo, se recomienda confirmarlo cuando finalice el procedimiento.

   Después de ejecutar el `sgareinstall` Comando, se eliminan todas las cuentas, contraseñas y claves SSH aprovisionados de StorageGRID, y se generan nuevas claves del host.

Inicie la instalación del dispositivo StorageGRID

Para instalar StorageGRID en un nodo de almacenamiento del dispositivo, utilice el instalador de dispositivos StorageGRID, que se incluye en el dispositivo.

Antes de empezar

- El dispositivo se ha instalado en un bastidor, conectado a las redes y encendido.
- Se han configurado los enlaces de red y las direcciones IP para el dispositivo mediante el instalador de dispositivos de StorageGRID.
- Conoce la dirección IP del nodo de administrador principal para la cuadrícula StorageGRID.
- Todas las subredes de red de cuadrícula que aparecen en la página Configuración de IP del instalador de dispositivos StorageGRID se definieron en la lista de subredes de redes de cuadrícula del nodo de administración principal.
- Ha completado estas tareas de requisitos previos siguiendo las instrucciones de instalación para el dispositivo de almacenamiento. Consulte "Inicio rápido para la instalación de hardware".
- Está utilizando un "navegador web compatible".
- Conoce una de las direcciones IP asignadas a la controladora de computación en el dispositivo. Es posible usar la dirección IP para la red de administración (puerto de gestión 1 en la controladora), la red de grid o la red de cliente.

Acerca de esta tarea

Para instalar StorageGRID en un nodo de almacenamiento de dispositivos:

- Especifique o confirme la dirección IP del nodo de administración principal y el nombre de host (nombre del sistema) del nodo.
- Inicia la instalación y espera a que los volúmenes estén configurados y el software esté instalado.
- Paso a través del proceso, la instalación se detiene. Para reanudar la instalación, debe iniciar sesión en Grid Manager y configurar el nodo de almacenamiento pendiente como reemplazo del nodo con errores.
- Una vez que haya configurado el nodo, se completa el proceso de instalación del dispositivo y el dispositivo se reinicia.

Pasos

1. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación en el dispositivo.

   `https://Controller_IP:8443`

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. En la sección Conexión del nodo de administración principal, determine si necesita especificar la dirección IP para el nodo de administración principal.

   El instalador de dispositivos de StorageGRID puede detectar esta dirección IP automáticamente, suponiendo que el nodo de administración principal o, al menos, otro nodo de grid con ADMIN_IP configurado, esté presente en la misma subred.

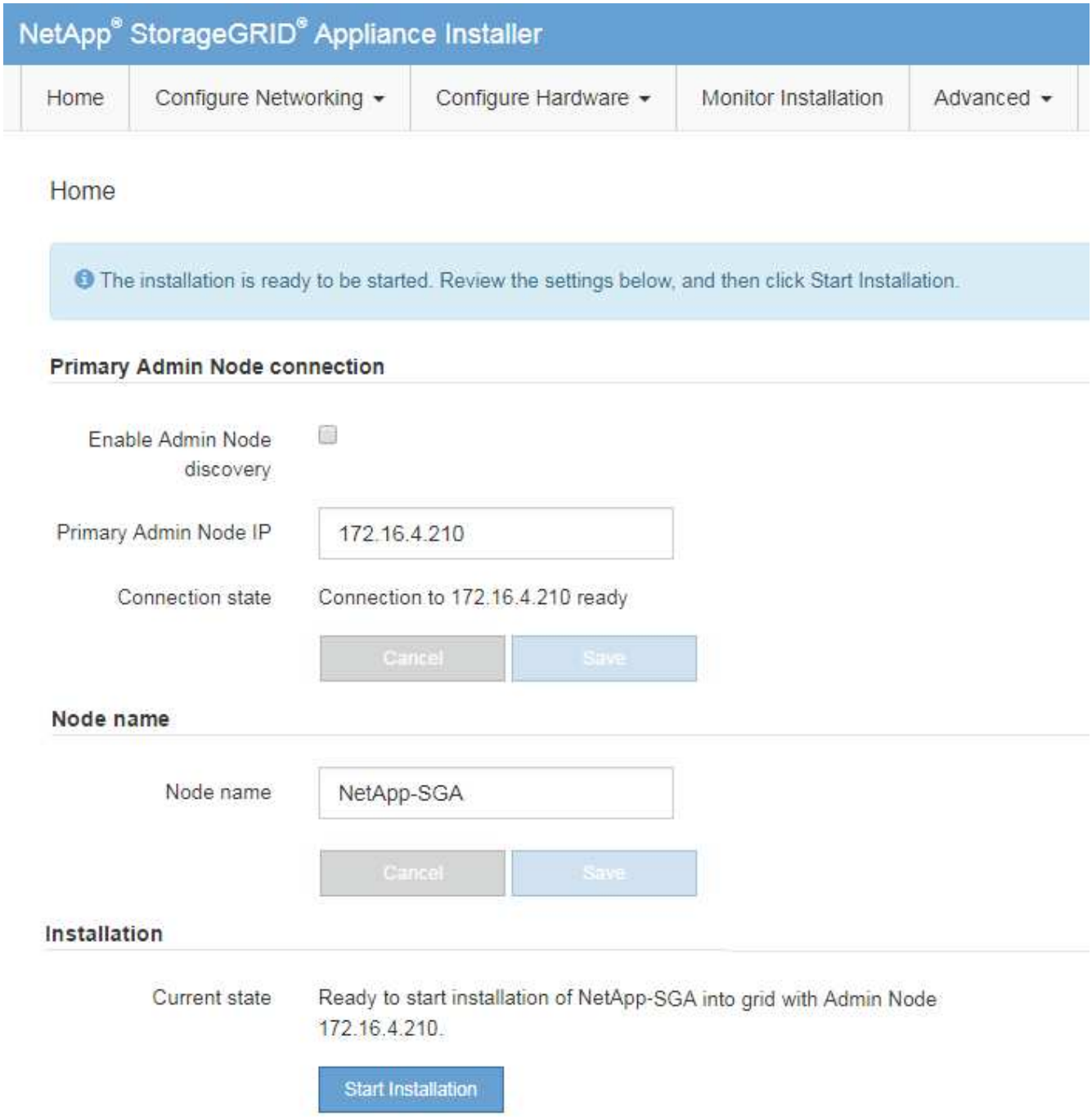
3. Si no se muestra esta dirección IP o es necesario modificarla, especifique la dirección:

Opción	Pasos
Entrada IP manual	a. Desactive la casilla de verificación **Enable Admin Node discovery**. b. Introduzca la dirección IP de forma manual. c. Haga clic en **Guardar**. d. Espere hasta que el estado de conexión de la nueva dirección IP esté listo.
Detección automática de todos los nodos principales de administración conectados	a. Seleccione la casilla de verificación **Enable Admin Node discovery**. b. En la lista de direcciones IP detectadas, seleccione el nodo de administrador principal para la cuadrícula en la que se pondrá en marcha este nodo de almacenamiento del dispositivo. c. Haga clic en **Guardar**. d. Espere hasta que el estado de conexión de la nueva dirección IP esté listo.

4. En el campo **Nombre del nodo**, introduzca el mismo nombre de host (nombre del sistema) que se utilizó para el nodo que está recuperando y haga clic en **Guardar**.
5. En la sección instalación, confirme que el estado actual es "Listo para iniciar la instalación de `node name` En la cuadrícula con el nodo de administración principal `*admin_ip*' y que el botón **Iniciar instalación** está habilitado.

Si el botón **Iniciar instalación** no está activado, es posible que deba cambiar la configuración de red o la configuración del puerto. Para obtener instrucciones, consulte las instrucciones de mantenimiento de su aparato.

6. En la página de inicio del instalador de dispositivos StorageGRID, haga clic en **Iniciar instalación**.



El estado actual cambia a «Instalación en curso» y se muestra la página de instalación del monitor.

> Si necesita acceder a la página de instalación del monitor manualmente, haga clic en **instalación del monitor** en la barra de menús. Consulte "Supervise la instalación del dispositivo".

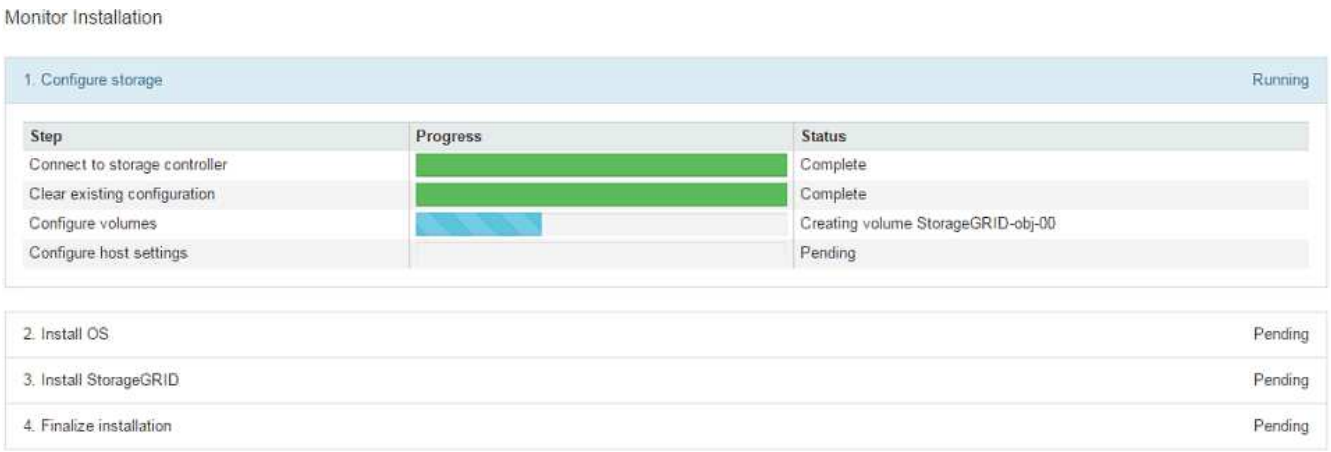
Supervise la instalación del dispositivo StorageGRID

El instalador del dispositivo StorageGRID proporciona el estado hasta que se completa la instalación. Una vez finalizada la instalación del software, el dispositivo se reinicia.

Pasos

1. Para supervisar el progreso de la instalación, haga clic en **instalación del monitor** en la barra de menús.

   La página Monitor Installation (instalación del monitor) muestra el progreso de la instalación.



   La barra de estado azul indica qué tarea está en curso actualmente. Las barras de estado verdes indican tareas que se han completado correctamente.

   > Installer garantiza que las tareas completadas en una instalación anterior no se vuelvan a ejecutar. Si vuelve a ejecutar una instalación, las tareas que no necesitan volver a ejecutarse se muestran con una barra de estado verde y el estado “Omitida”.

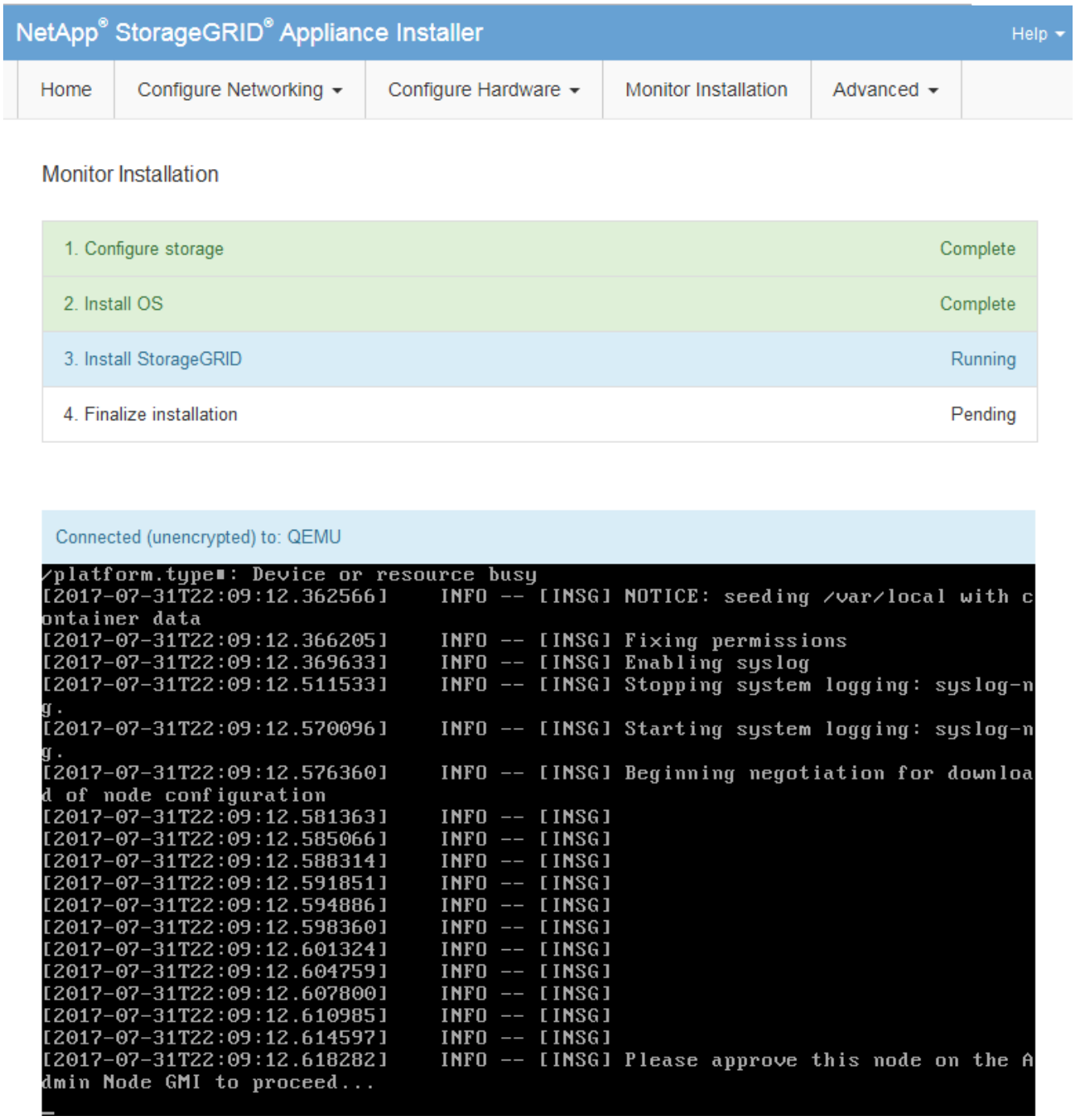
2. Revise el progreso de las dos primeras etapas de instalación.
   - **1. Configurar almacenamiento**

     En esta fase, el instalador se conecta a la controladora de almacenamiento, borra todas las configuraciones existentes, se comunica con el sistema operativo SANtricity para configurar los volúmenes y configura los ajustes del host.

   - **2. Instalar OS**

     Durante esta fase, el instalador copia la imagen del sistema operativo base para StorageGRID en el dispositivo.

3. Continúe supervisando el progreso de la instalación hasta que la etapa **instalar StorageGRID** se detenga y aparezca un mensaje en la consola integrada que le pedirá que apruebe este nodo en el nodo Admin mediante el Administrador de grid.



4. Vaya a. "Seleccione Start Recovery para configurar el nodo de almacenamiento del dispositivo".

Seleccione Start Recovery para configurar el nodo de almacenamiento del dispositivo

Debe seleccionar Start Recovery en el Grid Manager para configurar un Storage Node del dispositivo como reemplazo del nodo con errores.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento.

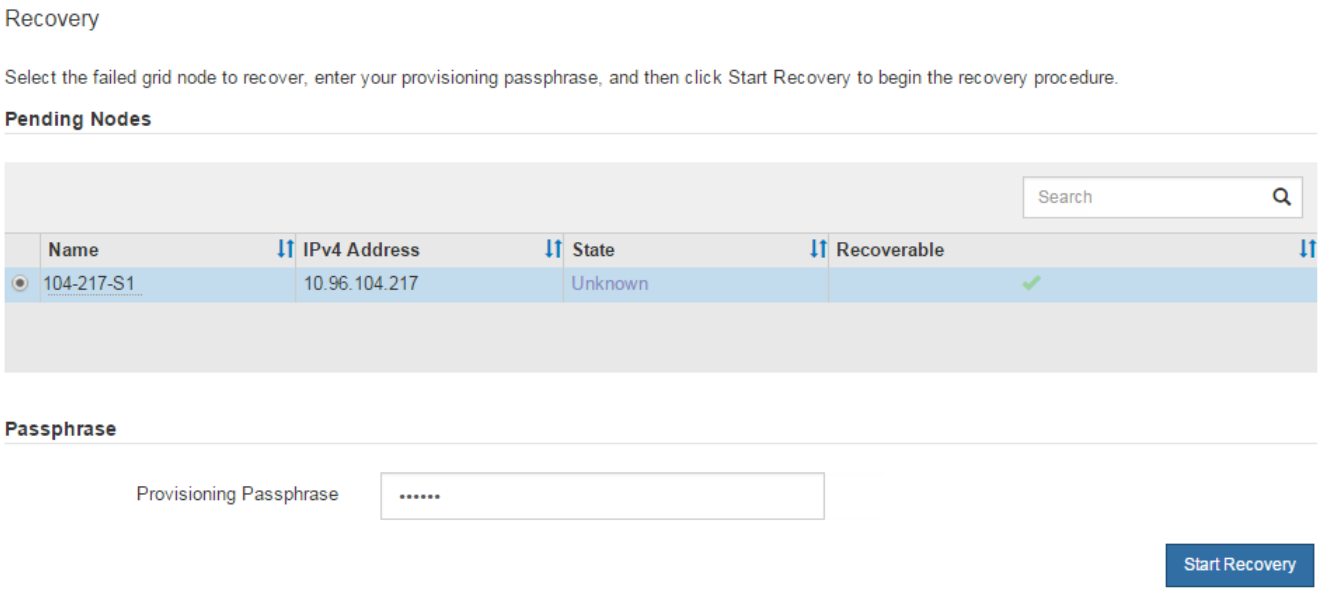
- Instaló un nodo de almacenamiento del dispositivo de recuperación.
- Tiene la fecha de inicio de cualquier trabajo de reparación para datos codificados de borrado.
- Ha verificado que el nodo de almacenamiento no se ha reconstruido en los últimos 15 días.

Pasos

1. En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **recuperación**.
2. Seleccione el nodo de cuadrícula que desea recuperar en la lista Pending Nodes.

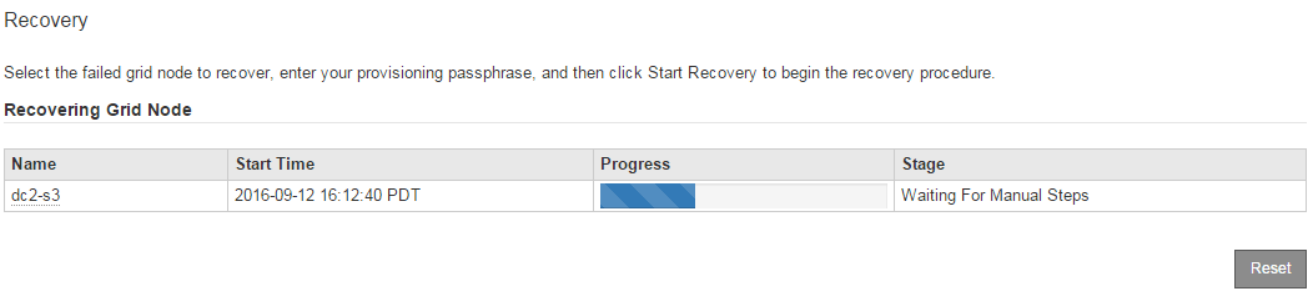
   Los nodos aparecen en la lista después de que fallan, pero no puede seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduzca la **frase de paso de aprovisionamiento**.
4. Haga clic en **Iniciar recuperación**.

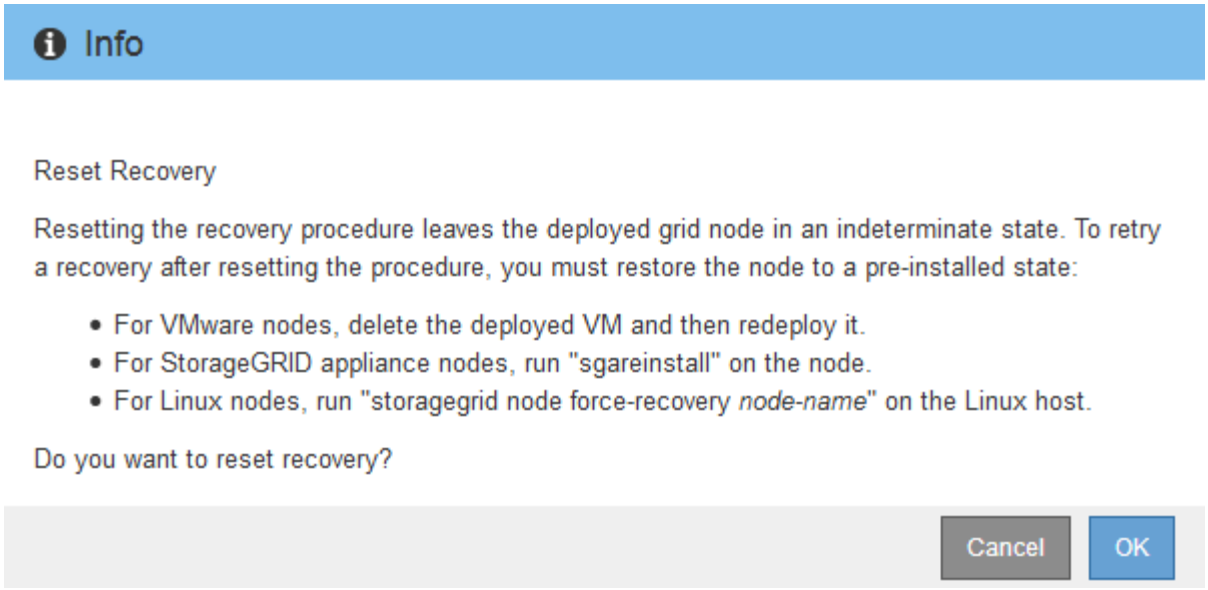


5. Supervise el progreso de la recuperación en la tabla recuperando Grid Node.

   Cuando el nodo de la cuadrícula alcance la etapa «Esperando pasos manuales», vaya al tema siguiente y siga los pasos manuales para volver a montar y formatear los volúmenes de almacenamiento del dispositivo.



> En cualquier momento durante la recuperación, puede hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparece un cuadro de diálogo que indica que el nodo quedará en un estado indeterminado si restablece el procedimiento.



Si desea volver a intentar la recuperación después de restablecer el procedimiento, debe restaurar el nodo del dispositivo a un estado preinstalado mediante la ejecución `sgareinstall` en el nodo.

Volver a montar y volver a formatear los volúmenes de almacenamiento de los dispositivos (pasos manuales)

Se deben ejecutar manualmente dos scripts para volver a montar los volúmenes de almacenamiento conservados y formatear los volúmenes de almacenamiento con errores. El primer script remonta volúmenes con un formato correcto como volúmenes de almacenamiento de StorageGRID. El segundo script reformatea todos los volúmenes desmontados, reconstruye la base de datos de Cassandra, si es necesario, e inicia los servicios.

Antes de empezar

- Ya ha sustituido el hardware de todos los volúmenes de almacenamiento con errores que necesite sustituir.

  Ejecutando el `sn-remount-volumes` el script puede ayudar a identificar volúmenes de almacenamiento adicionales donde se han producido fallos.

- Comprobó que un decomisionado del nodo de almacenamiento no está en curso o que ha pausado el procedimiento para decomisionar el nodo. (En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **misión**.)
- Ha comprobado que una expansión no está en curso. (En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **expansión**.)

> ! Póngase en contacto con el soporte técnico si hay más de un nodo de almacenamiento sin conexión o si se ha reconstruido un nodo de almacenamiento en este grid en los últimos 15 días. No ejecute el `sn-recovery-postinstall.sh` guión. Si se reconstruye Cassandra en dos o más nodos de almacenamiento en un plazo de 15 días entre sí, se puede producir una pérdida de datos.

Acerca de esta tarea

Para completar este procedimiento, realice estas tareas de alto nivel:

- Inicie sesión en el nodo de almacenamiento recuperado.
- Ejecute el `sn-remount-volumes` script para volver a montar volúmenes de almacenamiento con formato correcto. Cuando se ejecuta este script, realiza lo siguiente:
  - Monta y desmonta cada volumen de almacenamiento para reproducir el diario XFS.
  - Realiza una comprobación de consistencia de archivos XFS.
  - Si el sistema de archivos es coherente, determina si el volumen de almacenamiento es un volumen de almacenamiento de StorageGRID con el formato correcto.
  - Si el volumen de almacenamiento tiene el formato correcto, vuelve a montar el volumen de almacenamiento. Todos los datos existentes en el volumen permanecen intactos.
- Revise el resultado del script y resuelva cualquier problema.
- Ejecute el `sn-recovery-postinstall.sh` guión. Cuando se ejecuta este script, realiza lo siguiente.

> No reinicie un nodo de almacenamiento durante la recuperación antes de ejecutar `sn-recovery-postinstall.sh` (paso 4) para volver a formatear los volúmenes de almacenamiento que han fallado y restaurar los metadatos de objetos. Reinicie el nodo de almacenamiento antes `sn-recovery-postinstall.sh` Completa provoca errores en los servicios que se intentan iniciar y provoca que los nodos del dispositivo StorageGRID salgan del modo de mantenimiento.

  - Vuelva a formatear los volúmenes de almacenamiento que tenga `sn-remount-volumes` la secuencia de comandos no se pudo montar o se encontró que el formato era incorrecto.

> Si se vuelve a formatear un volumen de almacenamiento, se pierden todos los datos de ese volumen. Debe realizar un procedimiento adicional para restaurar datos de objetos desde otras ubicaciones de la cuadrícula, suponiendo que se hayan configurado las reglas de ILM para almacenar más de una copia de objetos.

  - Reconstruye la base de datos Cassandra en el nodo, si es necesario.
  - Inicia los servicios en el nodo de almacenamiento.

Pasos

1. Inicie sesión en el nodo de almacenamiento recuperado:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Ejecute el primer script para volver a montar todos los volúmenes de almacenamiento con un formato correcto.

Si todos los volúmenes de almacenamiento son nuevos y se deben formatear, o bien si se producen errores en todos los volúmenes de almacenamiento, es posible omitir este paso y ejecutar el segundo script para volver a formatear todos los volúmenes de almacenamiento desmontados.

a. Ejecute el script: `sn-remount-volumes`

   Este script puede tardar horas en ejecutarse en volúmenes de almacenamiento que contienen datos.

b. A medida que se ejecuta el script, revise la salida y responda a las peticiones.

   Según sea necesario, puede utilizar la `tail -f` comando para supervisar el contenido del archivo de registro del script (`/var/local/log/sn-remount-volumes.log`) . El archivo de registro contiene información más detallada que el resultado de la línea de comandos.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
```

```
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

En la salida de ejemplo, se remontó correctamente un volumen de almacenamiento y se produjeron errores en tres volúmenes de almacenamiento.

- `/dev/sdb` Superó la comprobación de consistencia del sistema de archivos XFS y tenía una estructura de volumen válida, por lo que se remontó correctamente. Se conservan los datos de los

dispositivos que se remontan mediante el script.

- `/dev/sdc` No se pudo realizar la comprobación de consistencia del sistema de archivos XFS porque el volumen de almacenamiento era nuevo o estaba dañado.
- `/dev/sdd` no se ha podido montar porque el disco no se ha inicializado o porque el superbloque del disco está dañado. Cuando el script no puede montar un volumen de almacenamiento, le pregunta si desea ejecutar la comprobación de consistencia del sistema de archivos.
  - Si el volumen de almacenamiento está conectado a un nuevo disco, responda **N** al indicador. No es necesario que compruebe el sistema de archivos en un disco nuevo.
  - Si el volumen de almacenamiento está conectado a un disco existente, responda **y** al indicador. Puede utilizar los resultados de la comprobación del sistema de archivos para determinar el origen de los daños. Los resultados se guardan en la `/var/local/log/sn-remount-volumes.log` archivo de registro.
- `/dev/sde` Pasó la comprobación de consistencia del sistema de archivos XFS y tenía una estructura de volumen válida; sin embargo, el ID de nodo LDR en `volID` El archivo no coincide con el ID de este nodo de almacenamiento (el `configured LDR noid` mostrado en la parte superior). Este mensaje indica que este volumen pertenece a otro nodo de almacenamiento.

3. Revise el resultado del script y resuelva cualquier problema.

> Si un volumen de almacenamiento no superó la comprobación de consistencia del sistema de archivos XFS o no pudo montarse, revise con cuidado los mensajes de error del resultado. Debe comprender las implicaciones de ejecutar el `sn-recovery-postinstall.sh` guión en estos volúmenes.

a. Compruebe que los resultados incluyan una entrada de todos los volúmenes esperados. Si hay algún volumen que no aparece en la lista, vuelva a ejecutar el script.

b. Revise los mensajes de todos los dispositivos montados. Asegúrese de que no haya errores que indiquen que un volumen de almacenamiento no pertenece a este nodo de almacenamiento.

   En el ejemplo, el resultado de /dev/sde incluye el siguiente mensaje de error:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> Si un volumen de almacenamiento se informa como que pertenece a otro nodo de almacenamiento, póngase en contacto con el soporte técnico. Si ejecuta el `sn-recovery-postinstall.sh` script, se reformateará el volumen de almacenamiento, lo que puede provocar la pérdida de datos.

c. Si no se pudo montar ningún dispositivo de almacenamiento, anote el nombre del dispositivo y repare o reemplace el dispositivo.

> Debe reparar o sustituir cualquier dispositivo de almacenamiento que no pueda montarse.

   Utilizará el nombre del dispositivo para buscar el ID de volumen, que es necesario introducir cuando ejecute el `repair-data` script para restaurar datos de objetos en el volumen (el siguiente procedimiento).

d. Después de reparar o sustituir todos los dispositivos que no se pueden montar, ejecute el `sn-remount-volumes` vuelva a script para confirmar que se han vuelto a montar todos los volúmenes de almacenamiento que pueden remontarse.

> Si un volumen de almacenamiento no se puede montar o se formatea de forma incorrecta y se continúa con el siguiente paso, se eliminarán el volumen y todos los datos del volumen. Si tenía dos copias de datos de objetos, sólo tendrá una copia única hasta que complete el siguiente procedimiento (restaurando datos de objetos).

> No ejecute el `sn-recovery-postinstall.sh` Script si cree que los datos que quedan en un volumen de almacenamiento con fallos no se pueden reconstruir desde otro lugar del grid (por ejemplo, si la política de ILM usa una regla que solo realice una copia o si los volúmenes han fallado en varios nodos). En su lugar, póngase en contacto con el soporte técnico para determinar cómo recuperar los datos.

4. Ejecute el `sn-recovery-postinstall.sh` guión: `sn-recovery-postinstall.sh`

   Este script reformatea todos los volúmenes de almacenamiento que no se pudieron montar o que se encontraron con un formato incorrecto; reconstruye la base de datos de Cassandra en el nodo, si es necesario; e inicia los servicios en el nodo de almacenamiento.

   Tenga en cuenta lo siguiente:

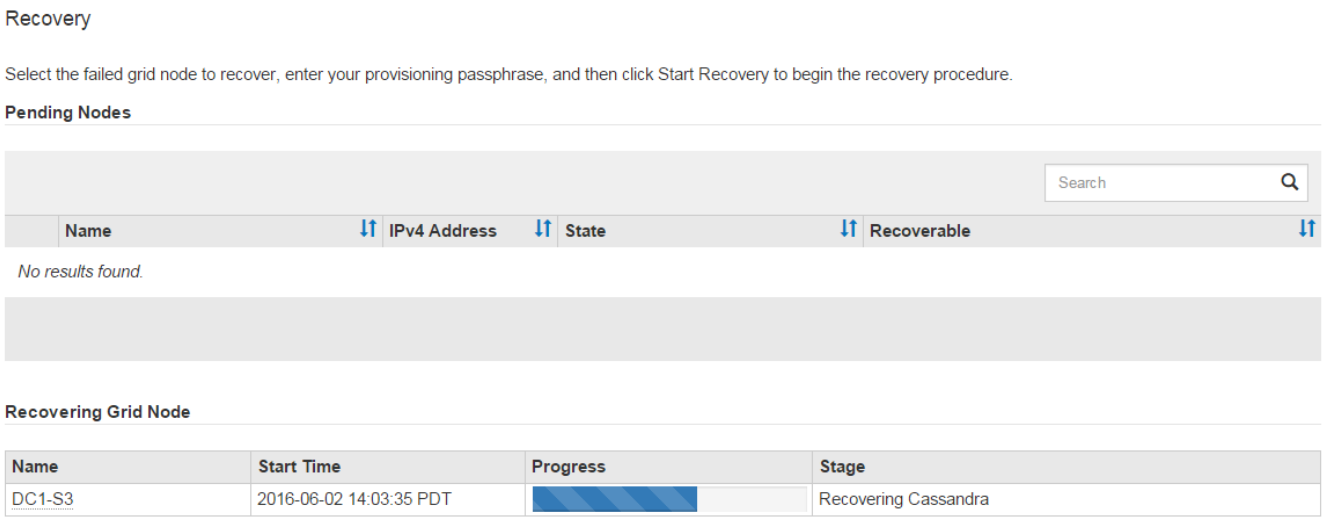
   - El script puede tardar horas en ejecutarse.
   - En general, debe dejar la sesión SSH sola mientras el script está en ejecución.
   - No pulse **Ctrl+C** mientras la sesión SSH esté activa.
   - El script se ejecutará en segundo plano si se produce una interrupción de red y finaliza la sesión SSH, pero puede ver el progreso desde la página Recovery.
   - Si Storage Node utiliza el servicio RSM, puede parecer que el script se atasca durante 5 minutos mientras se reinician los servicios de nodos. Este retraso de 5 minutos se espera siempre que el servicio RSM arranque por primera vez.

   > El servicio RSM está presente en los nodos de almacenamiento que incluyen el servicio ADC.

   > Algunos procedimientos de recuperación de StorageGRID usan Reaper para gestionar las reparaciones de Cassandra. Las reparaciones se realizan automáticamente tan pronto como se hayan iniciado los servicios relacionados o necesarios. Es posible que note la salida de un script que menciona “reaper” o “Cassandra repair”. Si ve un mensaje de error que indica que la reparación ha fallado, ejecute el comando indicado en el mensaje de error.

5. Como la `sn-recovery-postinstall.sh` Se ejecuta Script, supervise la página Recovery en Grid Manager.

   La barra de progreso y la columna Stage de la página Recovery proporcionan un estado de alto nivel de `sn-recovery-postinstall.sh` guión.



6. Después del `sn-recovery-postinstall.sh` script ha iniciado servicios en el nodo, puede restaurar datos de objetos en cualquier volumen de almacenamiento que haya formateado el script.

   El script le pregunta si desea utilizar el proceso de restauración del volumen de Grid Manager.

   - En la mayoría de los casos, usted debería "Restaurar datos de objetos con Grid Manager". Responda `y` Para utilizar Grid Manager.
   - En raras ocasiones, como cuando se lo indica el soporte técnico o cuando sabe que el nodo de reemplazo tiene menos volúmenes disponibles para el almacenamiento de objetos que el nodo original, debe "restaurar datos de objetos manualmente" con el `repair-data` guión. Si se aplica uno de estos casos, responda `n`.

   > Si responde `n` Para utilizar el proceso de restauración de volúmenes de Grid Manager (restaurar datos de objetos manualmente):
   >
   > - No puede restaurar datos de objetos con Grid Manager.
   > - Puede supervisar el progreso de los trabajos de restauración manual con Grid Manager.

   Después de realizar su selección, el script se completa y se muestran los siguientes pasos para recuperar los datos del objeto. Después de revisar estos pasos, pulse cualquier tecla para volver a la línea de comandos.

Restaure datos de objetos al volumen de almacenamiento de dispositivo

Después de recuperar los volúmenes de almacenamiento para el nodo de almacenamiento del dispositivo, se pueden restaurar los datos de objetos replicados o con código de borrado que se perdieron cuando falló el nodo de almacenamiento.

¿Qué procedimiento debo usar?

Siempre que sea posible, restaure los datos del objeto utilizando la página **Volume restoration** en Grid Manager.

- Si los volúmenes aparecen en **MANTENIMIENTO** > **Restauración de volumen** > **Nodos a restaurar**, restaure los datos del objeto con el "Página de restauración de volúmenes en Grid Manager".

- Si los volúmenes no aparecen en **MANTENIMIENTO** > **Restauración de volumen** > **Nodos a restaurar**, siga los pasos que se indican a continuación para usar el `repair-data` script para restaurar datos de objeto.

  Si el nodo de almacenamiento recuperado contiene menos volúmenes que el nodo en el que sustituye, debe utilizar el `repair-data` guión.

> El script repair-data está obsoleto y se eliminará en una versión futura. Cuando sea posible, utilice el "Procedimiento de restauración de volúmenes en Grid Manager".

Utilice la `repair-data` script para restaurar datos de objeto

Antes de empezar

- Ha confirmado que el nodo de almacenamiento recuperado tiene un estado de conexión de **Connected** En la ficha **NODES** > **Descripción general** de Grid Manager.

Acerca de esta tarea

Los datos de objetos se pueden restaurar desde otros nodos de almacenamiento, un nodo de archivado o un pool de almacenamiento en cloud si se configuran las reglas de gestión del ciclo de vida de la información del grid de modo que las copias de objetos estén disponibles.

Tenga en cuenta lo siguiente:

- Si se configuró una regla de ILM para almacenar una sola copia replicada y esa copia estaba en un volumen de almacenamiento que falló, no podrá recuperar el objeto.
- Si la única copia restante de un objeto se encuentra en un Cloud Storage Pool, StorageGRID debe emitir varias solicitudes al extremo Cloud Storage Pool para restaurar datos de objetos. Antes de realizar este procedimiento, póngase en contacto con el soporte técnico para obtener ayuda a la hora de calcular el plazo de recuperación y los costes asociados.
- Si la única copia restante de un objeto se encuentra en un nodo de archivado, los datos de objeto se recuperan del nodo de archivado. La restauración de datos de objetos en un nodo de almacenamiento desde un nodo de archivado tarda más que en restaurar copias de otros nodos de almacenamiento, debido a la latencia asociada a las recuperaciones desde sistemas de almacenamiento de archivado externos.

Acerca de la `repair-data` guión

Para restaurar datos de objeto, ejecute el `repair-data` guión. Este script inicia el proceso de restauración de datos de objetos y funciona con el análisis de ILM para garantizar que se cumplan las reglas de ILM.

Seleccione **datos replicados** o **datos codificados con borrado (EC)** a continuación para conocer las diferentes opciones para `repair-data` script, en función de si va a restaurar datos replicados o datos codificados de borrado. Si necesita restaurar ambos tipos de datos, debe ejecutar ambos conjuntos de comandos.

> Para obtener más información acerca de `repair-data` guión, introduzca `repair-data --help` Desde la línea de comandos del nodo de administrador principal.

> El script repair-data está obsoleto y se eliminará en una versión futura. Cuando sea posible, utilice el "Procedimiento de restauración de volúmenes en Grid Manager".

Datos replicados

Hay dos comandos disponibles para restaurar los datos replicados, según si necesita reparar el nodo completo o solo ciertos volúmenes del nodo:

```
repair-data start-replicated-node-repair

repair-data start-replicated-volume-repair
```

Puede realizar un seguimiento de las reparaciones de los datos replicados con este comando:

```
repair-data show-replicated-repair-status
```

Datos con código de borrado (EC)

Hay dos comandos disponibles para restaurar datos codificados de borrado a partir de si necesita reparar el nodo completo o solo ciertos volúmenes en el nodo:

```
repair-data start-ec-node-repair

repair-data start-ec-volume-repair
```

Puede realizar un seguimiento de las reparaciones de datos codificados de borrado con este comando:

```
repair-data show-ec-repair-status
```

> Las reparaciones de datos codificados para borrado pueden comenzar con algunos nodos de almacenamiento sin conexión. Sin embargo, si no se pueden tener en cuenta todos los datos con código de borrado, no se podrá completar la reparación. La reparación se completará después de que todos los nodos estén disponibles.

> El trabajo de reparación de la CE reserva temporalmente una gran cantidad de almacenamiento. Es posible que se activen las alertas de almacenamiento, pero se resolverán cuando se complete la reparación. Si no hay suficiente almacenamiento para la reserva, el trabajo de reparación de la CE fallará. Las reservas de almacenamiento se liberan cuando se completa el trabajo de reparación de EC, tanto si el trabajo ha fallado como si ha sido correcto.

Busque el nombre de host del nodo de almacenamiento

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Utilice la `/etc/hosts` File para encontrar el nombre de host del nodo de almacenamiento para los volúmenes de almacenamiento restaurados. Para ver una lista de todos los nodos de la cuadrícula,

introduzca lo siguiente: `cat /etc/hosts`.

Repare los datos si todos los volúmenes presentan errores

Si todos los volúmenes de almacenamiento presentan errores, repare todo el nodo. Siga las instrucciones para **datos replicados**, **datos codificados con borrado (EC)**, o ambos, en función de si utiliza datos replicados, datos codificados con borrado (EC), o ambos.

Si solo se produjo un error en algunos volúmenes, vaya a. Repare los datos si solo algunos volúmenes han fallado.

> No puedes correr `repair-data` operaciones para más de un nodo a la vez. Para recuperar varios nodos, póngase en contacto con el soporte técnico.

Datos replicados

Si la cuadrícula incluye datos replicados, utilice `repair-data start-replicated-node-repair` con el `--nodes` opción, donde `--nodes` Es el nombre de host (nombre del sistema), para reparar todo el nodo de almacenamiento.

Este comando repara los datos replicados en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> A medida que se restauran los datos del objeto, la alerta de **Objetos perdidos** se activa si el sistema StorageGRID no puede localizar los datos de objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Debe determinar la causa de la pérdida y si es posible la recuperación. Consulte "Investigar los objetos perdidos".

Datos con código de borrado (EC)

Si el grid contiene datos con código de borrado, utilice `repair-data start-ec-node-repair` con el `--nodes` opción, donde `--nodes` Es el nombre de host (nombre del sistema), para reparar todo el nodo de almacenamiento.

Este comando repara los datos codificados con borrado en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

La operación devuelve un valor exclusivo `repair ID` eso lo identifica `repair_data` funcionamiento. Utilice esto `repair ID` para realizar un seguimiento del progreso y el resultado de la `repair_data` funcionamiento. No se devuelve ningún otro comentario cuando finaliza el proceso de recuperación.

> Las reparaciones de datos codificados para borrado pueden comenzar con algunos nodos de almacenamiento sin conexión. La reparación se completará después de que todos los nodos estén disponibles.

Repare los datos si solo algunos volúmenes han fallado

Si solo se produjo un error en algunos de los volúmenes, repare los volúmenes afectados. Siga las

instrucciones para **datos replicados**, **datos codificados con borrado (EC)**, o ambos, en función de si utiliza datos replicados, datos codificados con borrado (EC), o ambos.

Si todos los volúmenes presentan errores, vaya a. Repare los datos si todos los volúmenes presentan errores.

Introduzca los ID de volumen en hexadecimal. Por ejemplo: `0000` es el primer volumen y. `000F` es el volumen decimosexto. Puede especificar un volumen, un rango de volúmenes o varios volúmenes que no estén en una secuencia.

Todos los volúmenes deben estar en el mismo nodo de almacenamiento. Si necesita restaurar volúmenes para más de un nodo de almacenamiento, póngase en contacto con el soporte técnico.

Datos replicados

Si la cuadrícula contiene datos replicados, utilice `start-replicated-volume-repair` con el `--nodes` opción para identificar el nodo (dónde `--nodes` es el nombre de host del nodo). A continuación, agregue el `--volumes` o. `--volume-range` como se muestra en los siguientes ejemplos.

Single volume: Este comando restaura los datos replicados al volumen `0002` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Intervalo de volúmenes: Este comando restaura los datos replicados a todos los volúmenes del intervalo `0003` para `0009` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Varios volúmenes que no están en una secuencia: Este comando restaura los datos replicados a los volúmenes `0001`, `0005`, y. `0008` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> ⓘ A medida que se restauran los datos del objeto, la alerta de **Objetos perdidos** se activa si el sistema StorageGRID no puede localizar los datos de objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Tenga en cuenta la descripción de la alerta y las acciones recomendadas para determinar la causa de la pérdida y si la recuperación es posible.

Datos con código de borrado (EC)

Si el grid contiene datos con código de borrado, utilice `start-ec-volume-repair` con el `--nodes` opción para identificar el nodo (dónde `--nodes` es el nombre de host del nodo). A continuación, agregue el `--volumes` o. `--volume-range` como se muestra en los siguientes ejemplos.

Volumen único: Este comando restaura los datos codificados por borrado al volumen `0007` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Intervalo de volúmenes: Este comando restaura los datos codificados por borrado a todos los volúmenes del intervalo `0004` para `0006` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Múltiples volúmenes no en una secuencia: Este comando restaura datos codificados por borrado a volúmenes `000A`, `000C`, y. `000E` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

La `repair-data` la operación devuelve un valor exclusivo `repair ID` eso lo identifica `repair_data` funcionamiento. Utilice esto `repair ID` para realizar un seguimiento del progreso y el resultado de la `repair_data` funcionamiento. No se devuelve ningún otro comentario cuando finaliza el proceso de

recuperación.

> Las reparaciones de datos codificados para borrado pueden comenzar con algunos nodos de almacenamiento sin conexión. La reparación se completará después de que todos los nodos estén disponibles.

Reparaciones del monitor

Supervise el estado de los trabajos de reparación, en función de si utiliza **datos replicados**, **datos codificados por borrado (EC)** o ambos.

También es posible supervisar el estado de los trabajos de restauración de volúmenes en curso y ver un historial de los trabajos de restauración completados en "Administrador de grid".

Datos replicados

- Para obtener un porcentaje de finalización estimado para la reparación replicada, agregue el `show-replicated-repair-status` opción del comando repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Para determinar si las reparaciones están completas:
  a. Seleccione **NODES** > ***Storage Node que se está reparando*** > **ILM**.
  b. Revise los atributos en la sección Evaluación. Una vez completadas las reparaciones, el atributo **esperando - todo** indica 0 objetos.
- Para supervisar la reparación con más detalle:
  a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
  b. Seleccione ***grid*** > ***nodo de almacenamiento que se está reparando*** > **LDR** > **almacén de datos**.
  c. Utilice una combinación de los siguientes atributos para determinar, como sea posible, si las reparaciones replicadas se han completado.

  > Puede haber incoherencias en Cassandra y no se realiza un seguimiento de las reparaciones fallidas.

  - **Reparaciones intentadas (XRPA)**: Utilice este atributo para realizar un seguimiento del progreso de las reparaciones replicadas. Este atributo aumenta cada vez que un nodo de almacenamiento intenta reparar un objeto de alto riesgo. Cuando este atributo no aumenta durante un período más largo que el período de exploración actual (proporcionado por el atributo **período de exploración — estimado**), significa que el análisis de ILM no encontró objetos de alto riesgo que necesitan ser reparados en ningún nodo.

    > Los objetos de alto riesgo son objetos que corren el riesgo de perderse por completo. Esto no incluye objetos que no cumplen con la configuración de ILM.

  - **Período de exploración — estimado (XSCM)**: Utilice este atributo para estimar cuándo se aplicará un cambio de directiva a objetos ingeridos previamente. Si el atributo **reparos intentados** no aumenta durante un período más largo que el período de adquisición actual, es probable que se realicen reparaciones replicadas. Tenga en cuenta que el período de adquisición puede cambiar. El atributo **período de exploración — estimado (XSCM)** se aplica a toda la cuadrícula y es el máximo de todos los periodos de exploración de nodos. Puede consultar el historial de atributos **período de exploración — Estimated** de la cuadrícula para determinar un intervalo de tiempo adecuado.

Datos con código de borrado (EC)

Para supervisar la reparación de datos codificados mediante borrado y vuelva a intentar cualquier solicitud que pudiera haber fallado:

1. Determine el estado de las reparaciones de datos codificadas por borrado:
   - Seleccione **SUPPORT** > **Tools** > **Metrics** para ver el tiempo estimado hasta la finalización y el porcentaje de finalización del trabajo actual. A continuación, seleccione **EC Overview** en la sección Grafana. Consulte los paneles **tiempo estimado de trabajo de Grid EC hasta finalización** y **Porcentaje de trabajo de Grid EC completado**.

- Utilice este comando para ver el estado de un elemento específico `repair-data` operación:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilice este comando para enumerar todas las reparaciones:

  ```
  repair-data show-ec-repair-status
  ```

El resultado muestra información, como `repair ID`, para todas las reparaciones que se estén ejecutando anteriormente y actualmente.

2. Si el resultado muestra que la operación de reparación ha dado error, utilice el `--repair-id` opción de volver a intentar la reparación.

   Este comando vuelve a intentar una reparación de nodo con fallos mediante el ID de reparación 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Este comando reintenta realizar una reparación de volumen con fallos mediante el ID de reparación 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Compruebe el estado de almacenamiento después de recuperar el nodo de almacenamiento del dispositivo

Después de recuperar un nodo de almacenamiento de dispositivo, debe comprobar que el estado deseado del nodo de almacenamiento del dispositivo está establecido en online y que el estado estará en línea de forma predeterminada cada vez que se reinicie el servidor del nodo de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- El nodo de almacenamiento se ha recuperado y se completó la recuperación de datos.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Compruebe los valores de **Nodo de almacenamiento recuperado** > **LDR** > **Almacenamiento** > **Estado de almacenamiento — deseado** y **Estado de almacenamiento — actual**.

   El valor de ambos atributos debe ser en línea.

3. Si el estado de almacenamiento — deseado está establecido en sólo lectura, realice los siguientes pasos:
   a. Haga clic en la ficha **Configuración**.
   b. En la lista desplegable **Estado de almacenamiento — deseado**, seleccione **Online**.
   c. Haga clic en **aplicar cambios**.
   d. Haga clic en la ficha **Descripción general** y confirme que los valores de **Estado de almacenamiento — deseado** y **Estado de almacenamiento — actual** se actualizan a Online.

Recupérese de un fallo en el volumen de almacenamiento, donde la unidad del sistema está intacta

Recupérese de un fallo del volumen de almacenamiento donde la unidad del sistema está intacta: Descripción general

Debe completar una serie de tareas para recuperar un nodo de almacenamiento basado en software en el que uno o varios volúmenes de almacenamiento del nodo de almacenamiento han fallado, pero la unidad del sistema está intacta. Si solo los volúmenes de almacenamiento fallan, el nodo de almacenamiento sigue disponible para el sistema StorageGRID.

> Este procedimiento de recuperación se aplica únicamente a los nodos de almacenamiento basados en software. Si los volúmenes de almacenamiento tienen errores en un nodo de almacenamiento del dispositivo, use el procedimiento del dispositivo: "Recupere el nodo de almacenamiento del dispositivo".

Este procedimiento de recuperación incluye las siguientes tareas:

- "Revise las advertencias para la recuperación del volumen de almacenamiento"
- "Identifique y desmonte los volúmenes de almacenamiento que han fallado"
- "Recupere los volúmenes y reconstruya la base de datos Cassandra"
- "Restaurar datos de objeto"
- "Compruebe el estado del almacenamiento"

Advertencias para la recuperación del volumen de almacenamiento

Antes de recuperar volúmenes de almacenamiento con errores para un nodo de almacenamiento, revise las siguientes advertencias.

Los volúmenes de almacenamiento (o mapedbs) de un nodo de almacenamiento se identifican con un número hexadecimal, que se conoce como el ID del volumen. Por ejemplo, 0000 es el primer volumen y 000F es el decimosexto volumen. El primer almacén de objetos (volumen 0) en cada nodo de almacenamiento usa hasta 4 TB de espacio para los metadatos de objetos y las operaciones de la base de datos de Cassandra; todo el espacio restante en ese volumen se usa para los datos de objetos. El resto de volúmenes de almacenamiento se utilizan exclusivamente para datos de objetos.

Si se produce un error en el volumen 0 y se debe recuperar, la base de datos de Cassandra puede reconstruirse como parte del procedimiento de recuperación de volumen. Cassandra también se puede reconstruir en las siguientes circunstancias:

- Un nodo de almacenamiento se vuelve a conectar después de haber estado desconectado más de 15 días.
- La unidad del sistema y uno o más volúmenes de almacenamiento fallan y se recuperan.

Cuando se reconstruye Cassandra, el sistema utiliza información de otros nodos de almacenamiento. Si hay demasiados nodos de almacenamiento sin conexión, es posible que algunos datos de Cassandra no estén disponibles. Si Cassandra se ha reconstruido recientemente, es posible que los datos de Cassandra aún no sean coherentes en toda la cuadrícula. Se pueden perder datos si Cassandra se vuelve a generar cuando hay demasiados nodos de almacenamiento sin conexión o si se reconstruyen dos o más nodos de

almacenamiento en un plazo de 15 días entre sí.

Si más de un nodo de almacenamiento presenta errores (o está sin conexión), póngase en contacto con el soporte técnico. No realice el siguiente procedimiento de recuperación. Podrían perderse datos.

Si este es el segundo fallo del nodo de almacenamiento en menos de 15 días después de un fallo o una recuperación en el nodo de almacenamiento, póngase en contacto con el soporte técnico. La reconstrucción de Cassandra en dos o más nodos de almacenamiento en 15 días puede provocar la pérdida de datos.

Si se produce un error en más de un nodo de almacenamiento de un sitio, es posible que se requiera un procedimiento de recuperación del sitio. Consulte "Cómo el soporte técnico recupera un sitio".

Si las reglas de ILM se configuran para almacenar una sola copia replicada y existe una en un volumen de almacenamiento donde se produjo un error, no podrá recuperar el objeto.

Si encuentra una alarma Services: Status - Cassandra (SVST) durante la recuperación, consulte "Recuperar volúmenes de almacenamiento con fallos y reconstruir la base de datos de Cassandra". Una vez reconstruida Cassandra, las alarmas se deberían borrar. Si las alarmas no se borran, póngase en contacto con el soporte técnico.

Información relacionada

"Advertencias y consideraciones sobre los procesos de recuperación de nodos de grid"

Identifique y desmonte los volúmenes de almacenamiento que han fallado

Al recuperar un nodo de almacenamiento con volúmenes de almacenamiento con fallos, se deben identificar y desmontar los volúmenes con errores. Debe verificar que solo los volúmenes de almacenamiento con errores se hayan reformateado como parte del procedimiento de recuperación.

Antes de empezar

Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".

Acerca de esta tarea

Debe recuperar Lo antes posible. de volúmenes de almacenamiento con errores.

El primer paso del proceso de recuperación es detectar volúmenes que se han desvinculado, se deben desmontar o se producen errores de I/O. Si los volúmenes con fallos siguen conectados pero tienen un sistema de archivos dañado de forma aleatoria, es posible que el sistema no detecte ningún daño en partes del disco que no estén en uso o no estén asignados.

Debe finalizar este procedimiento antes de realizar los pasos manuales para recuperar los volúmenes, como añadir o volver a conectar los discos, detener el nodo, iniciar el nodo o reiniciar. De lo contrario, cuando ejecute el `reformat_storage_block_devices.rb` script, puede encontrar un error del sistema de archivos que provoca el bloqueo o el error del script.

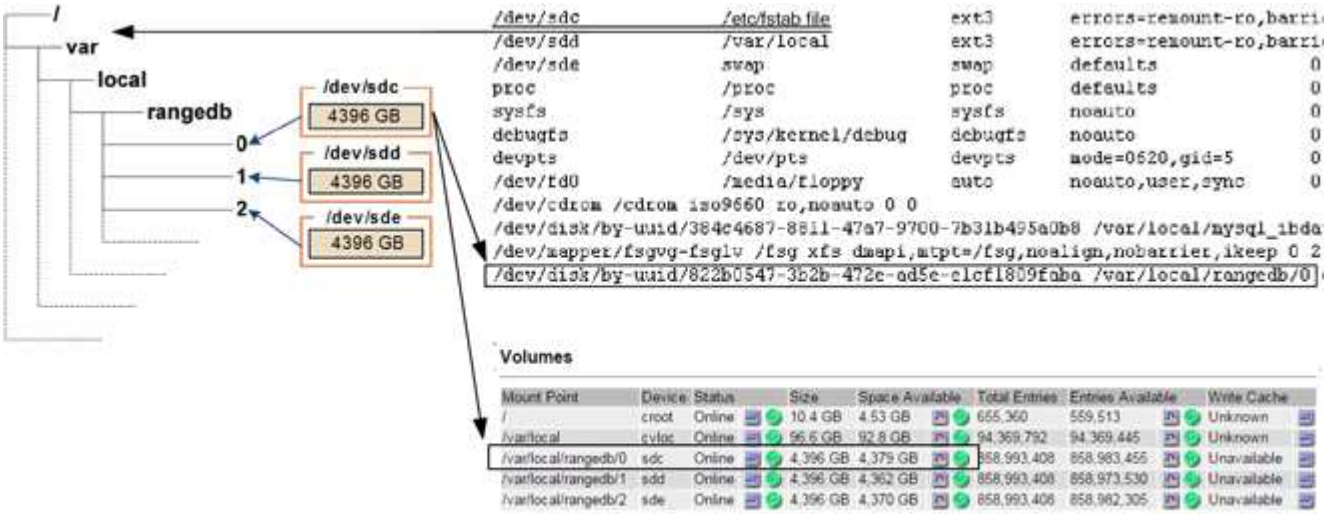
Repare el hardware y conecte correctamente los discos antes de ejecutar el `reboot` comando.

Identifique cuidadosamente los volúmenes de almacenamiento fallidos. Utilizará esta información para verificar qué volúmenes se deben reformatear. Una vez reformateado un volumen, no se pueden recuperar los datos del volumen.

Para recuperar correctamente los volúmenes de almacenamiento con fallos, es necesario conocer los nombres de los dispositivos de los volúmenes de almacenamiento con errores y sus ID de volumen.

En la instalación, a cada dispositivo de almacenamiento se le asigna un identificador único universal (UUID) del sistema de archivos y se monta en un directorio de configuración en el nodo de almacenamiento utilizando ese UUID del sistema de archivos asignado. El UUID del sistema de archivos y el directorio rangedb se muestran en la `/etc/fstab` archivo. El nombre del dispositivo, el directorio rangedb y el tamaño del volumen montado se muestran en el Administrador de grid.

En el siguiente ejemplo, dispositivo `/dev/sdc` Tiene un tamaño de volumen de 4 TB, se monta a. `/var/local/rangedb/0`, utilizando el nombre del dispositivo `/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba` en la `/etc/fstab` archivo:



Pasos

1. Complete los siguientes pasos para registrar los volúmenes de almacenamiento que han fallado y sus nombres de dispositivo:

   a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.

   b. Selecciona **SITE** > **Nodo de almacenamiento fallido** > **LDR** > **Almacenamiento** > **Descripción general** > **Principal** y busca almacenes de objetos con alarmas.

Object Stores

ID	Total	Available	Stored Data	Stored (%)	Health
0000	96.6 GB	96.6 GB	823 KB	0.001 %	Error
0001	107 GB	107 GB	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 %	No Errors

c. Seleccione **SITE** > **Nodo de almacenamiento fallido** > **SSM** > **Recursos** > **Descripción general** > **Principal**. Determine el punto de montaje y el tamaño del volumen de cada volumen de almacenamiento con error identificado en el paso anterior.

   Los almacenes de objetos están numerados en notación hexadecimal. Por ejemplo, 0000 es el primer volumen y 000F es el decimosexto volumen. En el ejemplo, el almacén de objetos con un ID de 0000 corresponde a. `/var/local/rangedb/0` Con nombre de dispositivo sdc y un tamaño de 107 GB.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	croot	Online	10.4 GB	4.17 GB	655,360	554,806	Unknown
/var/local	cvloc	Online	96.6 GB	96.1 GB	94,369,792	94,369,423	Unknown
/var/local/rangedb/0	sdc	Online	107 GB	107 GB	104,857,600	104,856,202	Enabled
/var/local/rangedb/1	sdd	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled
/var/local/rangedb/2	sde	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled

2. Inicie sesión en el nodo de almacenamiento con errores:

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

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

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

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

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

3. Ejecute el siguiente script para desmontar un volumen de almacenamiento con errores:

   ```
   sn-unmount-volume object_store_ID
   ```

   La `object_store_ID` Es el ID del volumen de almacenamiento con errores. Por ejemplo, especifique `0` En el comando de un almacén de objetos con ID 0000.

4. Si se le solicita, pulse **y** para detener el servicio Cassandra en función del volumen de almacenamiento 0.

   > Si el servicio Cassandra ya está detenido, no se le preguntará. El servicio Cassandra se ha detenido solo para el volumen 0.

   ```
   root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
   Services depending on storage volume 0 (cassandra) aren't down.
   Services depending on storage volume 0 must be stopped before running
   this script.
   Stop services that require storage volume 0 [y/N]? y
   Shutting down services that require storage volume 0.
   Services requiring storage volume 0 stopped.
   Unmounting /var/local/rangedb/0
   /var/local/rangedb/0 is unmounted.
   ```

   En unos segundos, el volumen se desmonta. Aparecen mensajes que indican cada paso del proceso. El

mensaje final indica que el volumen no está asociado.

5. Si el desmontaje falla porque el volumen está ocupado, puede forzar el desmontaje con el `--use -umountof` opción:

> Forzar un desmontaje con el `--use-umountof` la opción puede hacer que los procesos o servicios que utilizan el volumen se comporten inesperadamente o se bloqueen.

```
root@Storage-180:~ # sn-unmount-volume --use-umountof
/var/local/rangedb/2
Unmounting /var/local/rangedb/2 using umountof
/var/local/rangedb/2 is unmounted.
Informing LDR service of changes to storage volumes
```

Recuperar volúmenes de almacenamiento con fallos y reconstruir la base de datos de Cassandra

Debe ejecutar una secuencia de comandos que reformatea y remonta el almacenamiento en volúmenes de almacenamiento con fallos y reconstruye la base de datos Cassandra en el nodo de almacenamiento si el sistema determina que es necesario.

Antes de empezar

- Usted tiene la `Passwords.txt` archivo.
- Las unidades del sistema en el servidor están intactas.
- Se ha identificado la causa del fallo y, si es necesario, ya se ha adquirido un hardware de almacenamiento de reemplazo.
- El tamaño total del almacenamiento de reemplazo es el mismo que el original.
- Comprobó que un decomisionado del nodo de almacenamiento no está en curso o que ha pausado el procedimiento para decomisionar el nodo. (En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **misión**.)
- Ha comprobado que una expansión no está en curso. (En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **expansión**.)
- Ya tienes "se revisaron las advertencias sobre la recuperación del volumen de almacenamiento".

Pasos

1. Según sea necesario, reemplace el almacenamiento físico o virtual con errores asociado a los volúmenes de almacenamiento con errores que ha identificado y desmontado anteriormente.

   No vuelva a montar los volúmenes en este paso. El almacenamiento se vuelve a montar y se añade a. `/etc/fstab` en un paso posterior.

2. En Grid Manager, vaya a **NODES** > **`appliance Storage Node`** > **Hardware**. En la sección StorageGRID Appliance de la página, compruebe que el modo RAID de almacenamiento esté en buen estado.
3. Inicie sesión en el nodo de almacenamiento con errores:

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

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

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

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

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

4. Utilice un editor de texto (vi o vim) para eliminar los volúmenes con errores del `/etc/fstab` y, a continuación, guarde el archivo.

> Comentando un volumen fallido en el `/etc/fstab` el archivo no es suficiente. Debe eliminarse el volumen de `fstab` a medida que el proceso de recuperación verifica que todas las líneas del `fstab` el archivo coincide con los sistemas de archivos montados.

5. Vuelva a formatear los volúmenes de almacenamiento con fallos y vuelva a generar la base de datos de Cassandra si es necesario. Introduzca: `reformat_storage_block_devices.rb`

   - Cuando se desmonta el volumen de almacenamiento 0, las solicitudes y los mensajes indicarán que el servicio Cassandra se está deteniendo.
   - Se le pedirá que reconstruya la base de datos de Cassandra si es necesario.
     - Revise las advertencias. Si no se aplica ninguno de ellos, vuelva a generar la base de datos Cassandra. Introduzca: **Y**
     - Si hay más de un nodo de almacenamiento desconectado o si se ha reconstruido otro nodo de almacenamiento en los últimos 15 días. Introduzca: **N**

       La secuencia de comandos se cerrará sin reconstruir Cassandra. Póngase en contacto con el soporte técnico.
   - Para cada unidad de configuración del nodo de almacenamiento, cuando se le solicite lo siguiente: `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`, escriba una de las siguientes respuestas:
     - **y** para volver a formatear una unidad con errores. De esta forma, se vuelve a formatear el volumen de almacenamiento y se agrega el volumen de almacenamiento reformateado al `/etc/fstab` archivo.
     - **n** si la unidad no contiene errores, y no desea volver a formatearla.

> Al seleccionar **n**, se sale de la secuencia de comandos. Monte la unidad (si cree que los datos en ella deben conservarse y que la unidad se ha desmontado de error) o quite la unidad. A continuación, ejecute el `reformat_storage_block_devices.rb` comando de nuevo.

> Algunos procedimientos de recuperación de StorageGRID usan Reaper para gestionar las reparaciones de Cassandra. Las reparaciones se realizan automáticamente tan pronto como se hayan iniciado los servicios relacionados o necesarios. Es posible que note la salida de un script que menciona “reaper” o “Cassandra repair”. Si ve un mensaje de error que indica que la reparación ha fallado, ejecute el comando indicado en el mensaje de error.

En el siguiente ejemplo, la unidad `/dev/sdf` Se debe volver a formatear y Cassandra no tuvo que ser reconstruida:

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? y
Successfully formatted /dev/sdf with UUID b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done.  Now do manual steps to
restore copies of data.
```

Una vez que se reformateen y se vuelvan a montar los volúmenes de almacenamiento y se completen las operaciones de Cassandra necesarias, es posible "Restaurar datos de objetos con Grid Manager".

Restaure los datos de objetos al volumen de almacenamiento donde la unidad del sistema esté intacta

Después de recuperar un volumen de almacenamiento en un nodo de almacenamiento donde la unidad del sistema esté intacta, se pueden restaurar los datos de objetos replicados o de código de borrado que se perdieron si se produjo un error en el volumen de almacenamiento.

¿Qué procedimiento debo usar?

Siempre que sea posible, restaure los datos del objeto utilizando la página **Volume restoration** en Grid Manager.

- Si los volúmenes aparecen en **MANTENIMIENTO** > **Restauración de volumen** > **Nodos a restaurar**, restaure los datos del objeto con el "Página de restauración de volúmenes en Grid Manager".
- Si los volúmenes no aparecen en **MANTENIMIENTO** > **Restauración de volumen** > **Nodos a restaurar**, siga los pasos que se indican a continuación para usar el `repair-data` script para restaurar datos de objeto.

  Si el nodo de almacenamiento recuperado contiene menos volúmenes que el nodo en el que sustituye, debe utilizar el `repair-data` guión.

> El script repair-data está obsoleto y se eliminará en una versión futura. Cuando sea posible, utilice el "Procedimiento de restauración de volúmenes en Grid Manager".

Utilice la `repair-data` script para restaurar datos de objeto

Antes de empezar

- Ha confirmado que el nodo de almacenamiento recuperado tiene un estado de conexión de **Connected** En la ficha **NODES** > **Descripción general** de Grid Manager.

Acerca de esta tarea

Los datos de objetos se pueden restaurar desde otros nodos de almacenamiento, un nodo de archivado o un pool de almacenamiento en cloud si se configuran las reglas de gestión del ciclo de vida de la información del grid de modo que las copias de objetos estén disponibles.

Tenga en cuenta lo siguiente:

- Si se configuró una regla de ILM para almacenar una sola copia replicada y esa copia estaba en un volumen de almacenamiento que falló, no podrá recuperar el objeto.
- Si la única copia restante de un objeto se encuentra en un Cloud Storage Pool, StorageGRID debe emitir varias solicitudes al extremo Cloud Storage Pool para restaurar datos de objetos. Antes de realizar este procedimiento, póngase en contacto con el soporte técnico para obtener ayuda a la hora de calcular el plazo de recuperación y los costes asociados.
- Si la única copia restante de un objeto se encuentra en un nodo de archivado, los datos de objeto se recuperan del nodo de archivado. La restauración de datos de objetos en un nodo de almacenamiento desde un nodo de archivado tarda más que en restaurar copias de otros nodos de almacenamiento, debido a la latencia asociada a las recuperaciones desde sistemas de almacenamiento de archivado externos.

Acerca de la `repair-data` guión

Para restaurar datos de objeto, ejecute el `repair-data` guión. Este script inicia el proceso de restauración de datos de objetos y funciona con el análisis de ILM para garantizar que se cumplan las reglas de ILM.

Seleccione **datos replicados** o **datos codificados con borrado (EC)** a continuación para conocer las diferentes opciones para `repair-data` script, en función de si va a restaurar datos replicados o datos codificados de borrado. Si necesita restaurar ambos tipos de datos, debe ejecutar ambos conjuntos de comandos.

Para obtener más información acerca de `repair-data` guión, introduzca `repair-data --help` Desde la línea de comandos del nodo de administrador principal.

El script repair-data está obsoleto y se eliminará en una versión futura. Cuando sea posible, utilice el "Procedimiento de restauración de volúmenes en Grid Manager".

Datos replicados

Hay dos comandos disponibles para restaurar los datos replicados, según si necesita reparar el nodo completo o solo ciertos volúmenes del nodo:

```
repair-data start-replicated-node-repair

repair-data start-replicated-volume-repair
```

Puede realizar un seguimiento de las reparaciones de los datos replicados con este comando:

```
repair-data show-replicated-repair-status
```

Datos con código de borrado (EC)

Hay dos comandos disponibles para restaurar datos codificados de borrado a partir de si necesita reparar el nodo completo o solo ciertos volúmenes en el nodo:

```
repair-data start-ec-node-repair

repair-data start-ec-volume-repair
```

Puede realizar un seguimiento de las reparaciones de datos codificados de borrado con este comando:

```
repair-data show-ec-repair-status
```

> Las reparaciones de datos codificados para borrado pueden comenzar con algunos nodos de almacenamiento sin conexión. Sin embargo, si no se pueden tener en cuenta todos los datos con código de borrado, no se podrá completar la reparación. La reparación se completará después de que todos los nodos estén disponibles.

> El trabajo de reparación de la CE reserva temporalmente una gran cantidad de almacenamiento. Es posible que se activen las alertas de almacenamiento, pero se resolverán cuando se complete la reparación. Si no hay suficiente almacenamiento para la reserva, el trabajo de reparación de la CE fallará. Las reservas de almacenamiento se liberan cuando se completa el trabajo de reparación de EC, tanto si el trabajo ha fallado como si ha sido correcto.

Busque el nombre de host del nodo de almacenamiento

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Utilice la `/etc/hosts` File para encontrar el nombre de host del nodo de almacenamiento para los volúmenes de almacenamiento restaurados. Para ver una lista de todos los nodos de la cuadrícula,

introduzca lo siguiente: `cat /etc/hosts`.

Repare los datos si todos los volúmenes presentan errores

Si todos los volúmenes de almacenamiento presentan errores, repare todo el nodo. Siga las instrucciones para **datos replicados**, **datos codificados con borrado (EC)**, o ambos, en función de si utiliza datos replicados, datos codificados con borrado (EC), o ambos.

Si solo se produjo un error en algunos volúmenes, vaya a. Repare los datos si solo algunos volúmenes han fallado.

> No puedes correr `repair-data` operaciones para más de un nodo a la vez. Para recuperar varios nodos, póngase en contacto con el soporte técnico.

Datos replicados

Si la cuadrícula incluye datos replicados, utilice `repair-data start-replicated-node-repair` con el `--nodes` opción, donde `--nodes` Es el nombre de host (nombre del sistema), para reparar todo el nodo de almacenamiento.

Este comando repara los datos replicados en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> A medida que se restauran los datos del objeto, la alerta de **Objetos perdidos** se activa si el sistema StorageGRID no puede localizar los datos de objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Debe determinar la causa de la pérdida y si es posible la recuperación. Consulte "Investigar los objetos perdidos".

Datos con código de borrado (EC)

Si el grid contiene datos con código de borrado, utilice `repair-data start-ec-node-repair` con el `--nodes` opción, donde `--nodes` Es el nombre de host (nombre del sistema), para reparar todo el nodo de almacenamiento.

Este comando repara los datos codificados con borrado en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

La operación devuelve un valor exclusivo `repair ID` eso lo identifica `repair_data` funcionamiento. Utilice esto `repair ID` para realizar un seguimiento del progreso y el resultado de la `repair_data` funcionamiento. No se devuelve ningún otro comentario cuando finaliza el proceso de recuperación.

> Las reparaciones de datos codificados para borrado pueden comenzar con algunos nodos de almacenamiento sin conexión. La reparación se completará después de que todos los nodos estén disponibles.

Repare los datos si solo algunos volúmenes han fallado

Si solo se produjo un error en algunos de los volúmenes, repare los volúmenes afectados. Siga las

instrucciones para **datos replicados**, **datos codificados con borrado (EC)**, o ambos, en función de si utiliza datos replicados, datos codificados con borrado (EC), o ambos.

Si todos los volúmenes presentan errores, vaya a. Repare los datos si todos los volúmenes presentan errores.

Introduzca los ID de volumen en hexadecimal. Por ejemplo: `0000` es el primer volumen y. `000F` es el volumen decimosexto. Puede especificar un volumen, un rango de volúmenes o varios volúmenes que no estén en una secuencia.

Todos los volúmenes deben estar en el mismo nodo de almacenamiento. Si necesita restaurar volúmenes para más de un nodo de almacenamiento, póngase en contacto con el soporte técnico.

Datos replicados

Si la cuadrícula contiene datos replicados, utilice `start-replicated-volume-repair` con el `--nodes` opción para identificar el nodo (dónde `--nodes` es el nombre de host del nodo). A continuación, agregue el `--volumes` o. `--volume-range` como se muestra en los siguientes ejemplos.

Single volume: Este comando restaura los datos replicados al volumen `0002` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Intervalo de volúmenes: Este comando restaura los datos replicados a todos los volúmenes del intervalo `0003` para `0009` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Varios volúmenes que no están en una secuencia: Este comando restaura los datos replicados a los volúmenes `0001`, `0005`, y. `0008` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> ⓘ A medida que se restauran los datos del objeto, la alerta de **Objetos perdidos** se activa si el sistema StorageGRID no puede localizar los datos de objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Tenga en cuenta la descripción de la alerta y las acciones recomendadas para determinar la causa de la pérdida y si la recuperación es posible.

Datos con código de borrado (EC)

Si el grid contiene datos con código de borrado, utilice `start-ec-volume-repair` con el `--nodes` opción para identificar el nodo (dónde `--nodes` es el nombre de host del nodo). A continuación, agregue el `--volumes` o. `--volume-range` como se muestra en los siguientes ejemplos.

Volumen único: Este comando restaura los datos codificados por borrado al volumen `0007` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Intervalo de volúmenes: Este comando restaura los datos codificados por borrado a todos los volúmenes del intervalo `0004` para `0006` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Múltiples volúmenes no en una secuencia: Este comando restaura datos codificados por borrado a volúmenes `000A`, `000C`, y. `000E` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

La `repair-data` la operación devuelve un valor exclusivo `repair ID` eso lo identifica `repair_data` funcionamiento. Utilice esto `repair ID` para realizar un seguimiento del progreso y el resultado de la `repair_data` funcionamiento. No se devuelve ningún otro comentario cuando finaliza el proceso de

recuperación.

> Las reparaciones de datos codificados para borrado pueden comenzar con algunos nodos de almacenamiento sin conexión. La reparación se completará después de que todos los nodos estén disponibles.

Reparaciones del monitor

Supervise el estado de los trabajos de reparación, en función de si utiliza **datos replicados**, **datos codificados por borrado (EC)** o ambos.

También es posible supervisar el estado de los trabajos de restauración de volúmenes en curso y ver un historial de los trabajos de restauración completados en "Administrador de grid".

Datos replicados

- Para obtener un porcentaje de finalización estimado para la reparación replicada, agregue el `show-replicated-repair-status` opción del comando repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Para determinar si las reparaciones están completas:
  a. Seleccione **NODES** > ***Storage Node que se está reparando*** > **ILM**.
  b. Revise los atributos en la sección Evaluación. Una vez completadas las reparaciones, el atributo **esperando - todo** indica 0 objetos.
- Para supervisar la reparación con más detalle:
  a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
  b. Seleccione ***grid*** > ***nodo de almacenamiento que se está reparando*** > **LDR** > **almacén de datos**.
  c. Utilice una combinación de los siguientes atributos para determinar, como sea posible, si las reparaciones replicadas se han completado.

  > Puede haber incoherencias en Cassandra y no se realiza un seguimiento de las reparaciones fallidas.

  - **Reparaciones intentadas (XRPA)**: Utilice este atributo para realizar un seguimiento del progreso de las reparaciones replicadas. Este atributo aumenta cada vez que un nodo de almacenamiento intenta reparar un objeto de alto riesgo. Cuando este atributo no aumenta durante un período más largo que el período de exploración actual (proporcionado por el atributo **período de exploración — estimado**), significa que el análisis de ILM no encontró objetos de alto riesgo que necesitan ser reparados en ningún nodo.

    > Los objetos de alto riesgo son objetos que corren el riesgo de perderse por completo. Esto no incluye objetos que no cumplen con la configuración de ILM.

  - **Período de exploración — estimado (XSCM)**: Utilice este atributo para estimar cuándo se aplicará un cambio de directiva a objetos ingeridos previamente. Si el atributo **reparos intentados** no aumenta durante un período más largo que el período de adquisición actual, es probable que se realicen reparaciones replicadas. Tenga en cuenta que el período de adquisición puede cambiar. El atributo **período de exploración — estimado (XSCM)** se aplica a toda la cuadrícula y es el máximo de todos los periodos de exploración de nodos. Puede consultar el historial de atributos **período de exploración — Estimated** de la cuadrícula para determinar un intervalo de tiempo adecuado.

Datos con código de borrado (EC)

Para supervisar la reparación de datos codificados mediante borrado y vuelva a intentar cualquier solicitud que pudiera haber fallado:

1. Determine el estado de las reparaciones de datos codificadas por borrado:
   - Seleccione **SUPPORT** > **Tools** > **Metrics** para ver el tiempo estimado hasta la finalización y el porcentaje de finalización del trabajo actual. A continuación, seleccione **EC Overview** en la sección Grafana. Consulte los paneles **tiempo estimado de trabajo de Grid EC hasta finalización** y **Porcentaje de trabajo de Grid EC completado**.

- Utilice este comando para ver el estado de un elemento específico `repair-data` operación:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilice este comando para enumerar todas las reparaciones:

  ```
  repair-data show-ec-repair-status
  ```

El resultado muestra información, como `repair ID`, para todas las reparaciones que se estén ejecutando anteriormente y actualmente.

2. Si el resultado muestra que la operación de reparación ha dado error, utilice el `--repair-id` opción de volver a intentar la reparación.

   Este comando vuelve a intentar una reparación de nodo con fallos mediante el ID de reparación 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Este comando reintenta realizar una reparación de volumen con fallos mediante el ID de reparación 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Comprobar el estado del almacenamiento después de recuperar los volúmenes de almacenamiento

Después de recuperar los volúmenes de almacenamiento, debe comprobar que el estado deseado del nodo de almacenamiento está establecido en online y que el estado estará en línea de forma predeterminada cada vez que se reinicie el servidor del nodo de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- El nodo de almacenamiento se ha recuperado y se completó la recuperación de datos.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Compruebe los valores de **Nodo de almacenamiento recuperado** > **LDR** > **Almacenamiento** > **Estado de almacenamiento — deseado** y **Estado de almacenamiento — actual**.

   El valor de ambos atributos debe ser en línea.

3. Si el estado de almacenamiento — deseado está establecido en sólo lectura, realice los siguientes pasos:
   a. Haga clic en la ficha **Configuración**.
   b. En la lista desplegable **Estado de almacenamiento — deseado**, seleccione **Online**.
   c. Haga clic en **aplicar cambios**.
   d. Haga clic en la ficha **Descripción general** y confirme que los valores de **Estado de almacenamiento — deseado** y **Estado de almacenamiento — actual** se actualizan a Online.

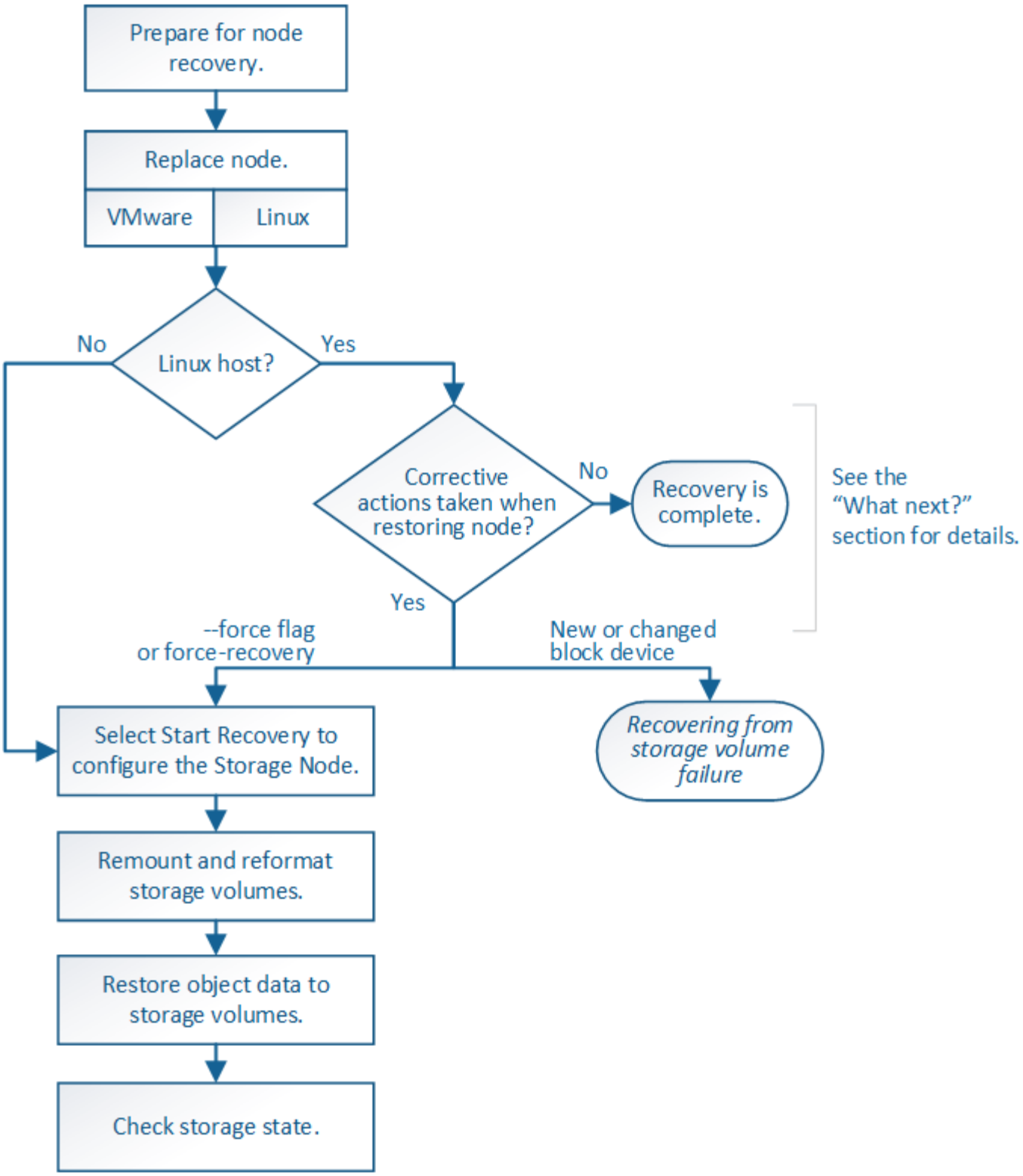
Recupere datos de un fallo de unidad del sistema

Recupere de un fallo de la unidad del sistema: Flujo de trabajo

Si falló la unidad del sistema en un nodo de almacenamiento basado en software, el nodo de almacenamiento no está disponible para el sistema StorageGRID. Debe completar un conjunto específico de tareas para recuperar el sistema de un fallo de unidad.

Utilice este procedimiento para recuperarse de un error de la unidad del sistema en un nodo de almacenamiento basado en software. Este procedimiento incluye los pasos que se deben seguir si alguno de los volúmenes de almacenamiento también falla o no puede volver a montarse.

> Este procedimiento se aplica únicamente a nodos de almacenamiento basados en software. Debe seguir un procedimiento diferente a. "Recuperar un nodo de almacenamiento de dispositivo".



Advertencias para la recuperación de las unidades del sistema del nodo de almacenamiento

Antes de recuperar una unidad de sistema con fallos de un nodo de almacenamiento, revise el documento general "advertencias y consideraciones para la recuperación de nodos de grid" y las siguientes advertencias específicas.

Los nodos de almacenamiento tienen una base de datos Cassandra que incluye metadatos de objetos. La base de datos Cassandra puede reconstruirse en las siguientes circunstancias:

- Un nodo de almacenamiento se vuelve a conectar después de haber estado desconectado más de 15 días.
- Se produjo un error en un volumen de almacenamiento y se recuperó.
- La unidad del sistema y uno o más volúmenes de almacenamiento fallan y se recuperan.

Cuando se reconstruye Cassandra, el sistema utiliza información de otros nodos de almacenamiento. Si hay demasiados nodos de almacenamiento sin conexión, es posible que algunos datos de Cassandra no estén disponibles. Si Cassandra se ha reconstruido recientemente, es posible que los datos de Cassandra aún no sean coherentes en toda la cuadrícula. Se pueden perder datos si Cassandra se vuelve a generar cuando hay demasiados nodos de almacenamiento sin conexión o si se reconstruyen dos o más nodos de almacenamiento en un plazo de 15 días entre sí.

Si más de un nodo de almacenamiento presenta errores (o está sin conexión), póngase en contacto con el soporte técnico. No realice el siguiente procedimiento de recuperación. Podrían perderse datos.

Si este es el segundo fallo del nodo de almacenamiento en menos de 15 días después de un fallo o una recuperación en el nodo de almacenamiento, póngase en contacto con el soporte técnico. La reconstrucción de Cassandra en dos o más nodos de almacenamiento en 15 días puede provocar la pérdida de datos.

Si se produce un error en más de un nodo de almacenamiento de un sitio, es posible que se requiera un procedimiento de recuperación del sitio. Consulte "Cómo el soporte técnico recupera un sitio".

Si este nodo de almacenamiento está en modo de mantenimiento de solo lectura para permitir la recuperación de objetos por otro nodo de almacenamiento con volúmenes de almacenamiento con fallos, recupere los volúmenes en el nodo de almacenamiento con volúmenes de almacenamiento con errores antes de recuperar este nodo de almacenamiento con errores. Consulte las instrucciones a. "recupere de un fallo en el volumen de almacenamiento donde la unidad del sistema esté intacta".

Si las reglas de ILM se configuran para almacenar una sola copia replicada y existe una en un volumen de almacenamiento donde se produjo un error, no podrá recuperar el objeto.

Si encuentra una alarma Services: Status - Cassandra (SVST) durante la recuperación, consulte "Recuperar volúmenes de almacenamiento con fallos y reconstruir la base de datos de Cassandra". Una vez reconstruida Cassandra, las alarmas se deberían borrar. Si las alarmas no se borran, póngase en contacto con el soporte técnico.

Sustituya el nodo de almacenamiento

Si la unidad del sistema presenta errores, primero debe reemplazar el nodo de almacenamiento.

Debe seleccionar el procedimiento de sustitución de nodo para su plataforma. Los pasos para reemplazar un nodo son los mismos para todos los tipos de nodos de grid.

Este procedimiento se aplica únicamente a nodos de almacenamiento basados en software. Debe seguir un procedimiento diferente a. "Recuperar un nodo de almacenamiento de dispositivo".

Linux: Si no está seguro de si la unidad del sistema ha fallado, siga las instrucciones para reemplazar el nodo para determinar qué pasos de recuperación son necesarios.

Plataforma	Procedimiento
VMware	"Sustituya un nodo VMware"
Linux	"Sustituya un nodo Linux"
OpenStack	Las operaciones de recuperación ya no son compatibles con los archivos de disco de máquinas virtuales y los scripts de OpenStack que proporciona NetApp. Si necesita recuperar un nodo que se ejecuta en una implementación de OpenStack, descargue los archivos para el sistema operativo Linux. A continuación, siga el procedimiento para "Reemplazar un nodo Linux".

Seleccione Start Recovery para configurar Storage Node

Después de reemplazar un nodo de almacenamiento, debe seleccionar Iniciar recuperación en el Administrador de grid para configurar el nodo nuevo como reemplazo del nodo con error.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento.
- Implementó y configuró el nodo de reemplazo.
- Tiene la fecha de inicio de cualquier trabajo de reparación para datos codificados de borrado.
- Ha verificado que el nodo de almacenamiento no se ha reconstruido en los últimos 15 días.

Acerca de esta tarea

Si el nodo de almacenamiento está instalado como un contenedor en un host Linux, debe realizar este paso solo si uno de estos valores es true:

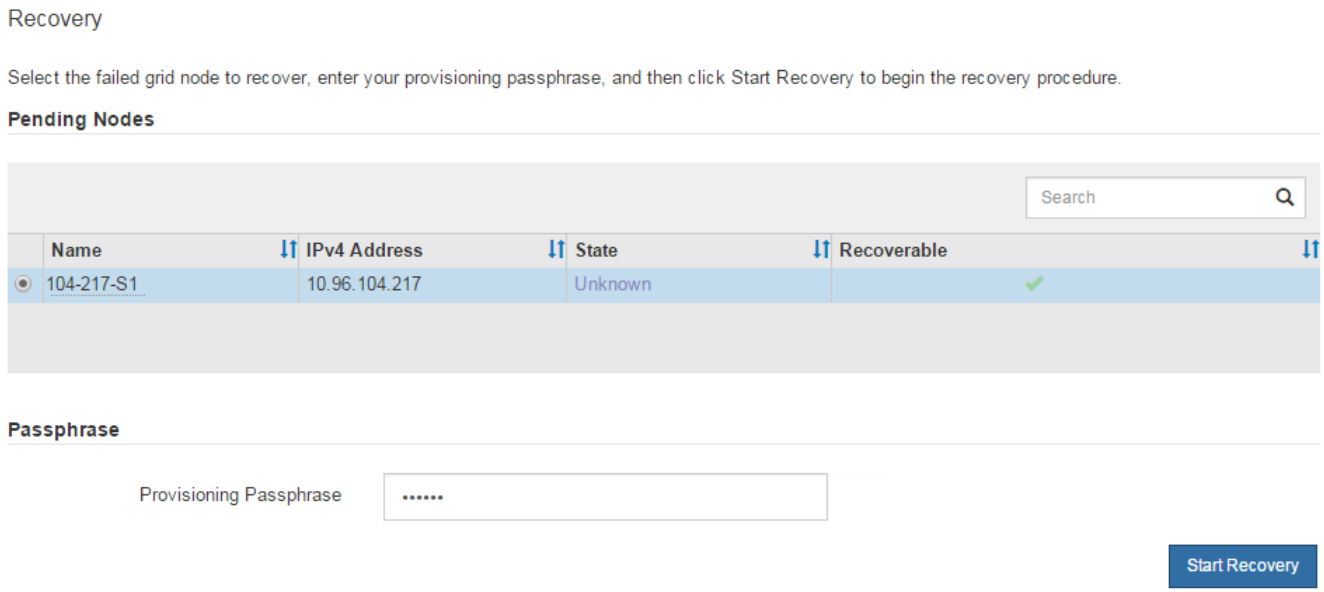
- Tenía que usar el `--force` indicador para importar el nodo o ha emitido `storagegrid node force-recovery node-name`
- Tenía que hacer una reinstalación de nodo completa o tenía que restaurar /var/local.

Pasos

1. En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **recuperación**.
2. Seleccione el nodo de cuadrícula que desea recuperar en la lista Pending Nodes.

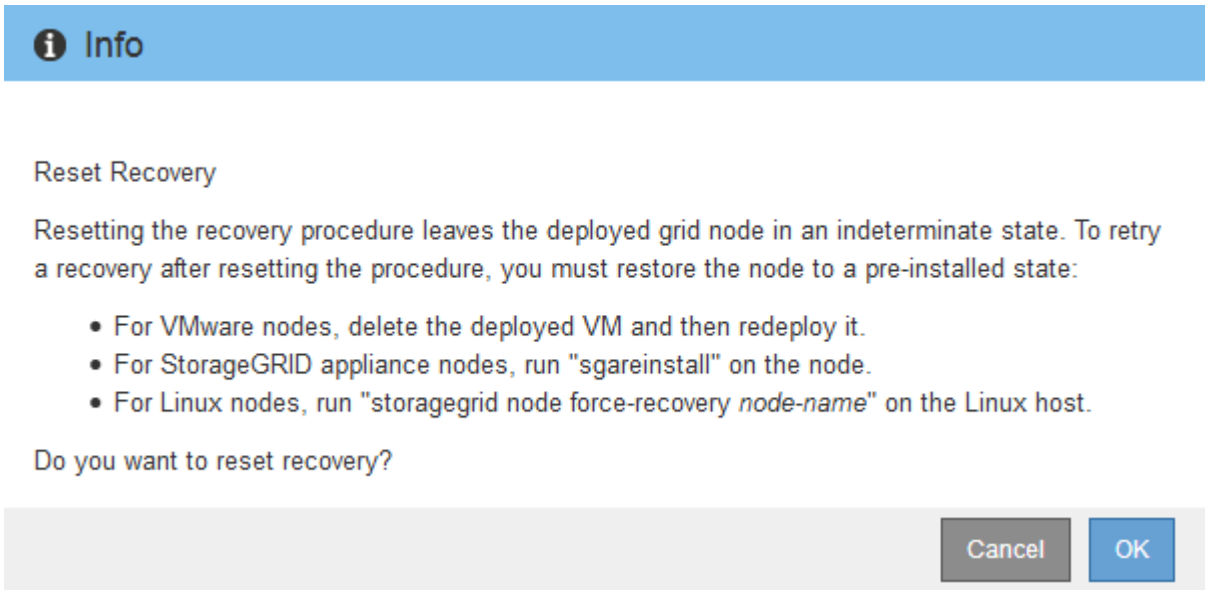
   Los nodos aparecen en la lista después de que fallan, pero no puede seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduzca la **frase de paso de aprovisionamiento**.
4. Haga clic en **Iniciar recuperación**.



5. Supervise el progreso de la recuperación en la tabla recuperando Grid Node.

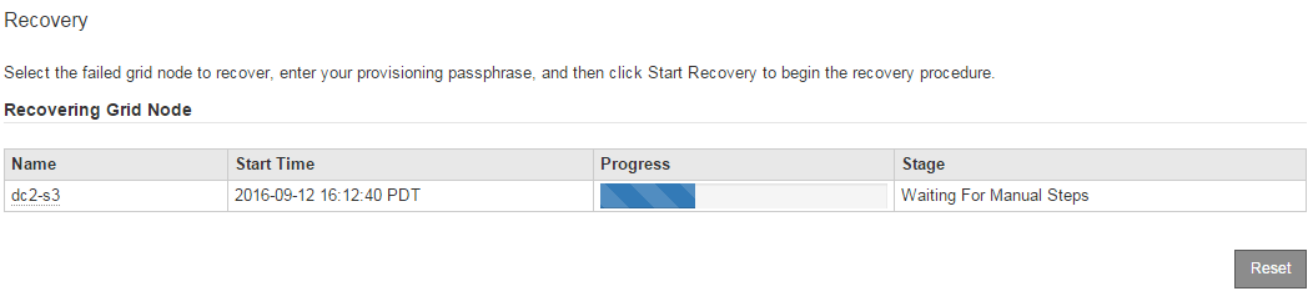
> Mientras se está ejecutando el procedimiento de recuperación, puede hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparece un cuadro de diálogo que indica que el nodo quedará en un estado indeterminado si restablece el procedimiento.



Si desea volver a intentar la recuperación después de restablecer el procedimiento, debe restaurar el nodo a un estado preinstalado, de la manera siguiente:

- **VMware**: Elimine el nodo de la cuadrícula virtual desplegada. A continuación, una vez que esté listo para reiniciar la recuperación, vuelva a poner el nodo en marcha.
- **Linux**: Reinicie el nodo ejecutando este comando en el host Linux: `storagegrid node force-recovery node-name`

6. Cuando el nodo de almacenamiento alcance la etapa «Esperando pasos manuales», vaya a. "Volver a montar y volver a formatear los volúmenes de almacenamiento (pasos manuales)".



Volver a montar y volver a formatear los volúmenes de almacenamiento (pasos manuales)

Se deben ejecutar manualmente dos scripts para volver a montar los volúmenes de almacenamiento conservados y formatear los volúmenes de almacenamiento con errores. El primer script remonta volúmenes con un formato correcto como volúmenes de almacenamiento de StorageGRID. El segundo script reformatea todos los volúmenes desmontados, reconstruye Cassandra, si es necesario, e inicia los servicios.

Antes de empezar

- Ya ha sustituido el hardware de todos los volúmenes de almacenamiento con errores que necesite sustituir.

  Ejecutando el `sn-remount-volumes` el script puede ayudar a identificar volúmenes de almacenamiento adicionales donde se han producido fallos.

- Comprobó que un decomisionado del nodo de almacenamiento no está en curso o que ha pausado el procedimiento para decomisionar el nodo. (En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **misión**.)
- Ha comprobado que una expansión no está en curso. (En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **expansión**.)
- Ya tienes "Se revisaron las advertencias de recuperación de la unidad del sistema en el nodo de almacenamiento".

> Póngase en contacto con el soporte técnico si hay más de un nodo de almacenamiento sin conexión o si se ha reconstruido un nodo de almacenamiento en este grid en los últimos 15 días. No ejecute el `sn-recovery-postinstall.sh` guión. Si se reconstruye Cassandra en dos o más nodos de almacenamiento en un plazo de 15 días entre sí, se puede producir una pérdida de datos.

Acerca de esta tarea

Para completar este procedimiento, realice estas tareas de alto nivel:

- Inicie sesión en el nodo de almacenamiento recuperado.
- Ejecute el `sn-remount-volumes` script para volver a montar volúmenes de almacenamiento con formato correcto. Cuando se ejecuta este script, realiza lo siguiente:
  - Monta y desmonta cada volumen de almacenamiento para reproducir el diario XFS.

- Realiza una comprobación de consistencia de archivos XFS.
- Si el sistema de archivos es coherente, determina si el volumen de almacenamiento es un volumen de almacenamiento de StorageGRID con el formato correcto.
- Si el volumen de almacenamiento tiene el formato correcto, vuelve a montar el volumen de almacenamiento. Todos los datos existentes en el volumen permanecen intactos.

- Revise el resultado del script y resuelva cualquier problema.
- Ejecute el `sn-recovery-postinstall.sh` guión. Cuando se ejecuta este script, realiza lo siguiente.

> No reinicie un nodo de almacenamiento durante la recuperación antes de ejecutar `sn-recovery-postinstall.sh` para volver a formatear los volúmenes de almacenamiento en los que se ha producido un error y restaurar los metadatos de objetos. Reinicie el nodo de almacenamiento antes `sn-recovery-postinstall.sh` Completa provoca errores en los servicios que se intentan iniciar y provoca que los nodos del dispositivo StorageGRID salgan del modo de mantenimiento. Consulte el paso para script posterior a la instalación.

  - Vuelva a formatear los volúmenes de almacenamiento que tenga `sn-remount-volumes` la secuencia de comandos no se pudo montar o se encontró que el formato era incorrecto.

> Si se vuelve a formatear un volumen de almacenamiento, se pierden todos los datos de ese volumen. Debe realizar un procedimiento adicional para restaurar datos de objetos desde otras ubicaciones de la cuadrícula, suponiendo que se hayan configurado las reglas de ILM para almacenar más de una copia de objetos.

  - Reconstruye la base de datos Cassandra en el nodo, si es necesario.
  - Inicia los servicios en el nodo de almacenamiento.

Pasos

1. Inicie sesión en el nodo de almacenamiento recuperado:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Ejecute el primer script para volver a montar todos los volúmenes de almacenamiento con un formato correcto.

> Si todos los volúmenes de almacenamiento son nuevos y se deben formatear, o bien si se producen errores en todos los volúmenes de almacenamiento, es posible omitir este paso y ejecutar el segundo script para volver a formatear todos los volúmenes de almacenamiento desmontados.

   a. Ejecute el script: `sn-remount-volumes`

      Este script puede tardar horas en ejecutarse en volúmenes de almacenamiento que contienen datos.

b. A medida que se ejecuta el script, revise la salida y responda a las peticiones.

> Según sea necesario, puede utilizar la `tail -f` comando para supervisar el contenido del archivo de registro del script (`/var/local/log/sn-remount-volumes.log`) . El archivo de registro contiene información más detallada que el resultado de la línea de comandos.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
```

```
to
recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
```

```
volume and re-run this script.
```

En la salida de ejemplo, se remontó correctamente un volumen de almacenamiento y se produjeron errores en tres volúmenes de almacenamiento.

- `/dev/sdb` Superó la comprobación de consistencia del sistema de archivos XFS y tenía una estructura de volumen válida, por lo que se remontó correctamente. Se conservan los datos de los dispositivos que se remontan mediante el script.
- `/dev/sdc` No se pudo realizar la comprobación de consistencia del sistema de archivos XFS porque el volumen de almacenamiento era nuevo o estaba dañado.
- `/dev/sdd` no se ha podido montar porque el disco no se ha inicializado o porque el superbloque del disco está dañado. Cuando el script no puede montar un volumen de almacenamiento, le pregunta si desea ejecutar la comprobación de consistencia del sistema de archivos.
  - Si el volumen de almacenamiento está conectado a un nuevo disco, responda **N** al indicador. No es necesario que compruebe el sistema de archivos en un disco nuevo.
  - Si el volumen de almacenamiento está conectado a un disco existente, responda **y** al indicador. Puede utilizar los resultados de la comprobación del sistema de archivos para determinar el origen de los daños. Los resultados se guardan en la `/var/local/log/sn-remount-volumes.log` archivo de registro.
- `/dev/sde` Pasó la comprobación de consistencia del sistema del archivo XFS y tenía una estructura de volumen válida; sin embargo, el ID de nodo LDR del archivo volId no coincide con el ID de este nodo de almacenamiento (la `configured LDR noid` mostrado en la parte superior). Este mensaje indica que este volumen pertenece a otro nodo de almacenamiento.

3. Revise el resultado del script y resuelva cualquier problema.

> ⚠ Si un volumen de almacenamiento no superó la comprobación de consistencia del sistema de archivos XFS o no pudo montarse, revise con cuidado los mensajes de error del resultado. Debe comprender las implicaciones de ejecutar el `sn-recovery-postinstall.sh` guión en estos volúmenes.

a. Compruebe que los resultados incluyan una entrada de todos los volúmenes esperados. Si hay algún volumen que no aparece en la lista, vuelva a ejecutar el script.

b. Revise los mensajes de todos los dispositivos montados. Asegúrese de que no haya errores que indiquen que un volumen de almacenamiento no pertenece a este nodo de almacenamiento.

   En el ejemplo, el resultado para `/dev/sde` incluye el siguiente mensaje de error:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> ⚠ Si un volumen de almacenamiento se informa como que pertenece a otro nodo de almacenamiento, póngase en contacto con el soporte técnico. Si ejecuta el `sn-recovery-postinstall.sh` script, se reformateará el volumen de almacenamiento, lo que puede provocar la pérdida de datos.

c. Si no se pudo montar ningún dispositivo de almacenamiento, anote el nombre del dispositivo y repare o reemplace el dispositivo.

Debe reparar o sustituir cualquier dispositivo de almacenamiento que no pueda montarse.

Utilizará el nombre del dispositivo para buscar el ID de volumen, que es necesario introducir cuando ejecute el `repair-data` script para restaurar datos de objetos en el volumen (el siguiente procedimiento).

d. Después de reparar o sustituir todos los dispositivos que no se pueden montar, ejecute el `sn-remount-volumes` vuelva a script para confirmar que se han vuelto a montar todos los volúmenes de almacenamiento que pueden remontarse.

Si un volumen de almacenamiento no se puede montar o se formatea de forma incorrecta y se continúa con el siguiente paso, se eliminarán el volumen y todos los datos del volumen. Si tenía dos copias de datos de objetos, sólo tendrá una copia única hasta que complete el siguiente procedimiento (restaurando datos de objetos).

No ejecute el `sn-recovery-postinstall.sh` Script si cree que los datos que quedan en un volumen de almacenamiento con fallos no se pueden reconstruir desde otro lugar del grid (por ejemplo, si la política de ILM usa una regla que solo realice una copia o si los volúmenes han fallado en varios nodos). En su lugar, póngase en contacto con el soporte técnico para determinar cómo recuperar los datos.

4. Ejecute el `sn-recovery-postinstall.sh` guión: `sn-recovery-postinstall.sh`

Este script reformatea todos los volúmenes de almacenamiento que no se pudieron montar o que se encontraron con un formato incorrecto; reconstruye la base de datos de Cassandra en el nodo, si es necesario; e inicia los servicios en el nodo de almacenamiento.

Tenga en cuenta lo siguiente:

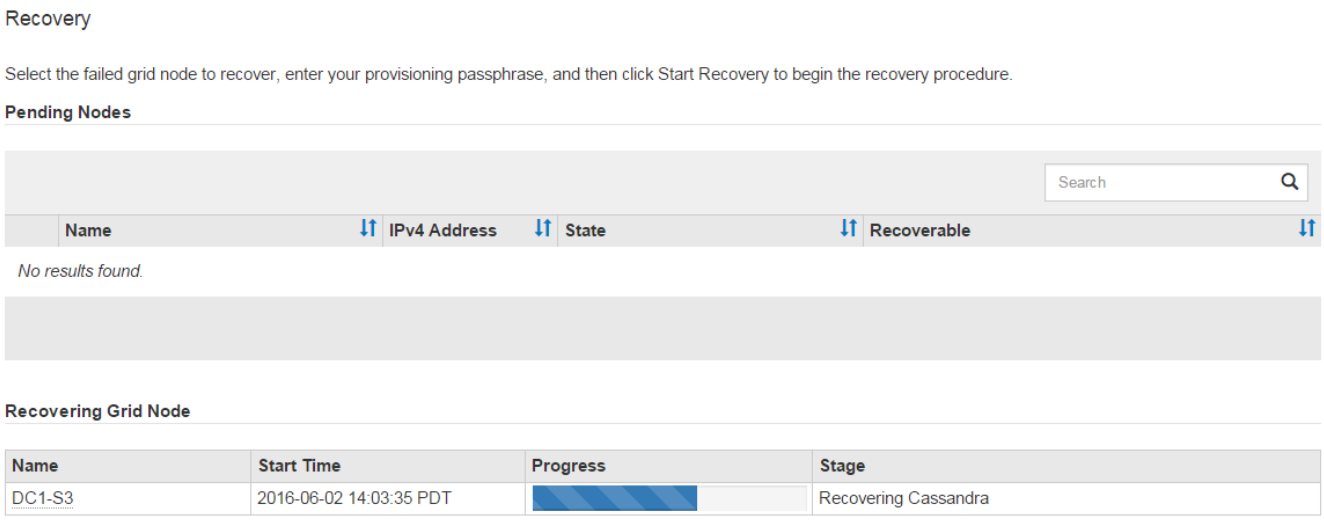
- El script puede tardar horas en ejecutarse.
- En general, debe dejar la sesión SSH sola mientras el script está en ejecución.
- No pulse **Ctrl+C** mientras la sesión SSH esté activa.
- El script se ejecutará en segundo plano si se produce una interrupción de red y finaliza la sesión SSH, pero puede ver el progreso desde la página Recovery.
- Si Storage Node utiliza el servicio RSM, puede parecer que el script se atasca durante 5 minutos mientras se reinician los servicios de nodos. Este retraso de 5 minutos se espera siempre que el servicio RSM arranque por primera vez.

El servicio RSM está presente en los nodos de almacenamiento que incluyen el servicio ADC.

Algunos procedimientos de recuperación de StorageGRID usan Reaper para gestionar las reparaciones de Cassandra. Las reparaciones se realizan automáticamente tan pronto como se hayan iniciado los servicios relacionados o necesarios. Es posible que note la salida de un script que menciona “reaper” o “Cassandra repair”. Si ve un mensaje de error que indica que la reparación ha fallado, ejecute el comando indicado en el mensaje de error.

5. como el `sn-recovery-postinstall.sh` Se ejecuta Script, supervise la página Recovery en Grid Manager.

La barra de progreso y la columna Stage de la página Recovery proporcionan un estado de alto nivel de `sn-recovery-postinstall.sh` guión.



6. Después del `sn-recovery-postinstall.sh` script ha iniciado servicios en el nodo, puede restaurar datos de objetos en cualquier volumen de almacenamiento que haya formateado el script.

   El script le pregunta si desea utilizar el proceso de restauración del volumen de Grid Manager.

   - En la mayoría de los casos, usted debería "Restaurar datos de objetos con Grid Manager". Responda `y` Para utilizar Grid Manager.
   - En raras ocasiones, como cuando se lo indica el soporte técnico o cuando sabe que el nodo de reemplazo tiene menos volúmenes disponibles para el almacenamiento de objetos que el nodo original, debe "restaurar datos de objetos manualmente" con el `repair-data` guión. Si se aplica uno de estos casos, responda `n`.

   > Si responde `n` Para utilizar el proceso de restauración de volúmenes de Grid Manager (restaurar datos de objetos manualmente):
   >
   > - No puede restaurar datos de objetos con Grid Manager.
   > - Puede supervisar el progreso de los trabajos de restauración manual con Grid Manager.

   Después de realizar su selección, el script se completa y se muestran los siguientes pasos para recuperar los datos del objeto. Después de revisar estos pasos, pulse cualquier tecla para volver a la línea de comandos.

Restauración de los datos de objetos en un volumen de almacenamiento (fallo de unidad de sistema)

Después de recuperar los volúmenes de almacenamiento para un nodo de almacenamiento que no sea de dispositivo, se pueden restaurar los datos de objetos replicados o con código de borrado que se perdieron cuando se produjo un error en el nodo de almacenamiento.

¿Qué procedimiento debo usar?

Siempre que sea posible, restaure los datos del objeto utilizando la página **Volume restoration** en Grid Manager.

- Si los volúmenes aparecen en **MANTENIMIENTO** > **Restauración de volumen** > **Nodos a restaurar**, restaure los datos del objeto con el "Página de restauración de volúmenes en Grid Manager".
- Si los volúmenes no aparecen en **MANTENIMIENTO** > **Restauración de volumen** > **Nodos a restaurar**, siga los pasos que se indican a continuación para usar el `repair-data` script para restaurar datos de objeto.

  Si el nodo de almacenamiento recuperado contiene menos volúmenes que el nodo en el que sustituye, debe utilizar el `repair-data` guión.

> El script repair-data está obsoleto y se eliminará en una versión futura. Cuando sea posible, utilice el "Procedimiento de restauración de volúmenes en Grid Manager".

Utilice la `repair-data` script para restaurar datos de objeto

Antes de empezar

- Ha confirmado que el nodo de almacenamiento recuperado tiene un estado de conexión de **Connected** En la ficha **NODES** > **Descripción general** de Grid Manager.

Acerca de esta tarea

Los datos de objetos se pueden restaurar desde otros nodos de almacenamiento, un nodo de archivado o un pool de almacenamiento en cloud si se configuran las reglas de gestión del ciclo de vida de la información del grid de modo que las copias de objetos estén disponibles.

Tenga en cuenta lo siguiente:

- Si se configuró una regla de ILM para almacenar una sola copia replicada y esa copia estaba en un volumen de almacenamiento que falló, no podrá recuperar el objeto.
- Si la única copia restante de un objeto se encuentra en un Cloud Storage Pool, StorageGRID debe emitir varias solicitudes al extremo Cloud Storage Pool para restaurar datos de objetos. Antes de realizar este procedimiento, póngase en contacto con el soporte técnico para obtener ayuda a la hora de calcular el plazo de recuperación y los costes asociados.
- Si la única copia restante de un objeto se encuentra en un nodo de archivado, los datos de objeto se recuperan del nodo de archivado. La restauración de datos de objetos en un nodo de almacenamiento desde un nodo de archivado tarda más que en restaurar copias de otros nodos de almacenamiento, debido a la latencia asociada a las recuperaciones desde sistemas de almacenamiento de archivado externos.

Acerca de la `repair-data` guión

Para restaurar datos de objeto, ejecute el `repair-data` guión. Este script inicia el proceso de restauración de datos de objetos y funciona con el análisis de ILM para garantizar que se cumplan las reglas de ILM.

Seleccione **datos replicados** o **datos codificados con borrado (EC)** a continuación para conocer las diferentes opciones para `repair-data` script, en función de si va a restaurar datos replicados o datos codificados de borrado. Si necesita restaurar ambos tipos de datos, debe ejecutar ambos conjuntos de comandos.

Para obtener más información acerca de `repair-data` guión, introduzca `repair-data --help` Desde la línea de comandos del nodo de administrador principal.

El script repair-data está obsoleto y se eliminará en una versión futura. Cuando sea posible, utilice el "Procedimiento de restauración de volúmenes en Grid Manager".

Datos replicados

Hay dos comandos disponibles para restaurar los datos replicados, según si necesita reparar el nodo completo o solo ciertos volúmenes del nodo:

```
repair-data start-replicated-node-repair

repair-data start-replicated-volume-repair
```

Puede realizar un seguimiento de las reparaciones de los datos replicados con este comando:

```
repair-data show-replicated-repair-status
```

Datos con código de borrado (EC)

Hay dos comandos disponibles para restaurar datos codificados de borrado a partir de si necesita reparar el nodo completo o solo ciertos volúmenes en el nodo:

```
repair-data start-ec-node-repair

repair-data start-ec-volume-repair
```

Puede realizar un seguimiento de las reparaciones de datos codificados de borrado con este comando:

```
repair-data show-ec-repair-status
```

Las reparaciones de datos codificados para borrado pueden comenzar con algunos nodos de almacenamiento sin conexión. Sin embargo, si no se pueden tener en cuenta todos los datos con código de borrado, no se podrá completar la reparación. La reparación se completará después de que todos los nodos estén disponibles.

El trabajo de reparación de la CE reserva temporalmente una gran cantidad de almacenamiento. Es posible que se activen las alertas de almacenamiento, pero se resolverán cuando se complete la reparación. Si no hay suficiente almacenamiento para la reserva, el trabajo de reparación de la CE fallará. Las reservas de almacenamiento se liberan cuando se completa el trabajo de reparación de EC, tanto si el trabajo ha fallado como si ha sido correcto.

Busque el nombre de host del nodo de almacenamiento

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

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

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

2. Utilice la `/etc/hosts` File para encontrar el nombre de host del nodo de almacenamiento para los volúmenes de almacenamiento restaurados. Para ver una lista de todos los nodos de la cuadrícula, introduzca lo siguiente: `cat /etc/hosts`.

Repare los datos si todos los volúmenes presentan errores

Si todos los volúmenes de almacenamiento presentan errores, repare todo el nodo. Siga las instrucciones para **datos replicados**, **datos codificados con borrado (EC)**, o ambos, en función de si utiliza datos replicados, datos codificados con borrado (EC), o ambos.

Si solo se produjo un error en algunos volúmenes, vaya a. Repare los datos si solo algunos volúmenes han fallado.

> No puedes correr `repair-data` operaciones para más de un nodo a la vez. Para recuperar varios nodos, póngase en contacto con el soporte técnico.

Datos replicados

Si la cuadrícula incluye datos replicados, utilice `repair-data start-replicated-node-repair` con el `--nodes` opción, donde `--nodes` Es el nombre de host (nombre del sistema), para reparar todo el nodo de almacenamiento.

Este comando repara los datos replicados en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> A medida que se restauran los datos del objeto, la alerta de **Objetos perdidos** se activa si el sistema StorageGRID no puede localizar los datos de objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Debe determinar la causa de la pérdida y si es posible la recuperación. Consulte "Investigar los objetos perdidos".

Datos con código de borrado (EC)

Si el grid contiene datos con código de borrado, utilice `repair-data start-ec-node-repair` con el `--nodes` opción, donde `--nodes` Es el nombre de host (nombre del sistema), para reparar todo el nodo de almacenamiento.

Este comando repara los datos codificados con borrado en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

La operación devuelve un valor exclusivo `repair ID` eso lo identifica `repair_data` funcionamiento. Utilice esto `repair ID` para realizar un seguimiento del progreso y el resultado de la `repair_data` funcionamiento. No se devuelve ningún otro comentario cuando finaliza el proceso de recuperación.

> Las reparaciones de datos codificados para borrado pueden comenzar con algunos nodos de almacenamiento sin conexión. La reparación se completará después de que todos los nodos estén disponibles.

Repare los datos si solo algunos volúmenes han fallado

Si solo se produjo un error en algunos de los volúmenes, repare los volúmenes afectados. Siga las instrucciones para **datos replicados**, **datos codificados con borrado (EC)**, o ambos, en función de si utiliza datos replicados, datos codificados con borrado (EC), o ambos.

Si todos los volúmenes presentan errores, vaya a. Repare los datos si todos los volúmenes presentan errores.

Introduzca los ID de volumen en hexadecimal. Por ejemplo: `0000` es el primer volumen y. `000F` es el volumen decimosexto. Puede especificar un volumen, un rango de volúmenes o varios volúmenes que no estén en una secuencia.

Todos los volúmenes deben estar en el mismo nodo de almacenamiento. Si necesita restaurar volúmenes para más de un nodo de almacenamiento, póngase en contacto con el soporte técnico.

Datos replicados

Si la cuadrícula contiene datos replicados, utilice `start-replicated-volume-repair` con el `--nodes` opción para identificar el nodo (dónde `--nodes` es el nombre de host del nodo). A continuación, agregue el `--volumes` o. `--volume-range` como se muestra en los siguientes ejemplos.

Single volume: Este comando restaura los datos replicados al volumen `0002` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Intervalo de volúmenes: Este comando restaura los datos replicados a todos los volúmenes del intervalo `0003` para `0009` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Varios volúmenes que no están en una secuencia: Este comando restaura los datos replicados a los volúmenes `0001`, `0005`, y. `0008` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> ⓘ A medida que se restauran los datos del objeto, la alerta de **Objetos perdidos** se activa si el sistema StorageGRID no puede localizar los datos de objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Tenga en cuenta la descripción de la alerta y las acciones recomendadas para determinar la causa de la pérdida y si la recuperación es posible.

Datos con código de borrado (EC)

Si el grid contiene datos con código de borrado, utilice `start-ec-volume-repair` con el `--nodes` opción para identificar el nodo (dónde `--nodes` es el nombre de host del nodo). A continuación, agregue el `--volumes` o. `--volume-range` como se muestra en los siguientes ejemplos.

Volumen único: Este comando restaura los datos codificados por borrado al volumen `0007` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Intervalo de volúmenes: Este comando restaura los datos codificados por borrado a todos los volúmenes del intervalo `0004` para `0006` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Múltiples volúmenes no en una secuencia: Este comando restaura datos codificados por borrado a volúmenes `000A`, `000C`, y. `000E` En un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

La `repair-data` la operación devuelve un valor exclusivo `repair ID` eso lo identifica `repair_data` funcionamiento. Utilice esto `repair ID` para realizar un seguimiento del progreso y el resultado de la `repair_data` funcionamiento. No se devuelve ningún otro comentario cuando finaliza el proceso de

recuperación.

> Las reparaciones de datos codificados para borrado pueden comenzar con algunos nodos de almacenamiento sin conexión. La reparación se completará después de que todos los nodos estén disponibles.

Reparaciones del monitor

Supervise el estado de los trabajos de reparación, en función de si utiliza **datos replicados**, **datos codificados por borrado (EC)** o ambos.

También es posible supervisar el estado de los trabajos de restauración de volúmenes en curso y ver un historial de los trabajos de restauración completados en "Administrador de grid".

Datos replicados

- Para obtener un porcentaje de finalización estimado para la reparación replicada, agregue el `show-replicated-repair-status` opción del comando repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Para determinar si las reparaciones están completas:
  a. Seleccione **NODES** > ***Storage Node que se está reparando*** > **ILM**.
  b. Revise los atributos en la sección Evaluación. Una vez completadas las reparaciones, el atributo **esperando - todo** indica 0 objetos.
- Para supervisar la reparación con más detalle:
  a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
  b. Seleccione ***grid*** > ***nodo de almacenamiento que se está reparando*** > **LDR** > **almacén de datos**.
  c. Utilice una combinación de los siguientes atributos para determinar, como sea posible, si las reparaciones replicadas se han completado.

  > Puede haber incoherencias en Cassandra y no se realiza un seguimiento de las reparaciones fallidas.

  - **Reparaciones intentadas (XRPA)**: Utilice este atributo para realizar un seguimiento del progreso de las reparaciones replicadas. Este atributo aumenta cada vez que un nodo de almacenamiento intenta reparar un objeto de alto riesgo. Cuando este atributo no aumenta durante un período más largo que el período de exploración actual (proporcionado por el atributo **período de exploración — estimado**), significa que el análisis de ILM no encontró objetos de alto riesgo que necesitan ser reparados en ningún nodo.

    > Los objetos de alto riesgo son objetos que corren el riesgo de perderse por completo. Esto no incluye objetos que no cumplen con la configuración de ILM.

  - **Período de exploración — estimado (XSCM)**: Utilice este atributo para estimar cuándo se aplicará un cambio de directiva a objetos ingeridos previamente. Si el atributo **reparos intentados** no aumenta durante un período más largo que el período de adquisición actual, es probable que se realicen reparaciones replicadas. Tenga en cuenta que el período de adquisición puede cambiar. El atributo **período de exploración — estimado (XSCM)** se aplica a toda la cuadrícula y es el máximo de todos los periodos de exploración de nodos. Puede consultar el historial de atributos **período de exploración — Estimated** de la cuadrícula para determinar un intervalo de tiempo adecuado.

Datos con código de borrado (EC)

Para supervisar la reparación de datos codificados mediante borrado y vuelva a intentar cualquier solicitud que pudiera haber fallado:

1. Determine el estado de las reparaciones de datos codificadas por borrado:
   - Seleccione **SUPPORT** > **Tools** > **Metrics** para ver el tiempo estimado hasta la finalización y el porcentaje de finalización del trabajo actual. A continuación, seleccione **EC Overview** en la sección Grafana. Consulte los paneles **tiempo estimado de trabajo de Grid EC hasta finalización** y **Porcentaje de trabajo de Grid EC completado**.

- Utilice este comando para ver el estado de un elemento específico `repair-data` operación:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilice este comando para enumerar todas las reparaciones:

  ```
  repair-data show-ec-repair-status
  ```

El resultado muestra información, como `repair ID`, para todas las reparaciones que se estén ejecutando anteriormente y actualmente.

2. Si el resultado muestra que la operación de reparación ha dado error, utilice el `--repair-id` opción de volver a intentar la reparación.

   Este comando vuelve a intentar una reparación de nodo con fallos mediante el ID de reparación 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Este comando reintenta realizar una reparación de volumen con fallos mediante el ID de reparación 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Compruebe el estado de almacenamiento después de recuperar la unidad del sistema del nodo de almacenamiento

Después de recuperar la unidad del sistema para un nodo de almacenamiento, debe comprobar que el estado deseado del nodo de almacenamiento se establece en línea y que el estado estará en línea de forma predeterminada cada vez que se reinicie el servidor del nodo de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- El nodo de almacenamiento se ha recuperado y se completó la recuperación de datos.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Compruebe los valores de **Nodo de almacenamiento recuperado** > **LDR** > **Almacenamiento** > **Estado de almacenamiento — deseado** y **Estado de almacenamiento — actual**.

   El valor de ambos atributos debe ser en línea.

3. Si el estado de almacenamiento — deseado está establecido en sólo lectura, realice los siguientes pasos:
   a. Haga clic en la ficha **Configuración**.
   b. En la lista desplegable **Estado de almacenamiento — deseado**, seleccione **Online**.
   c. Haga clic en **aplicar cambios**.
   d. Haga clic en la ficha **Descripción general** y confirme que los valores de **Estado de almacenamiento — deseado** y **Estado de almacenamiento — actual** se actualizan a Online.

Restaurar datos de objetos con Grid Manager

Puede restaurar los datos de objetos para un volumen de almacenamiento con errores o un nodo de almacenamiento mediante Grid Manager. También puede utilizar Grid Manager para supervisar los procesos de restauración en curso y mostrar un historial de restauración.

Antes de empezar

- Completó cualquiera de estos procedimientos para formatear los volúmenes con errores:
  - "Volver a montar y volver a formatear los volúmenes de almacenamiento de los dispositivos (pasos manuales)"
  - "Volver a montar y volver a formatear los volúmenes de almacenamiento (pasos manuales)"
- Ha confirmado que el nodo de almacenamiento en el que está restaurando objetos tiene un estado de conexión de **Connected** En la ficha **NODES** > **Descripción general** de Grid Manager.
- Ha confirmado lo siguiente:
  - No hay una expansión de grid para agregar un nodo de almacenamiento en curso.
  - La retirada de nodo de almacenamiento no está en curso o no tiene errores.
  - No está en curso la recuperación de un volumen de almacenamiento con fallos.
  - No hay una recuperación de un nodo de almacenamiento con una unidad del sistema con fallos en curso.
  - No hay un trabajo de nuevo equilibrio de CE en curso.
  - La clonación de nodos del dispositivo no está en curso.

Acerca de esta tarea

Después de reemplazar las unidades y realizar los pasos manuales para formatear los volúmenes, Grid Manager muestra los volúmenes como candidatos para la restauración en la pestaña **MANTENIMIENTO** > **Restauración de volumen** > **Nodos para restaurar**.

Siempre que sea posible, restaure los datos de objetos con la página de restauración de volúmenes de Grid Manager. Puede hacer lo siguiente active el modo de restauración automática para iniciar automáticamente la restauración de volúmenes cuando los volúmenes estén listos para restaurarse o. realizar la restauración de volúmenes manualmente. Siga estas directrices:

- Si los volúmenes se enumeran en **MANTENIMIENTO** > **Restauración de volumen** > **Nodos a restaurar**, restaure los datos del objeto como se describe en los siguientes pasos. Se enumerará los volúmenes si:
  - Se produjo un error en algunos volúmenes de almacenamiento de un nodo, pero no en todos
  - Todos los volúmenes de almacenamiento de un nodo tienen errores y se reemplazan por la misma cantidad de volúmenes o más volúmenes

  La página de restauración de volumen en Grid Manager también le permite supervise el proceso de restauración de volúmenes y.. ver el historial de restauración.
- Si los volúmenes no aparecen en Grid Manager como candidatos para la restauración, siga los pasos que correspondan para usar el `repair-data` script para restaurar datos de objeto:
  - "Restauración de datos de objeto en un volumen de almacenamiento (fallo de unidad de sistema)"
  - "Restaure los datos de objetos al volumen de almacenamiento donde la unidad del sistema esté

intacta"

- "Restaure datos de objetos al volumen de almacenamiento de dispositivo"

> El script repair-data está obsoleto y se eliminará en una versión futura.

Si el nodo de almacenamiento recuperado contiene menos volúmenes que el nodo en el que sustituye, debe utilizar el `repair-data` guión.

Es posible restaurar dos tipos de datos de objetos:

- Los objetos de datos replicados se restauran desde otras ubicaciones, suponiendo que las reglas de ILM del grid se configuraron para que haya copias de objetos disponibles.
  - Si se configuró una regla de ILM para almacenar una sola copia replicada y esa copia estaba en un volumen de almacenamiento que falló, no podrá recuperar el objeto.
  - Si la única copia restante de un objeto se encuentra en un Cloud Storage Pool, StorageGRID debe emitir varias solicitudes al extremo Cloud Storage Pool para restaurar datos de objetos.
  - Si la única copia restante de un objeto se encuentra en un nodo de archivado, los datos de objeto se recuperan del nodo de archivado. Restaurar datos de objetos a un nodo de almacenamiento a partir de un nodo de archivado tarda más que restaurar copias de objetos desde otros nodos de almacenamiento.
- Los objetos de datos con código de borrado (EC) se restauran reensamblando los fragmentos almacenados. El algoritmo de código de borrado vuelve a crear los fragmentos dañados o perdidos a partir de los datos y fragmentos de paridad restantes.

  Las reparaciones de datos codificados para borrado pueden comenzar con algunos nodos de almacenamiento sin conexión. Sin embargo, si no se pueden tener en cuenta todos los datos con código de borrado, no se podrá completar la reparación. La reparación se completará después de que todos los nodos estén disponibles.

> La restauración de volúmenes depende de la disponibilidad de recursos donde se almacenan las copias de objetos. El progreso de la restauración de volúmenes no es lineal y puede tardar días o semanas en completarse.

Habilite el modo de restauración automática

Cuando se habilita el modo de restauración automática, la restauración de volúmenes se inicia automáticamente cuando los volúmenes están listos para restaurarse.

Pasos

1. En Grid Manager, vaya a **MANTENIMIENTO** > **Restauración de volumen**.
2. Seleccione la pestaña **Nodos a restaurar**, luego deslice el interruptor para **Modo de restauración automática** a la posición habilitada.
3. Cuando aparezca el cuadro de diálogo de confirmación, revise los detalles.

- No podrá iniciar manualmente trabajos de restauración de volúmenes en ningún nodo.
- Las restauraciones de volumen se iniciarán automáticamente solo cuando no haya otros procedimientos de mantenimiento en curso.
- Puede supervisar el estado del trabajo desde la página de supervisión de progreso.
- StorageGRID reintenta automáticamente restauraciones de volumen que no se inician.

4. Cuando comprenda los resultados de habilitar el modo de restauración automática, seleccione **Sí** en el cuadro de diálogo de confirmación.

   Puede desactivar el modo de restauración automática en cualquier momento.

Restaurar manualmente el nodo o el volumen fallido

Siga estos pasos para restaurar un nodo o volumen con errores.

Pasos

1. En Grid Manager, vaya a **MANTENIMIENTO** > **Restauración de volumen**.
2. Seleccione la pestaña **Nodos a restaurar**, luego deslice el interruptor para **Modo de restauración automática** a la posición desactivada.

   El número de la pestaña indica la cantidad de nodos con volúmenes que requieren restaurar.

3. Expanda cada nodo para ver los volúmenes que necesita restauración y su estado.
4. Corrija los problemas que impidan la restauración de cada volumen. Los problemas se indicarán al seleccionar **Esperando pasos manuales**, si se muestra como el estado del volumen.
5. Seleccione un nodo para restaurar donde todos los volúmenes indican el estado Listo para restaurar.

   Solo es posible restaurar los volúmenes de un nodo a la vez.

   Cada volumen del nodo debe indicar que está listo para restaurar.

6. Seleccione **Iniciar restauración**.
7. Aborda cualquier advertencia que pueda aparecer o selecciona **Iniciar de todos modos** para ignorar las advertencias e iniciar la restauración.

Los nodos se mueven de la pestaña **Nodes to restore** a la pestaña **Restoration Progress** cuando comienza la restauración.

Si no se puede iniciar una restauración de volumen, el nodo vuelve a la pestaña **Nodes to restore**.

Ver progreso de restauración

La pestaña **Progreso de la restauración** muestra el estado del proceso de restauración del volumen y la información sobre los volúmenes de un nodo que se está restaurando.

Las tasas de reparación de datos para objetos replicados y con código de borrado en todos los volúmenes son medias que resumen todas las restauraciones en curso, incluidas las restauraciones iniciadas mediante el `repair-data` guión. También se indica el porcentaje de objetos en esos volúmenes que están intactos y no requieren restauración.

> La restauración de datos replicada depende de la disponibilidad de los recursos donde se almacenan las copias replicadas. El progreso de la restauración de datos replicados no es lineal y puede tardar días o semanas en completarse.

La sección Trabajos de restauración muestra información sobre restauraciones de volúmenes iniciadas desde Grid Manager.

- El número del encabezado de la sección Trabajos de restauración indica el número de volúmenes que se restauran o se ponen en cola para la restauración.
- En la tabla se muestra información sobre cada volumen del nodo que se está restaurando y su progreso.
  - El progreso de cada nodo muestra el porcentaje de cada trabajo.
  - Expanda la columna Detalles para mostrar la hora de inicio de la restauración y el ID del trabajo.
- Si falla la restauración de un volumen:
  - La columna Estado indica `failed (attempting retry)`, y se reintentará automáticamente.
  - Si han fallado varios trabajos de restauración, el trabajo más reciente se volverá a intentar automáticamente en primer lugar.
  - La alerta **EC repair failure** se activa si los reintentos continúan fallando. Siga los pasos de la alerta para resolver el problema.

Ver historial de restauración

La pestaña **Historial de restauración** muestra información sobre todas las restauraciones de volumen que se han completado con éxito.

> Los tamaños no son aplicables para los objetos replicados y solo aparecen para las restauraciones que contienen objetos de datos con código de borrado (EC).

Supervisar trabajos de datos de reparación

Puede supervisar el estado de los trabajos de reparación mediante el `repair-data` script desde la línea de comandos.

Entre ellos se incluyen trabajos iniciados manualmente o trabajos que StorageGRID inició automáticamente como parte de un procedimiento de retirada.

> Si ejecuta trabajos de restauración de volúmenes, "Supervise el progreso y vea un historial de esos trabajos en Grid Manager" en su lugar.

Supervise el estado de `repair-data` Trabajos basados en si usa **datos replicados**, **datos codificados por borrado (EC)**, o ambos.

Datos replicados

- Para obtener un porcentaje de finalización estimado para la reparación replicada, agregue el `show-replicated-repair-status` opción del comando repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Para determinar si las reparaciones están completas:
  a. Seleccione **NODES** > ***Storage Node que se está reparando*** > **ILM**.
  b. Revise los atributos en la sección Evaluación. Una vez completadas las reparaciones, el atributo **esperando - todo** indica 0 objetos.
- Para supervisar la reparación con más detalle:
  a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
  b. Seleccione ***grid*** > ***nodo de almacenamiento que se está reparando*** > **LDR** > **almacén de datos**.
  c. Utilice una combinación de los siguientes atributos para determinar, como sea posible, si las reparaciones replicadas se han completado.

  > Puede haber incoherencias en Cassandra y no se realiza un seguimiento de las reparaciones fallidas.

  - **Reparaciones intentadas (XRPA)**: Utilice este atributo para realizar un seguimiento del progreso de las reparaciones replicadas. Este atributo aumenta cada vez que un nodo de almacenamiento intenta reparar un objeto de alto riesgo. Cuando este atributo no aumenta durante un período más largo que el período de exploración actual (proporcionado por el atributo **período de exploración — estimado**), significa que el análisis de ILM no encontró objetos de alto riesgo que necesitan ser reparados en ningún nodo.

    > Los objetos de alto riesgo son objetos que corren el riesgo de perderse por completo. Esto no incluye objetos que no cumplen con la configuración de ILM.

  - **Período de exploración — estimado (XSCM)**: Utilice este atributo para estimar cuándo se aplicará un cambio de directiva a objetos ingeridos previamente. Si el atributo **reparos intentados** no aumenta durante un período más largo que el período de adquisición actual, es probable que se realicen reparaciones replicadas. Tenga en cuenta que el período de adquisición puede cambiar. El atributo **período de exploración — estimado (XSCM)** se aplica a toda la cuadrícula y es el máximo de todos los periodos de exploración de nodos. Puede consultar el historial de atributos **período de exploración — Estimated** de la cuadrícula para determinar un intervalo de tiempo adecuado.

Datos con código de borrado (EC)

Para supervisar la reparación de datos codificados mediante borrado y vuelva a intentar cualquier solicitud que pudiera haber fallado:

1. Determine el estado de las reparaciones de datos codificadas por borrado:
   - Seleccione **SUPPORT** > **Tools** > **Metrics** para ver el tiempo estimado hasta la finalización y el porcentaje de finalización del trabajo actual. A continuación, seleccione **EC Overview** en la sección Grafana. Consulte los paneles **tiempo estimado de trabajo de Grid EC hasta finalización** y **Porcentaje de trabajo de Grid EC completado**.

- Utilice este comando para ver el estado de un elemento específico `repair-data` operación:

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilice este comando para enumerar todas las reparaciones:

  ```
  repair-data show-ec-repair-status
  ```

El resultado muestra información, como `repair ID`, para todas las reparaciones que se estén ejecutando anteriormente y actualmente.

2. Si el resultado muestra que la operación de reparación ha dado error, utilice el `--repair-id` opción de volver a intentar la reparación.

   Este comando vuelve a intentar una reparación de nodo con fallos mediante el ID de reparación 6949309319275667690:

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Este comando reintenta realizar una reparación de volumen con fallos mediante el ID de reparación 6949309319275667690:

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Recupere desde fallos de nodo de administrador

Recuperación de fallos de nodo de administración: Flujo de trabajo

El proceso de recuperación de un nodo de administrador depende de si se trata del nodo de administrador principal o del nodo de administrador que no es primario.

Los pasos de alto nivel para recuperar un nodo de administración primario o no primario son los mismos, aunque los detalles de los pasos son distintos.

Siga siempre el procedimiento de recuperación correcto para el nodo de administrador que se va a recuperar. Los procedimientos tienen el mismo aspecto en un nivel alto, pero difieren en los detalles.

Opciones

- "Recupere desde fallos del nodo de administrador principal"
- "Recupere el sistema de fallos de nodos de administrador que no son primarios"

Recupere desde fallos del nodo de administrador principal

Recuperación de fallos de nodo de administración principal: Descripción general

Debe completar un conjunto específico de tareas para recuperar el sistema después de un fallo en un nodo de administrador principal. El nodo de administrador principal aloja el servicio Configuration Management Node (CMN) de la cuadrícula.

Un nodo de administrador principal con fallos se debe reemplazar inmediatamente. El servicio nodo de gestión

de configuración (CMN) del nodo de administración principal es responsable de emitir bloques de identificadores de objetos para la cuadrícula. Estos identificadores se asignan a los objetos a medida que se ingieren. No se pueden ingerir nuevos objetos a menos que haya identificadores disponibles. La ingesta de objetos puede continuar mientras el CMN no está disponible porque el suministro de identificadores de aproximadamente un mes se almacena en caché en la cuadrícula. Sin embargo, después de que se agoten los identificadores almacenados en caché, no es posible añadir objetos nuevos.

> Debe reparar o sustituir un nodo de administrador principal con fallos dentro de un mes aproximadamente, o bien el grid podría perder su capacidad de procesar objetos nuevos. El período de tiempo exacto depende de la tasa de ingesta de objetos: Si necesita una evaluación más precisa del plazo para el grid, póngase en contacto con el soporte técnico.

Copie los registros de auditoría del nodo de administración principal con errores

Si puede copiar registros de auditoría del nodo de administración principal con errores, debe conservarlos para mantener el registro de la cuadrícula de la actividad y el uso del sistema. Es posible restaurar los registros de auditoría conservados al nodo administrador principal recuperado después de que esté activo y en ejecución.

Acerca de esta tarea

Este procedimiento copia los archivos de registro de auditoría del nodo de administración con errores en una ubicación temporal en un nodo de grid independiente. Estos registros de auditoría conservados se pueden copiar en el nodo admin de reemplazo. Los registros de auditoría no se copian automáticamente en el nuevo nodo de administración.

Según el tipo de error, es posible que no se puedan copiar los registros de auditoría de un nodo administrador con errores. Si la implementación solo tiene un nodo de administrador, el nodo de administrador recuperado inicia la grabación de eventos en el registro de auditoría en un nuevo archivo vacío y se pierden datos registrados previamente. Si la implementación incluye más de un nodo de administrador, puede recuperar los registros de auditoría desde otro nodo de administración.

> Si no se puede acceder a los registros de auditoría en el nodo de administración fallido ahora, es posible que pueda acceder a ellos más adelante, por ejemplo, después de la recuperación del host.

Pasos

1. Inicie sesión en el nodo de administrador con errores si es posible. De lo contrario, inicie sesión en el nodo de administración principal u otro nodo de administración, si está disponible.
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

2. Detenga el servicio AMS para evitar que cree un nuevo archivo de registro:`service ams stop`
3. Navegue al directorio de exportación de auditoría:

   ```
   cd /var/local/log
   ```

4. Cambie el nombre del origen `audit.log` archivo a un nombre de archivo numerado único. Por ejemplo, cambie el nombre del archivo audit.log a. `2023-10-25.txt.1`.

```
ls -l
mv audit.log 2023-10-25.txt.1
```

5. Reinicie el servicio AMS: `service ams start`
6. Cree el directorio para copiar todos los archivos de registro de auditoría a una ubicación temporal en un nodo de cuadrícula independiente: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Cuando se lo pida, introduzca la contraseña de administrador.

7. Copie todos los archivos de registro de auditoría en la ubicación temporal: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Cuando se lo pida, introduzca la contraseña de administrador.

8. Cerrar sesión como raíz: `exit`

Sustituya el nodo de administración principal

Para recuperar un nodo de administrador principal, primero es necesario reemplazar el hardware físico o virtual.

Puede reemplazar un nodo de administración principal con fallos por un nodo de administración principal que se ejecute en la misma plataforma, o bien puede reemplazar un nodo de administración principal que se ejecute en VMware o un host Linux por un nodo de administración principal alojado en un dispositivo de servicios.

Utilice el procedimiento que coincida con la plataforma de reemplazo seleccionada para el nodo. Una vez completado el procedimiento de sustitución de nodo (que es adecuado para todos los tipos de nodos), dicho procedimiento le dirigirá al siguiente paso para la recuperación del nodo de administración principal.

Plataforma de sustitución	Procedimiento
VMware	"Sustituya un nodo VMware"
Linux	"Sustituya un nodo Linux"
Servicios de aplicaciones SG100 y SG1000	"Sustituya un dispositivo de servicios"
OpenStack	Las operaciones de recuperación ya no son compatibles con los archivos de disco de máquinas virtuales y los scripts de OpenStack que proporciona NetApp. Si necesita recuperar un nodo que se ejecuta en una implementación de OpenStack, descargue los archivos para el sistema operativo Linux. A continuación, siga el procedimiento para "Reemplazar un nodo Linux".

Configure el nodo de administración principal de reemplazo

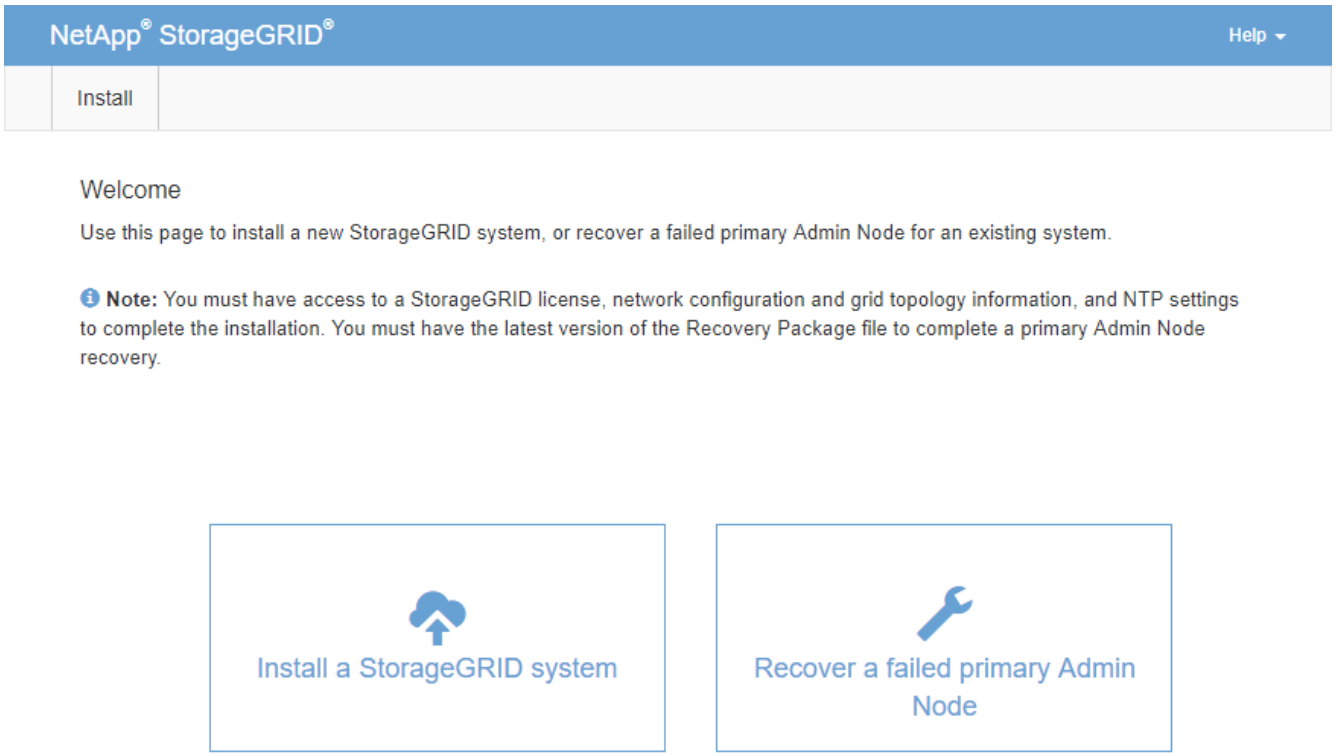
El nodo de reemplazo debe configurarse como nodo de administrador principal para el sistema StorageGRID.

Antes de empezar

- En el caso de los nodos de administración primarios alojados en máquinas virtuales, la máquina virtual se ha implementado, encendido e inicializado.
- En el caso de los nodos de administrador principales alojados en un dispositivo de servicios, ha sustituido el dispositivo y ha instalado software. Consulte "instrucciones de instalación del aparato".
- Tiene la última copia de seguridad del archivo Recovery Package (`sgws-recovery-package-id-revision.zip`).
- Tiene la clave de acceso de aprovisionamiento.

Pasos

1. Abra el explorador web y vaya a. `https://primary_admin_node_ip`.



2. Haga clic en **recuperar un nodo de administración principal con errores**.
3. Cargue la copia de seguridad más reciente del paquete de recuperación:
   a. Haga clic en **examinar**.
   b. Busque el archivo más reciente del paquete de recuperación para su sistema StorageGRID y haga clic en **Abrir**.
4. Introduzca la clave de acceso de aprovisionamiento.
5. Haga clic en **Iniciar recuperación**.

Se inicia el proceso de recuperación. Es posible que Grid Manager no esté disponible durante unos minutos a medida que se inician los servicios necesarios. Una vez finalizada la recuperación, se muestra la página de inicio de sesión.

6. Si el inicio de sesión único (SSO) está habilitado para el sistema StorageGRID y la confianza de la parte que confía para el nodo de administración que ha recuperado se configuró para utilizar el certificado de interfaz de gestión predeterminado, actualice (o elimine y vuelva a crear) la confianza de la parte que confía en el nodo en los Servicios de Federación de Active Directory (AD FS). Utilice el nuevo certificado de servidor predeterminado que se generó durante el proceso de recuperación del nodo de administración.

   > Para configurar una confianza de parte de confianza, consulte "Configurar el inicio de sesión único". Para acceder al certificado de servidor predeterminado, inicie sesión en el shell de comandos del nodo de administración. Vaya a la `/var/local/mgmt-api` y seleccione el `server.crt` archivo.

7. Determine si necesita aplicar una revisión.
   a. Inicie sesión en Grid Manager mediante una "navegador web compatible".
   b. Selecciona **NODOS**.
   c. En la lista de la izquierda, seleccione el nodo de administración principal.
   d. En la ficha Descripción general, observe la versión que aparece en el campo **Versión de software**.
   e. Seleccione cualquier otro nodo de grid.
   f. En la ficha Descripción general, observe la versión que aparece en el campo **Versión de software**.
      - Si las versiones que se muestran en los campos **Versión de software** son las mismas, no es necesario aplicar una revisión.
      - Si las versiones que se muestran en los campos **Versión de software** son diferentes, debe hacerlo "aplique una revisión" Para actualizar el nodo de administración principal recuperado a la misma versión.

Restaure el registro de auditoría en el nodo de administración principal recuperado

Si pudo conservar el registro de auditoría del nodo de administrador primario con errores, puede copiarlo al nodo de administrador principal que se está recuperando.

Antes de empezar

- El nodo de administración recuperado está instalado y en ejecución.
- Ha copiado los registros de auditoría en otra ubicación después de un error en el nodo de administración original.

Acerca de esta tarea

Si falla un nodo de administrador, los registros de auditoría guardados en ese nodo de administrador se perderán potencialmente. Es posible conservar los datos que no se perderán al copiar los registros de auditoría del nodo administrador con errores y luego restaurar estos registros de auditoría en el nodo de administrador recuperado. Según el error, es posible que no se puedan copiar los registros de auditoría del nodo administrador con errores. En ese caso, si la implementación tiene más de un nodo de administración, puede recuperar los registros de auditoría de otro nodo de administración a medida que se replican los registros de auditoría a todos los nodos de administrador.

Si solo hay un nodo de administración y el registro de auditoría no se puede copiar del nodo fallido, el nodo de

administración recuperado comienza a registrar eventos en el registro de auditoría como si la instalación fuera nueva.

Debe recuperar una Lo antes posible. de nodo de administrador para restaurar la funcionalidad de registro.

> De manera predeterminada, se envía la información de auditoría al registro de auditoría en los nodos admin. Puede omitir estos pasos si se aplica alguna de las siguientes situaciones:
>
> - Se configuraron un servidor de syslog externo y registros de auditoría ahora se envían al servidor de syslog en lugar de a los nodos de administrador.
> - Ha especificado explícitamente que los mensajes de auditoría se deben guardar sólo en los nodos locales que los han generado.
>
> Consulte "Configurar los mensajes de auditoría y los destinos de registro" para obtener más detalles.

Pasos

1. Inicie sesión en el nodo de administración recuperado:
   a. Introduzca el siguiente comando: `ssh admin@recovery_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Después de iniciar sesión como raíz, el símbolo del sistema cambia de `$` para `#`.
2. Compruebe qué archivos de auditoría se han conservado: `cd /var/local/log`
3. Copie los archivos de registro de auditoría conservados en el nodo admin recuperado: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   Cuando se lo pida, introduzca la contraseña de administrador.
4. Por motivos de seguridad, elimine los registros de auditoría del nodo de grid con errores después de verificar que se han copiado correctamente al nodo de administrador recuperado.
5. Actualice la configuración de usuario y grupo de los archivos de registro de auditoría en el nodo de administración recuperado: `chown ams-user: bycast *`
6. Cerrar sesión como raíz: `exit`

También debe restaurar cualquier acceso de cliente preexistente al recurso compartido de auditoría. Para obtener más información, consulte "Configure el acceso de los clientes de auditoría".

Restaure la base de datos del nodo de administrador al recuperar el nodo de administrador principal

Si desea conservar la información histórica sobre atributos, alarmas y alertas en un nodo de administración principal que tenga errores, puede restaurar la base de datos del nodo de administración. Solo puede restaurar esta base de datos si el sistema StorageGRID incluye otro nodo de administración.

Antes de empezar

- El nodo de administración recuperado está instalado y en ejecución.
- El sistema StorageGRID incluye al menos dos nodos de administración.
- Usted tiene la `Passwords.txt` archivo.
- Tiene la clave de acceso de aprovisionamiento.

Acerca de esta tarea

Si falla un nodo de administrador, se pierde la información histórica almacenada en su base de datos de nodos de administrador. Esta base de datos incluye la siguiente información:

- Historial de alertas
- Historial de alarmas
- Datos de atributos históricos, que se utilizan en los gráficos e informes de texto disponibles en la página **SUPPORT** > **Tools** > **Grid topology**.

Cuando se recupera un nodo de administrador, el proceso de instalación del software crea una base de datos vacía Admin Node en el nodo recuperado. Sin embargo, la nueva base de datos sólo incluye información sobre servidores y servicios que actualmente forman parte del sistema o que se agregan más adelante.

Si restauró un nodo de administrador principal y el sistema StorageGRID tiene otro nodo de administración, puede restaurar la información histórica copiando la base de datos del nodo de administración desde un nodo de administración no primario (el *Source Admin Node*) en el nodo de administración primario recuperado. Si el sistema sólo tiene un nodo de administración principal, no puede restaurar la base de datos del nodo de administración.

> La copia de la base de datos del nodo de administración puede llevar varias horas. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios se detengan en el nodo de administración de origen.

Pasos

1. Inicie sesión en el nodo de administrador de origen:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
2. Desde el nodo de administración de origen, detenga el servicio MI: `service mi stop`
3. En el nodo de administración de origen, detenga el servicio de la interfaz de programa de aplicaciones de gestión (API de gestión): `service mgmt-api stop`
4. Complete los siguientes pasos en el nodo de administración recuperado:
   a. Inicie sesión en el nodo de administración recuperado:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

b. Detenga EL servicio MI: `service mi stop`

c. Detenga el servicio API de gestión: `service mgmt-api stop`

d. Añada la clave privada SSH al agente SSH. Introduzca:`ssh-add`

e. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.

f. Copie la base de datos del nodo de administración de origen al nodo de administración recuperado: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. Cuando se le solicite, confirme que desea sobrescribir la base DE datos MI en el nodo de administración recuperado.

   La base de datos y sus datos históricos se copian en el nodo de administración recuperado. Una vez realizada la operación de copia, el script inicia el nodo de administración recuperado.

h. Cuando ya no necesite un acceso sin contraseñas a otros servidores, quite la clave privada del agente SSH. Introduzca:`ssh-add -D`

5. Reinicie los servicios en el nodo de administración de origen: `service servermanager start`

Restaurar las métricas de Prometheus al recuperar el nodo de administración principal

De manera opcional, puede conservar las métricas históricas que mantiene Prometheus en un nodo de administración principal que ha fallado. La métrica Prometheus solo se puede restaurar si su sistema StorageGRID incluye otro nodo de administración.

Antes de empezar

- El nodo de administración recuperado está instalado y en ejecución.
- El sistema StorageGRID incluye al menos dos nodos de administración.
- Usted tiene la `Passwords.txt` archivo.
- Tiene la clave de acceso de aprovisionamiento.

Acerca de esta tarea

Si falla un nodo de administración, se pierden las métricas que se mantienen en la base de datos Prometheus del nodo de administración. Cuando recupera el nodo de administración, el proceso de instalación del software crea una nueva base de datos Prometheus. Una vez iniciado el nodo de administración recuperado, este registra las métricas como si hubiera realizado una nueva instalación del sistema StorageGRID.

Si restauró un nodo de administración principal y el sistema StorageGRID tiene otro nodo de administración, puede restaurar las métricas históricas copiando la base de datos Prometheus desde un nodo de administración no primario (el *source Admin Node*) en el nodo de administración principal recuperado. Si el sistema solo tiene un nodo de administración principal, no puede restaurar la base de datos Prometheus.

> La copia de la base de datos Prometheus puede tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios se detengan en el nodo de administración de origen.

Pasos

1. Inicie sesión en el nodo de administrador de origen:

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

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

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

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

2. Desde el nodo de administración de origen, detenga el servicio Prometheus: `service prometheus stop`

3. Complete los siguientes pasos en el nodo de administración recuperado:

a. Inicie sesión en el nodo de administración recuperado:

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

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

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

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

b. Detenga el servicio Prometheus: `service prometheus stop`

c. Añada la clave privada SSH al agente SSH. Introduzca:`ssh-add`

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

e. Copie la base de datos Prometheus del nodo de administración de origen al nodo de administración recuperado: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Cuando se le solicite, pulse **Intro** para confirmar que desea destruir la nueva base de datos Prometheus del nodo de administración recuperado.

La base de datos Prometheus original y sus datos históricos se copian al nodo de administración recuperado. Una vez realizada la operación de copia, el script inicia el nodo de administración recuperado. Aparece el siguiente estado:

Base de datos clonada, servicios de inicio

a. Cuando ya no necesite un acceso sin contraseñas a otros servidores, quite la clave privada del agente SSH. Introduzca:`ssh-add -D`

4. Reinicie el servicio Prometheus en el nodo de administración de origen.`service prometheus start`

Recupere el sistema de fallos de nodos de administrador que no son primarios

Recuperación de fallos de nodos de administración no principales: Descripción general

Debe completar las siguientes tareas para recuperar el sistema de un fallo que no es del nodo de administrador principal. Un nodo de administrador aloja el servicio CMN (nodo de gestión de configuración) y se conoce como nodo de administración principal. Aunque puede tener varios nodos de administrador, cada sistema StorageGRID solo incluye un nodo de administrador primario. Todos los demás nodos de administrador son nodos de administrador no primarios.

Copie registros de auditoría del nodo administrador que no es principal con errores

Si puede copiar registros de auditoría del nodo administrador con errores, debe conservarlos para mantener el registro de la cuadrícula de actividad y uso del sistema. Es posible restaurar los registros de auditoría conservados en el nodo administrador no primario recuperado después de que esté activo y en ejecución.

Este procedimiento copia los archivos de registro de auditoría del nodo de administración con errores en una ubicación temporal en un nodo de grid independiente. Estos registros de auditoría conservados se pueden copiar en el nodo admin de reemplazo. Los registros de auditoría no se copian automáticamente en el nuevo nodo de administración.

Según el tipo de error, es posible que no se puedan copiar los registros de auditoría de un nodo administrador con errores. Si la implementación solo tiene un nodo de administrador, el nodo de administrador recuperado inicia la grabación de eventos en el registro de auditoría en un nuevo archivo vacío y se pierden datos registrados previamente. Si la implementación incluye más de un nodo de administrador, puede recuperar los registros de auditoría desde otro nodo de administración.

> Si no se puede acceder a los registros de auditoría en el nodo de administración fallido ahora, es posible que pueda acceder a ellos más adelante, por ejemplo, después de la recuperación del host.

1. Inicie sesión en el nodo de administrador con errores si es posible. De lo contrario, inicie sesión en el nodo de administración principal u otro nodo de administración, si está disponible.
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.
2. Detenga el servicio AMS para evitar que cree un nuevo archivo de registro:`service ams stop`
3. Navegue al directorio de exportación de auditoría:

   ```
   cd /var/local/log
   ```
4. Cambie el nombre del archivo audit.log de origen a un nombre de archivo numerado único. Por ejemplo, cambie el nombre del archivo audit.log a. `2023-10-25.txt.1`.

   ```
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```
5. Reinicie el servicio AMS: `service ams start`
6. Cree el directorio para copiar todos los archivos de registro de auditoría a una ubicación temporal en un nodo de cuadrícula independiente: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Cuando se lo pida, introduzca la contraseña de administrador.

7. Copie todos los archivos de registro de auditoría en la ubicación temporal: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Cuando se lo pida, introduzca la contraseña de administrador.

8. Cerrar sesión como raíz: `exit`

Sustituya el nodo de administrador que no es principal

Para recuperar un nodo de administrador que no sea el principal, en primer lugar debe reemplazar el hardware físico o virtual.

Puede reemplazar un nodo de administrador que no sea primario con fallos y un nodo de administrador que no sea primario y que se ejecute en la misma plataforma, o bien puede reemplazar un nodo de administrador que no sea primario que se ejecute en VMware o un host Linux por un nodo de administración no primario alojado en un dispositivo de servicios.

Utilice el procedimiento que coincida con la plataforma de reemplazo seleccionada para el nodo. Una vez completado el procedimiento de sustitución de nodos (que es adecuado para todos los tipos de nodos), dicho procedimiento le dirigirá al siguiente paso para la recuperación de nodos no primarios de administración.

Plataforma de sustitución	Procedimiento
VMware	"Sustituya un nodo VMware"
Linux	"Sustituya un nodo Linux"
Servicios de aplicaciones SG100 y SG1000	"Sustituya un dispositivo de servicios"
OpenStack	Las operaciones de recuperación ya no son compatibles con los archivos de disco de máquinas virtuales y los scripts de OpenStack que proporciona NetApp. Si necesita recuperar un nodo que se ejecuta en una implementación de OpenStack, descargue los archivos para el sistema operativo Linux. A continuación, siga el procedimiento para "Reemplazar un nodo Linux".

Seleccione Start Recovery para configurar el nodo de administrador que no es primario

Después de reemplazar un nodo de administración no primario, debe seleccionar Iniciar recuperación en el Administrador de grid para configurar el nuevo nodo como reemplazo del nodo con error.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento.

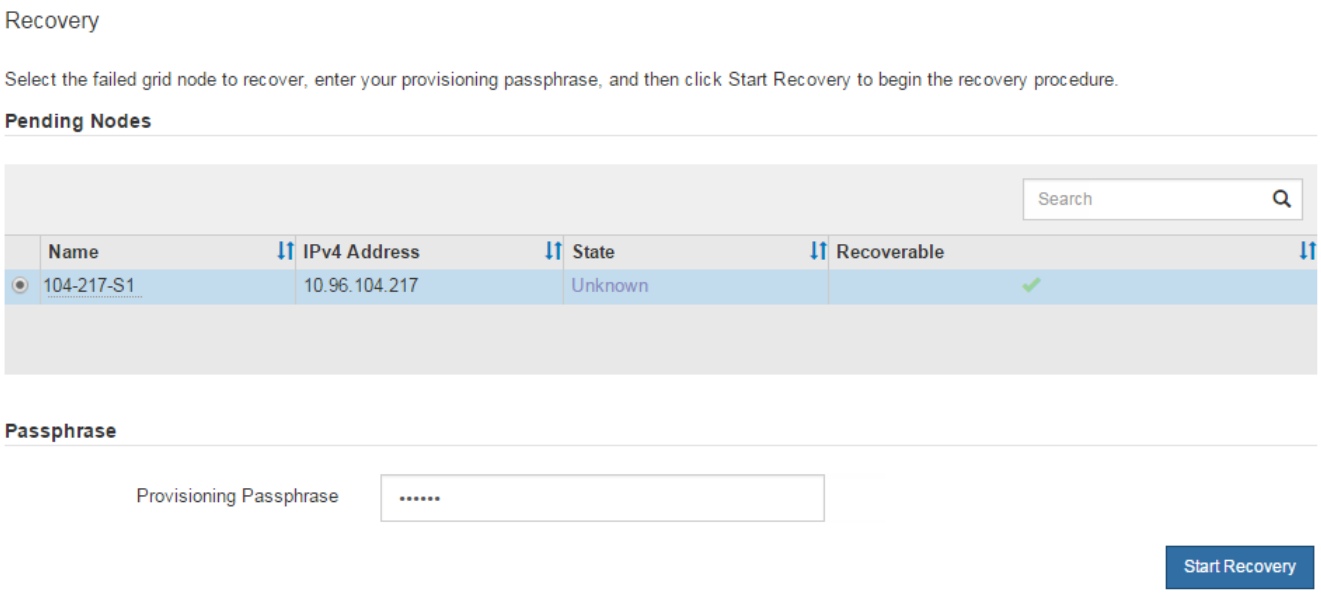
- Implementó y configuró el nodo de reemplazo.

Pasos

1. En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **recuperación**.
2. Seleccione el nodo de cuadrícula que desea recuperar en la lista Pending Nodes.

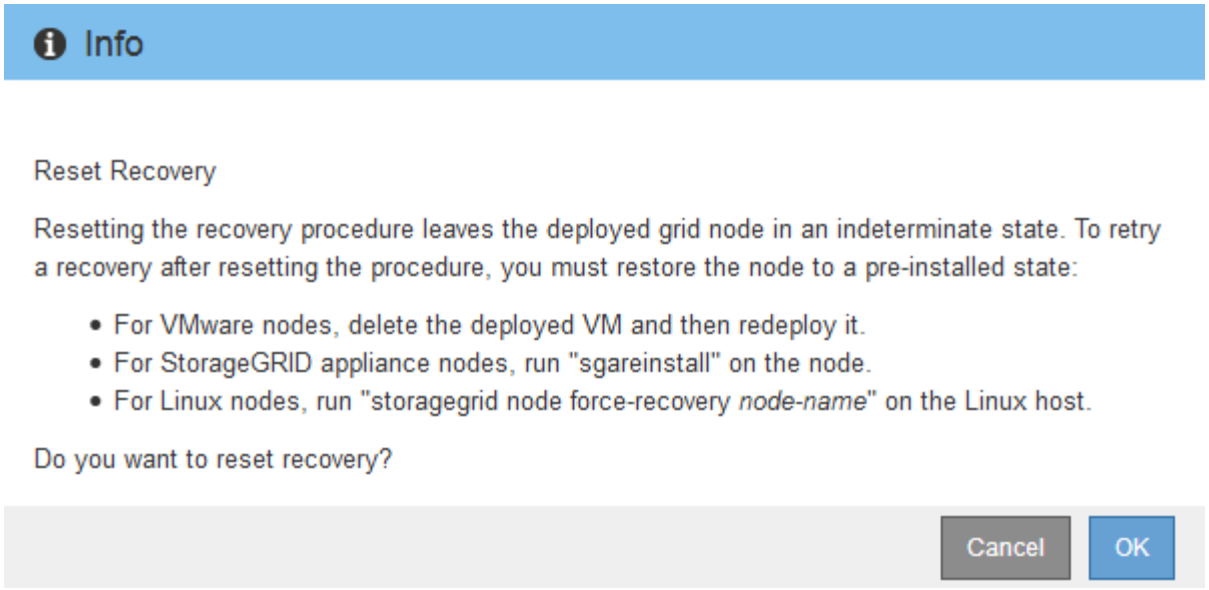
   Los nodos aparecen en la lista después de que fallan, pero no puede seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduzca la **frase de paso de aprovisionamiento**.
4. Haga clic en **Iniciar recuperación**.



5. Supervise el progreso de la recuperación en la tabla recuperando Grid Node.

> Mientras se está ejecutando el procedimiento de recuperación, puede hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparece un cuadro de diálogo que indica que el nodo quedará en un estado indeterminado si restablece el procedimiento.



Si desea volver a intentar la recuperación después de restablecer el procedimiento, debe restaurar el nodo a un estado preinstalado, de la manera siguiente:

- **VMware**: Elimine el nodo de la cuadrícula virtual desplegada. A continuación, una vez que esté listo para reiniciar la recuperación, vuelva a poner el nodo en marcha.
- **Linux**: Reinicie el nodo ejecutando este comando en el host Linux: `storagegrid node force-recovery node-name`
- **Dispositivo**: Si desea volver a intentar la recuperación después de reiniciar el procedimiento, debe restaurar el nodo del dispositivo a un estado preinstalado ejecutando `sgareinstall` en el nodo. Consulte "Preparar el aparato para su reinstalación (sólo sustitución de la plataforma)".

6. Si el inicio de sesión único (SSO) está habilitado para el sistema StorageGRID y la confianza de la parte que confía para el nodo de administración que ha recuperado se configuró para utilizar el certificado de interfaz de gestión predeterminado, actualice (o elimine y vuelva a crear) la confianza de la parte que confía en el nodo en los Servicios de Federación de Active Directory (AD FS). Utilice el nuevo certificado de servidor predeterminado que se generó durante el proceso de recuperación del nodo de administración.

> Para configurar una confianza de parte de confianza, consulte "Configurar el inicio de sesión único". Para acceder al certificado de servidor predeterminado, inicie sesión en el shell de comandos del nodo de administración. Vaya a la `/var/local/mgmt-api` y seleccione el `server.crt` archivo.

Restaure el registro de auditoría en el nodo de administración no primario recuperado

Si pudo conservar el registro de auditoría del nodo de administración no primario con errores, de manera que se conserve la información del registro de auditoría histórico, puede copiarla al nodo de administración no primario que se está recuperando.

Antes de empezar

- El nodo de administración recuperado está instalado y en ejecución.
- Ha copiado los registros de auditoría en otra ubicación después de un error en el nodo de administración original.

Acerca de esta tarea

Si falla un nodo de administrador, los registros de auditoría guardados en ese nodo de administrador se perderán potencialmente. Es posible conservar los datos que no se perderán al copiar los registros de auditoría del nodo administrador con errores y luego restaurar estos registros de auditoría en el nodo de administrador recuperado. Según el error, es posible que no se puedan copiar los registros de auditoría del nodo administrador con errores. En ese caso, si la implementación tiene más de un nodo de administración, puede recuperar los registros de auditoría de otro nodo de administración a medida que se replican los registros de auditoría a todos los nodos de administrador.

Si solo hay un nodo de administración y el registro de auditoría no se puede copiar del nodo fallido, el nodo de administración recuperado comienza a registrar eventos en el registro de auditoría como si la instalación fuera nueva.

Debe recuperar una Lo antes posible. de nodo de administrador para restaurar la funcionalidad de registro.

De manera predeterminada, se envía la información de auditoría al registro de auditoría en los nodos admin. Puede omitir estos pasos si se aplica alguna de las siguientes situaciones:

- Se configuraron un servidor de syslog externo y registros de auditoría ahora se envían al servidor de syslog en lugar de a los nodos de administrador.
- Ha especificado explícitamente que los mensajes de auditoría se deben guardar sólo en los nodos locales que los han generado.

Consulte "Configurar los mensajes de auditoría y los destinos de registro" para obtener más detalles.

Pasos

1. Inicie sesión en el nodo de administración recuperado:
   a. Introduzca el siguiente comando:

      ```
      ssh admin@recovery_Admin_Node_IP
      ```

   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

   Después de iniciar sesión como raíz, el símbolo del sistema cambia de `$` para `#`.

2. Compruebe qué archivos de auditoría se han conservado:

   ```
   cd /var/local/log
   ```

3. Copie los archivos de registro de auditoría conservados en el nodo admin recuperado:

   ```
   scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
   ```

   Cuando se lo pida, introduzca la contraseña de administrador.

4. Por motivos de seguridad, elimine los registros de auditoría del nodo de grid con errores después de verificar que se han copiado correctamente al nodo de administrador recuperado.
5. Actualice la configuración de usuario y grupo de los archivos de registro de auditoría en el nodo de

administración recuperado:

```
chown ams-user:bycast *
```

6. Cerrar sesión como raíz: `exit`

También debe restaurar cualquier acceso de cliente preexistente al recurso compartido de auditoría. Para obtener más información, consulte "Configure el acceso de los clientes de auditoría".

Restaure la base de datos del nodo de administrador al recuperar un nodo de administrador que no es primario

Si desea conservar la información histórica sobre atributos, alarmas y alertas en un nodo de administración que no sea primario con errores, puede restaurar la base de datos del nodo de administración desde el nodo de administración principal.

Antes de empezar

- El nodo de administración recuperado está instalado y en ejecución.
- El sistema StorageGRID incluye al menos dos nodos de administración.
- Usted tiene la `Passwords.txt` archivo.
- Tiene la clave de acceso de aprovisionamiento.

Acerca de esta tarea

Si falla un nodo de administrador, se pierde la información histórica almacenada en su base de datos de nodos de administrador. Esta base de datos incluye la siguiente información:

- Historial de alertas
- Historial de alarmas
- Datos de atributos históricos, que se utilizan en los gráficos e informes de texto disponibles en la página **SUPPORT** > **Tools** > **Grid topology**.

Cuando se recupera un nodo de administrador, el proceso de instalación del software crea una base de datos vacía Admin Node en el nodo recuperado. Sin embargo, la nueva base de datos sólo incluye información sobre servidores y servicios que actualmente forman parte del sistema o que se agregan más adelante.

Si restauró un nodo de administración no primario, puede restaurar la información histórica copiando la base de datos del nodo de administración principal (el *Source Admin Node*) en el nodo recuperado.

> La copia de la base de datos del nodo de administración puede llevar varias horas. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios estén detenidos en el nodo de origen.

Pasos

1. Inicie sesión en el nodo de administrador de origen:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

2. Ejecute el siguiente comando desde el nodo de administrador de origen. A continuación, introduzca la clave de acceso de aprovisionamiento si se le solicita. `recover-access-points`
3. Desde el nodo de administración de origen, detenga el servicio MI: `service mi stop`
4. En el nodo de administración de origen, detenga el servicio de la interfaz de programa de aplicaciones de gestión (API de gestión): `service mgmt-api stop`
5. Complete los siguientes pasos en el nodo de administración recuperado:
   a. Inicie sesión en el nodo de administración recuperado:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   b. Detenga EL servicio MI: `service mi stop`
   c. Detenga el servicio API de gestión: `service mgmt-api stop`
   d. Añada la clave privada SSH al agente SSH. Introduzca:`ssh-add`
   e. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.
   f. Copie la base de datos del nodo de administración de origen al nodo de administración recuperado: `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Cuando se le solicite, confirme que desea sobrescribir la base DE datos MI en el nodo de administración recuperado.

      La base de datos y sus datos históricos se copian en el nodo de administración recuperado. Una vez realizada la operación de copia, el script inicia el nodo de administración recuperado.

   h. Cuando ya no necesite un acceso sin contraseñas a otros servidores, quite la clave privada del agente SSH. Introduzca:`ssh-add -D`
6. Reinicie los servicios en el nodo de administración de origen: `service servermanager start`

Restaure las métricas de Prometheus al recuperar un nodo de administración que no sea primario

De manera opcional, puede conservar las métricas históricas que mantiene Prometheus en un nodo de administración no primario que haya fallado.

Antes de empezar

- El nodo de administración recuperado está instalado y en ejecución.
- El sistema StorageGRID incluye al menos dos nodos de administración.
- Usted tiene la `Passwords.txt` archivo.
- Tiene la clave de acceso de aprovisionamiento.

Acerca de esta tarea

Si falla un nodo de administración, se pierden las métricas que se mantienen en la base de datos Prometheus del nodo de administración. Cuando recupera el nodo de administración, el proceso de instalación del software crea una nueva base de datos Prometheus. Una vez iniciado el nodo de administración recuperado, este registra las métricas como si hubiera realizado una nueva instalación del sistema StorageGRID.

Si restauró un nodo de administración no primario, puede restaurar las métricas históricas copiando la base de datos Prometheus del nodo de administración principal (el *Source Admin Node*) en el nodo de administración recuperado.

> La copia de la base de datos Prometheus puede tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios se detengan en el nodo de administración de origen.

Pasos

1. Inicie sesión en el nodo de administrador de origen:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
2. Desde el nodo de administración de origen, detenga el servicio Prometheus: `service prometheus stop`
3. Complete los siguientes pasos en el nodo de administración recuperado:
   a. Inicie sesión en el nodo de administración recuperado:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   b. Detenga el servicio Prometheus: `service prometheus stop`
   c. Añada la clave privada SSH al agente SSH. Introduzca:`ssh-add`
   d. Introduzca la contraseña de acceso SSH que aparece en la `Passwords.txt` archivo.
   e. Copie la base de datos Prometheus del nodo de administración de origen al nodo de administración recuperado: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. Cuando se le solicite, pulse **Intro** para confirmar que desea destruir la nueva base de datos Prometheus del nodo de administración recuperado.

      La base de datos Prometheus original y sus datos históricos se copian al nodo de administración recuperado. Una vez realizada la operación de copia, el script inicia el nodo de administración recuperado. Aparece el siguiente estado:

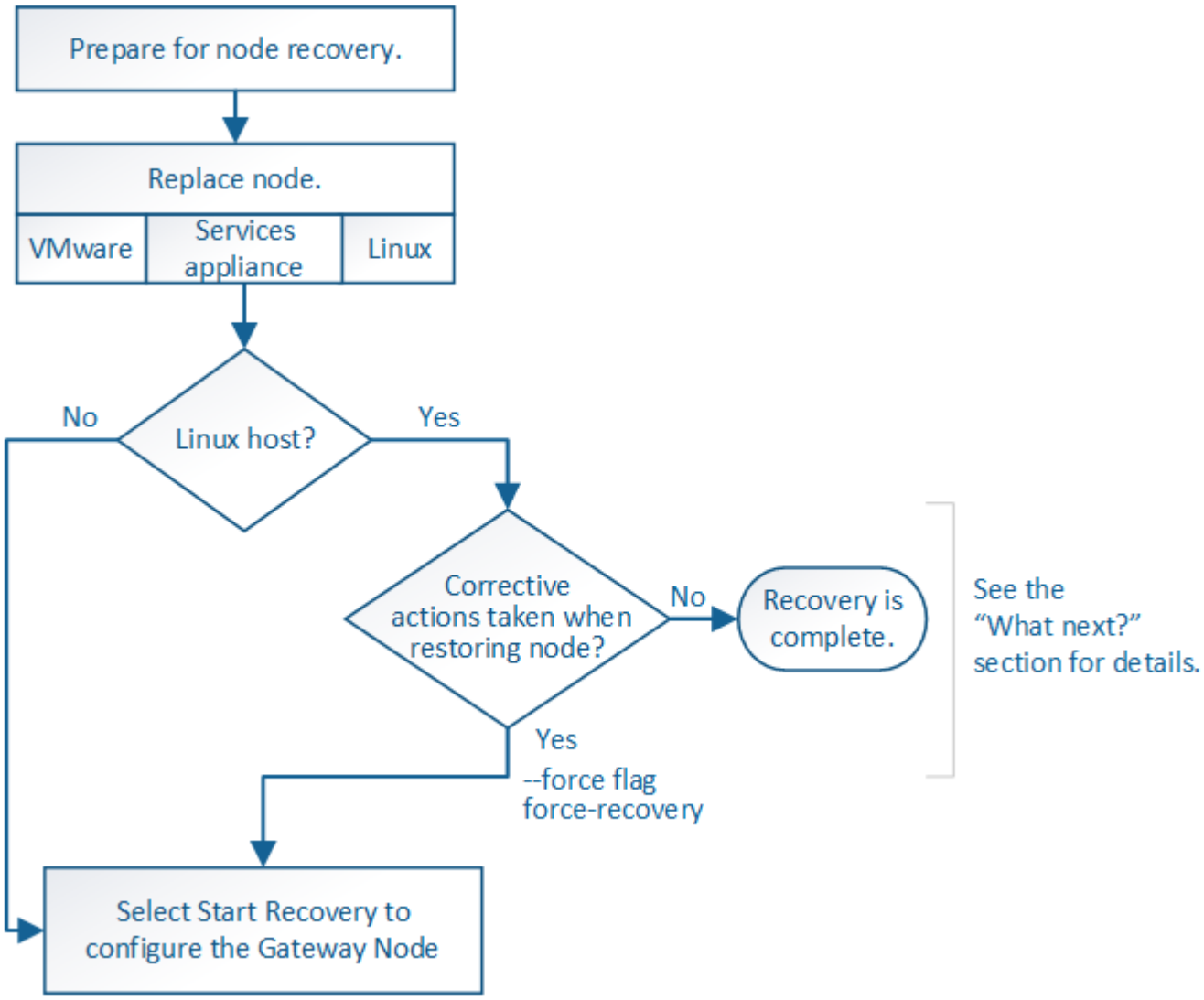
   Base de datos clonada, servicios de inicio

   a. Cuando ya no necesite un acceso sin contraseñas a otros servidores, quite la clave privada del agente SSH. Introduzca:`ssh-add -D`
4. Reinicie el servicio Prometheus en el nodo de administración de origen.`service prometheus start`

Recuperarse de fallos de nodo de puerta de enlace

Recuperación de Fallos de Nodos de Gateway: Flujo de trabajo

Debe completar una secuencia de tareas para poder recuperarlas de un fallo en el nodo de puerta de enlace.



Sustituya el nodo de puerta de enlace

Puede reemplazar un nodo de puerta de enlace con error por un nodo de puerta de enlace que se ejecute en el mismo hardware físico o virtual, o puede reemplazar un nodo de puerta de enlace que se ejecute en VMware o un host Linux por un nodo de puerta de enlace alojado en un dispositivo de servicios.

El procedimiento de sustitución de nodo que se debe seguir depende de la plataforma que utilice el nodo de reemplazo. Una vez completado el procedimiento de sustitución de nodo (que es adecuado para todos los tipos de nodos), dicho procedimiento le dirigirá al siguiente paso para la recuperación de nodos de puerta de enlace.

Plataforma de sustitución	Procedimiento
VMware	"Sustituya un nodo VMware"
Linux	"Sustituya un nodo Linux"
Servicios de aplicaciones SG100 y SG1000	"Sustituya un dispositivo de servicios"
OpenStack	Las operaciones de recuperación ya no son compatibles con los archivos de disco de máquinas virtuales y los scripts de OpenStack que proporciona NetApp. Si necesita recuperar un nodo que se ejecuta en una implementación de OpenStack, descargue los archivos para el sistema operativo Linux. A continuación, siga el procedimiento para "Reemplazar un nodo Linux".

Seleccione Start Recovery para configurar Gateway Node

Después de reemplazar un nodo de puerta de enlace, debe seleccionar Iniciar recuperación en el Administrador de grid para configurar el nuevo nodo como reemplazo del nodo con error.

Antes de empezar

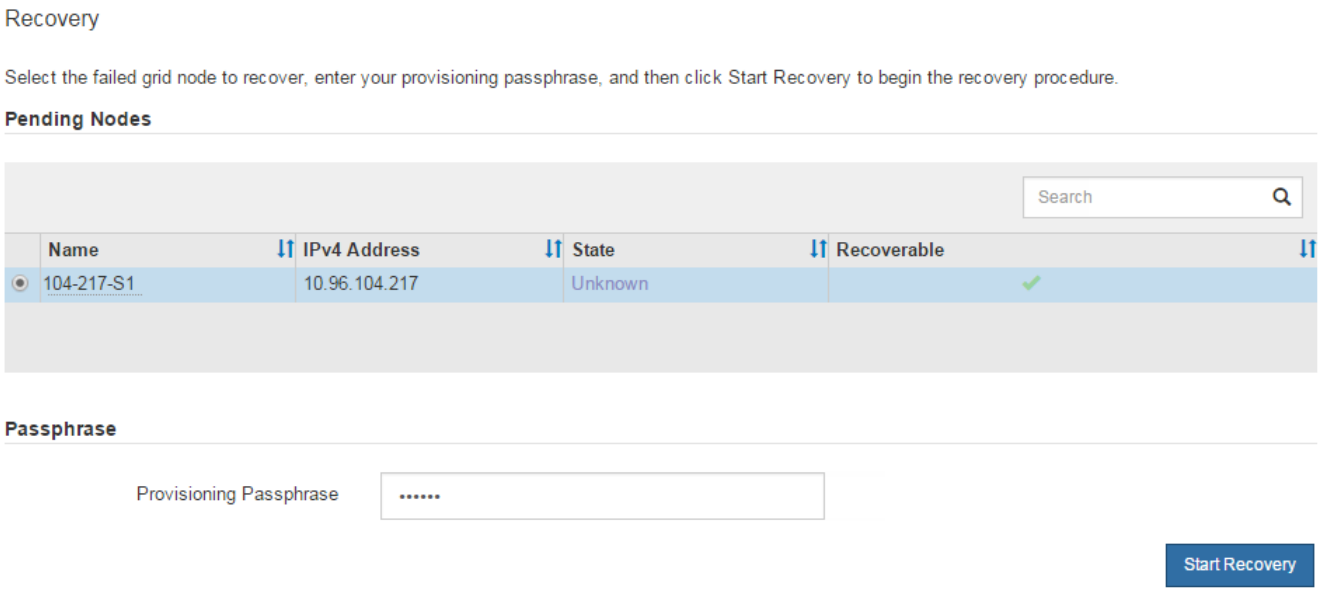
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento.
- Implementó y configuró el nodo de reemplazo.

Pasos

1. En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **recuperación**.
2. Seleccione el nodo de cuadrícula que desea recuperar en la lista Pending Nodes.

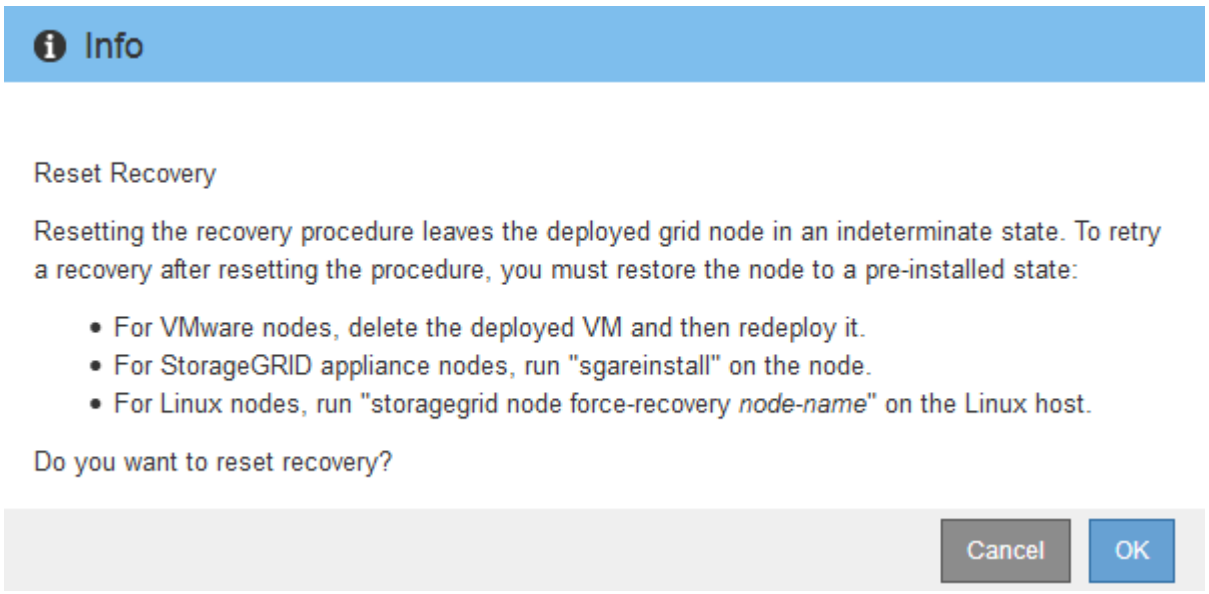
   Los nodos aparecen en la lista después de que fallan, pero no puede seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduzca la **frase de paso de aprovisionamiento**.
4. Haga clic en **Iniciar recuperación**.



5. Supervise el progreso de la recuperación en la tabla recuperando Grid Node.

> Mientras se está ejecutando el procedimiento de recuperación, puede hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparece un cuadro de diálogo que indica que el nodo quedará en un estado indeterminado si restablece el procedimiento.



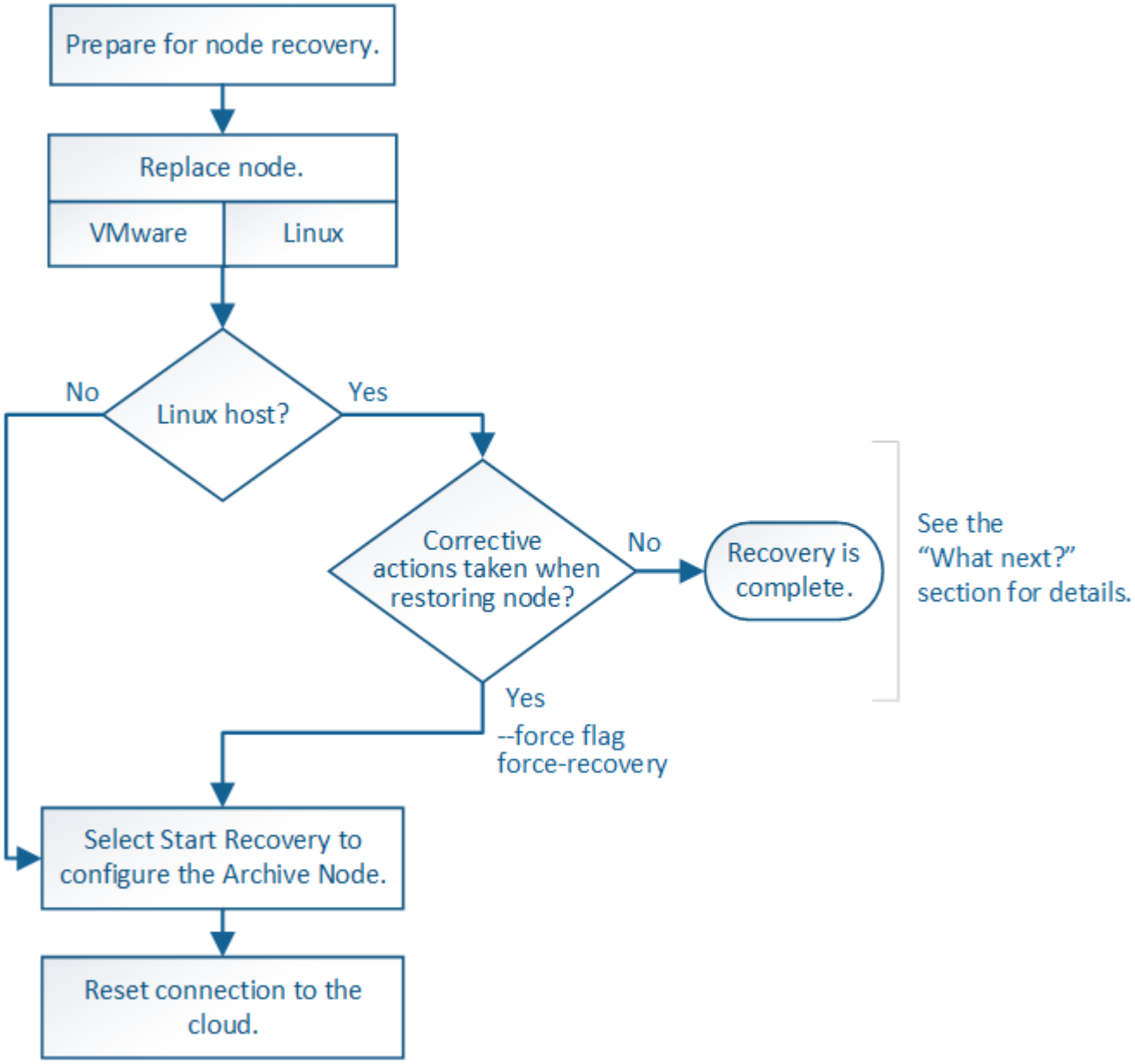
Si desea volver a intentar la recuperación después de restablecer el procedimiento, debe restaurar el nodo a un estado preinstalado, de la manera siguiente:

- **VMware**: Elimine el nodo de la cuadrícula virtual desplegada. A continuación, una vez que esté listo para reiniciar la recuperación, vuelva a poner el nodo en marcha.
- **Linux**: Reinicie el nodo ejecutando este comando en el host Linux: `storagegrid node force-recovery node-name`
- **Dispositivo**: Si desea volver a intentar la recuperación después de reiniciar el procedimiento, debe restaurar el nodo del dispositivo a un estado preinstalado ejecutando `sgareinstall` en el nodo. Consulte "Preparar el aparato para su reinstalación (sólo sustitución de la plataforma)".

Recupere desde errores de nodo de archivado

Recuperación de fallos de nodo de archivado: Flujo de trabajo

Debe completar una secuencia de tareas para poder recuperarlas de un fallo en el nodo de archivado.



La recuperación del nodo de archivado se ve afectada por los siguientes problemas:

- Si la política de ILM se configura para replicar una sola copia.

  En un sistema StorageGRID configurado para realizar una única copia de objetos, un error de nodo de archivado puede provocar una pérdida de datos irrecuperable. Si se produce un fallo, se pierden todos esos objetos; sin embargo, debe realizar procedimientos de recuperación para limpiar el sistema StorageGRID y depurar la información de objetos perdidos de la base de datos.

- Si se produce un fallo de un nodo de archivado durante la recuperación del nodo de almacenamiento.

Si el nodo de archivado falla al procesar recuperaciones masivas como parte de una recuperación de Storage Node, Debe repetir el procedimiento para recuperar copias de los datos del objeto en el nodo de almacenamiento desde el principio para garantizar que todos los datos del objeto recuperados del nodo de archivado se restauren en el nodo de almacenamiento.

Reemplace el nodo de archivado

Para recuperar un nodo de archivado, primero debe reemplazar el nodo.

Debe seleccionar el procedimiento de sustitución de nodo para su plataforma. Los pasos para reemplazar un nodo son los mismos para todos los tipos de nodos de grid.

Plataforma	Procedimiento
VMware	"Sustituya un nodo VMware"
Linux	"Sustituya un nodo Linux"
OpenStack	Las operaciones de recuperación ya no son compatibles con los archivos de disco de máquinas virtuales y los scripts de OpenStack que proporciona NetApp. Si necesita recuperar un nodo que se ejecuta en una implementación de OpenStack, descargue los archivos para el sistema operativo Linux. A continuación, siga el procedimiento para "Reemplazar un nodo Linux".

Seleccione Start Recovery para configurar Archive Node

Después de reemplazar un nodo de archivado, debe seleccionar Iniciar recuperación en el administrador de grid para configurar el nuevo nodo como reemplazo del nodo con error.

Antes de empezar

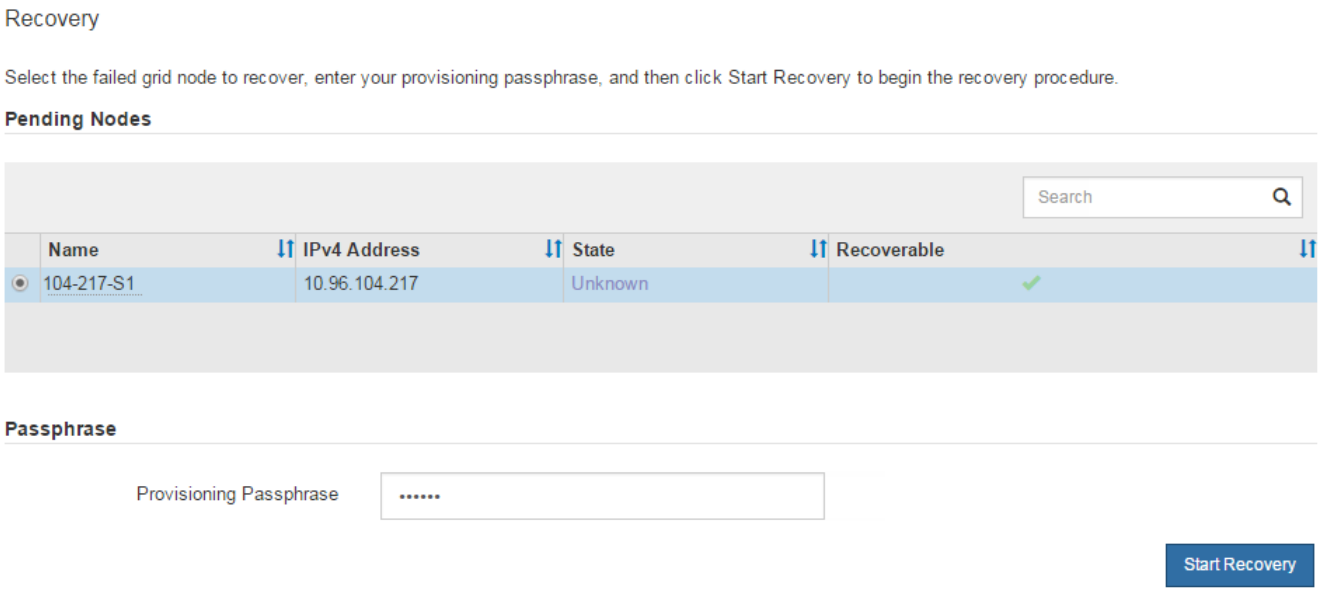
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Tiene la clave de acceso de aprovisionamiento.
- Implementó y configuró el nodo de reemplazo.

Pasos

1. En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **recuperación**.
2. Seleccione el nodo de cuadrícula que desea recuperar en la lista Pending Nodes.

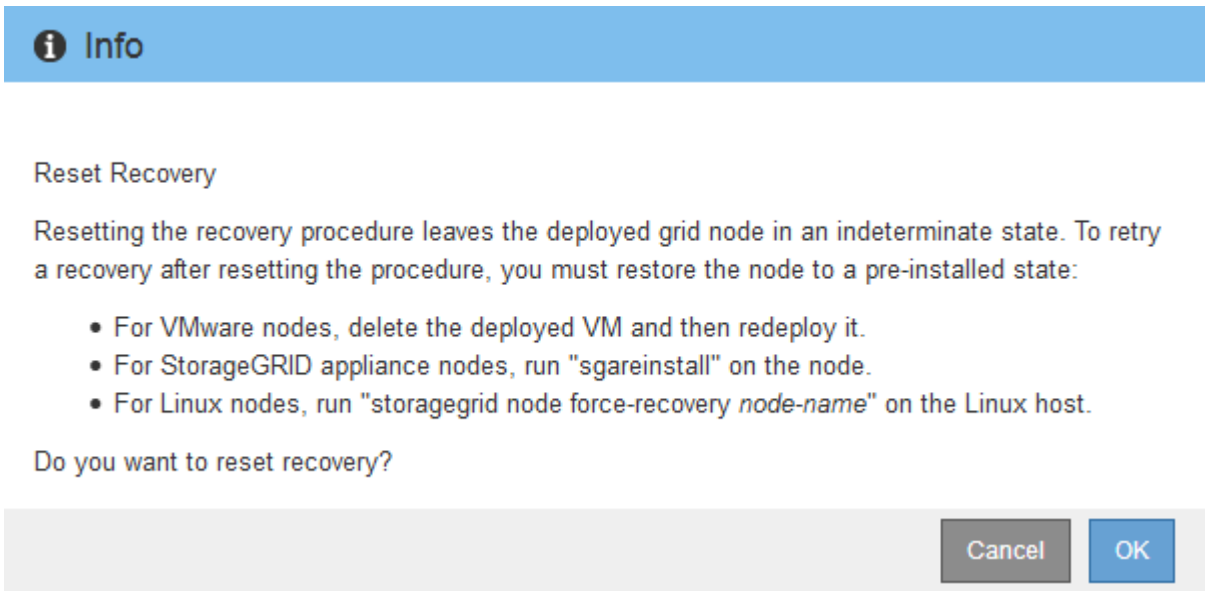
   Los nodos aparecen en la lista después de que fallan, pero no puede seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduzca la **frase de paso de aprovisionamiento**.
4. Haga clic en **Iniciar recuperación**.



5. Supervise el progreso de la recuperación en la tabla recuperando Grid Node.

> Mientras se está ejecutando el procedimiento de recuperación, puede hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparece un cuadro de diálogo que indica que el nodo quedará en un estado indeterminado si restablece el procedimiento.



Si desea volver a intentar la recuperación después de restablecer el procedimiento, debe restaurar el nodo a un estado preinstalado, de la manera siguiente:

- **VMware**: Elimine el nodo de la cuadrícula virtual desplegada. A continuación, una vez que esté listo para reiniciar la recuperación, vuelva a poner el nodo en marcha.
- **Linux**: Reinicie el nodo ejecutando este comando en el host Linux: `storagegrid node force-recovery node-name`

Restablezca la conexión de nodo de archivado con el cloud

Después de recuperar un nodo de archivado que se dirige al cloud a través de la API S3, debe modificar las opciones de configuración para restablecer las conexiones. Se activa una alarma Estado de replicación saliente (ORSU) si el nodo de archivado no puede recuperar datos de objeto.

> Si el nodo de archivado se conecta al almacenamiento externo a través del middleware TSM, el nodo se restablece automáticamente y no es necesario volver a configurarlo.

Antes de empezar

Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione **nodo de archivo** > **ARC** > **objetivo**.
3. Edite el campo **clave de acceso** introduciendo un valor incorrecto y haga clic en **aplicar cambios**.
4. Edite el campo **clave de acceso** introduciendo el valor correcto y haga clic en **aplicar cambios**.

Sustituya el nodo Linux

Sustituya el nodo Linux

Si un fallo requiere implementar uno o más hosts físicos o virtuales nuevos, o reinstalar Linux en un host existente, implemente y configure el host de reemplazo antes de poder recuperar el nodo de grid. Este procedimiento es un paso del proceso de recuperación de nodos de grid para todos los tipos de nodos de grid.

“Linux” se refiere a una implementación de Red Hat® Enterprise Linux®, Ubuntu® o Debian®. Para obtener una lista de las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp (IMT)".

Este procedimiento solo se realiza como un paso en el proceso de recuperación de nodos de almacenamiento basados en software, nodos de administración primarios o no primarios, nodos de puerta de enlace o nodos de archivado. Los pasos son idénticos independientemente del tipo de nodo de cuadrícula que se esté recuperando.

Si hay más de un nodo de grid alojado en un host físico o virtual Linux, es posible recuperar los nodos de grid en cualquier orden. Sin embargo, si se recupera primero un nodo de administración principal, si existe, impide que se cale el resto de nodos de grid, ya que intentan ponerse en contacto con el nodo de administración principal para registrarse para la recuperación.

Implemente nuevos hosts Linux

Salvo contadas excepciones, debe preparar los nuevos hosts como hizo durante el proceso de instalación inicial.

Para implementar hosts Linux físicos o virtuales nuevos o reinstalados, siga el procedimiento para preparar los hosts en las instrucciones de instalación de StorageGRID para el sistema operativo Linux:

- "Instalación de Linux (Red Hat Enterprise Linux)"
- "Instalar Linux (Ubuntu o Debian)"

Este procedimiento incluye los pasos necesarios para realizar las siguientes tareas:

1. Instale Linux.
2. Configure la red del host.
3. Configurar el almacenamiento del host.
4. Instale el motor del contenedor.
5. Instale el servicio de host StorageGRID.

> Deténgase después de completar la tarea de instalación del servicio host de StorageGRID en las instrucciones de instalación. No inicie la tarea de puesta en marcha de nodos de grid.

Cuando realice estos pasos, tenga en cuenta las siguientes directrices importantes:

- Asegúrese de usar los mismos nombres de interfaz de host que haya utilizado en el host original.
- Si utiliza almacenamiento compartido para admitir los nodos StorageGRID, o movió algunas o todas las unidades o SSD del nodo con error a los nodos de reemplazo, debe restablecer las mismas asignaciones de almacenamiento que se encontraban en el host original. Por ejemplo, si utilizó WWID y alias en `/etc/multipath.conf` Tal y como se recomienda en las instrucciones de instalación, asegúrese de utilizar las mismas parejas de alias/WWID en `/etc/multipath.conf` en el host de reemplazo.
- Si el nodo StorageGRID utiliza almacenamiento asignado de un sistema NetApp ONTAP, confirme que el volumen no tiene una política de organización en niveles de FabricPool habilitada. Al deshabilitar el almacenamiento en niveles de FabricPool para los volúmenes que se usan con los nodos StorageGRID, se simplifica la solución de problemas y las operaciones de almacenamiento.

> No utilice nunca FabricPool para colocar en niveles datos relacionados con StorageGRID en el propio StorageGRID. La organización en niveles de los datos de StorageGRID en StorageGRID aumenta la solución de problemas y la complejidad operativa.

Restaurar los nodos de grid en el host

Para restaurar un nodo de grid fallido en un nuevo host Linux, siga estos pasos para restaurar el archivo de configuración del nodo.

1. Restaure y valide el nodo mediante la restauración del archivo de configuración del nodo. Para una nueva instalación, cree un archivo de configuración de nodo para cada nodo de grid que se instalará en un host. Cuando restaura un nodo de grid en un host de reemplazo, restaura o sustituye el archivo de configuración de nodos en los nodos de grid con errores.
2. Inicie el servicio de host StorageGRID.
3. Según se necesite, recupere los nodos que no se inicien.

Si alguno de los volúmenes de almacenamiento en bloque se conservó del host anterior, es posible que deba realizar procedimientos de recuperación adicionales. Los comandos de esta sección le ayudan a determinar qué procedimientos adicionales son necesarios.

Restaurar y validar nodos de grid

Es necesario restaurar los archivos de configuración de grid para los nodos de grid con errores, a continuación, validar los archivos de configuración de grid y resolver los errores que se produzcan.

Acerca de esta tarea

Puede importar cualquier nodo de cuadrícula que deba estar presente en el host, siempre que lo esté `/var/local` no se perdió el volumen como resultado de un error del host anterior. Por ejemplo, la `/var/local` Es posible que el volumen siga existiendo si utilizó almacenamiento compartido para los volúmenes de datos del sistema StorageGRID, como se describe en las instrucciones de instalación de StorageGRID para el sistema operativo Linux. Al importar el nodo se restaura el archivo de configuración del nodo en el host.

Si no es posible importar los nodos que faltan, debe volver a crear sus archivos de configuración de cuadrícula.

A continuación, debe validar el archivo de configuración de grid y resolver cualquier problema de red o almacenamiento que pueda producirse antes de reiniciar StorageGRID. Cuando vuelva a crear el archivo de configuración para un nodo, debe usar el mismo nombre para el nodo de sustitución que se utilizó para el nodo que se está recuperando.

Consulte las instrucciones de instalación para obtener más información sobre la ubicación del `/var/local` volumen para un nodo.

- "Instalar StorageGRID en Red Hat Enterprise Linux"
- "Instalar StorageGRID en Ubuntu o Debian"

Pasos

1. En la línea de comandos del host recuperado, se muestran todos los nodos StorageGRID configurados actualmente:`sudo storagegrid node list`

   Si no se configura ningún nodo de cuadrícula, no se producirá ningún resultado. Si se configuran algunos nodos de grid, se debe esperar la salida con el siguiente formato:

   ```
   Name               Metadata-Volume
   ============================================================
   dc1-adm1           /dev/mapper/sgws-adm1-var-local
   dc1-gw1            /dev/mapper/sgws-gw1-var-local
   dc1-sn1            /dev/mapper/sgws-sn1-var-local
   dc1-arc1           /dev/mapper/sgws-arc1-var-local
   ```

   Si algunos o todos los nodos de cuadrícula que se deben configurar en el host no aparecen en la lista, debe restaurar los nodos de cuadrícula que faltan.

2. Para importar los nodos de cuadrícula que tienen un `/var/local` volumen:

   a. Ejecute el siguiente comando para cada nodo que desee importar:`sudo storagegrid node import node-var-local-volume-path`

      La `storagegrid node import` el comando solo se realiza correctamente si el nodo de destino se apaga correctamente en el host en el que se ejecutó por última vez. Si no es así, observará un error

similar al siguiente:

```
This node (node-name) appears to be owned by another host (UUID host-uuid).

Use the --force flag if you are sure import is safe.
```

a. Si ve el error sobre el nodo que pertenece a otro host, ejecute el comando de nuevo con el `--force` indicador para completar la importación:`sudo storagegrid --force node import node-var-local-volume-path`

> Todos los nodos importados con el `--force` esta opción requerirá pasos de recuperación adicionales antes de que puedan volver a unirse a la cuadrícula, tal y como se describe en "Lo siguiente: Si es necesario, realice pasos adicionales de recuperación".

3. Para los nodos de grid que no tienen un `/var/local` volume, vuelva a crear el archivo de configuración del nodo para restaurarlo al host. Para obtener instrucciones, consulte:
   - "Cree archivos de configuración de nodos para Red Hat Enterprise Linux"
   - "Crear archivos de configuración de nodos para Ubuntu o Debian"

> Cuando vuelva a crear el archivo de configuración para un nodo, debe usar el mismo nombre para el nodo de sustitución que se utilizó para el nodo que se está recuperando. En las implementaciones de Linux, asegúrese de que el nombre del archivo de configuración contenga el nombre del nodo. Se deben utilizar las mismas interfaces de red, asignaciones de dispositivos de bloque y direcciones IP cuando sea posible. Esta práctica minimiza la cantidad de datos que se debe copiar al nodo durante la recuperación, lo que puede hacer que la recuperación sea significativamente más rápida (en algunos casos, minutos en lugar de semanas).

> Si utiliza dispositivos de bloque nuevos (dispositivos que el nodo StorageGRID no utilizó anteriormente) como valores para cualquiera de las variables de configuración que comienzan por `BLOCK_DEVICE_` cuando vuelva a crear el archivo de configuración para un nodo, siga las directrices de Solucione los errores de dispositivo de bloque que faltan.

4. Ejecute el siguiente comando en el host recuperado para enumerar todos los nodos StorageGRID.

```
sudo storagegrid node list
```

5. Validar el archivo de configuración del nodo de cada nodo de cuadrícula cuyo nombre se muestra en el resultado de la lista de nodos StorageGRID:

```
sudo storagegrid node validate node-name
```

Debe solucionar cualquier error o advertencia antes de iniciar el servicio de host de StorageGRID. En las siguientes secciones se ofrecen más detalles sobre los errores que pueden tener un significado especial durante la recuperación.

Corrija los errores de interfaz de red que faltan

Si la red host no está configurada correctamente o se ha escrito un nombre de forma incorrecta, se produce un error cuando StorageGRID comprueba la asignación especificada en `/etc/storagegrid/nodes/node-`

name.conf archivo.

Es posible que aparezca un error o una advertencia que coincida con este patrón:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
       <node-name>: Interface <host-interface-name>' does not exist
```

Se puede informar del error en la red de cuadrícula, la red de administración o la red de cliente. Este error significa que /etc/storagegrid/nodes/*node-name*.conf El archivo asigna la red StorageGRID indicada a la interfaz del host llamada *host-interface-name*, pero no hay interfaz con ese nombre en el host actual.

Si recibe este error, compruebe que ha completado los pasos de "Implemente nuevos hosts Linux". Utilice los mismos nombres para todas las interfaces de host que se usaron en el host original.

Si no puede asignar un nombre a las interfaces del host para que coincidan con el archivo de configuración del nodo, puede editar el archivo de configuración del nodo y cambiar el valor DE GRID_NETWORK_TARGET, ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET para que coincida con una interfaz de host existente.

Asegúrese de que la interfaz del host proporciona acceso al puerto de red física o VLAN adecuados y que la interfaz no haga referencia directamente a un dispositivo de enlace o puente. Debe configurar una VLAN (u otra interfaz virtual) en la parte superior del dispositivo de enlace en el host o usar un puente y un par virtual Ethernet (veth).

Solucione los errores de dispositivo de bloque que faltan

El sistema comprueba que cada nodo recuperado se asigna a un archivo especial de dispositivo de bloque válido o a un archivo especial de dispositivo de bloque válido. Si StorageGRID encuentra una asignación no válida en /etc/storagegrid/nodes/*node-name*.conf archivo, aparece un error de dispositivo de bloque ausente.

Si observa un error que coincide con este patrón:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: BLOCK_DEVICE_PURPOSE = <path-name>
       <node-name>: <path-name> does not exist
```

Significa eso /etc/storagegrid/nodes/*node-name*.conf asigna el dispositivo de bloque utilizado por *node-name* para PURPOSE Para el nombre de ruta de acceso especificado en el sistema de archivos de Linux, pero no hay un archivo especial de dispositivo de bloque válido, o softlink a un archivo especial de dispositivo de bloque, en esa ubicación.

Compruebe que ha completado los pasos de la "Implemente nuevos hosts Linux". Utilice los mismos nombres de dispositivo persistentes para todos los dispositivos de bloque que se usaron en el host original.

Si no puede restaurar o volver a crear el archivo especial del dispositivo de bloque que falta, puede asignar un nuevo dispositivo de bloque con el tamaño y la categoría de almacenamiento adecuados y editar el archivo de

configuración del nodo para cambiar el valor de `BLOCK_DEVICE_PURPOSE` para apuntar al nuevo archivo especial del dispositivo de bloque.

Determine el tamaño y la categoría de almacenamiento adecuados mediante las tablas del sistema operativo Linux:

- "Requisitos de almacenamiento y rendimiento para Red Hat Enterprise Linux"
- "Requisitos de almacenamiento y rendimiento para Ubuntu o Debian"

Consulte las recomendaciones para configurar el almacenamiento del host antes de continuar con la sustitución del dispositivo de bloques:

- "Configurar el almacenamiento host para Red Hat Enterprise Linux"
- "Configurar el almacenamiento host para Ubuntu o Debian"

> Si debe proporcionar un nuevo dispositivo de almacenamiento en bloques para cualquiera de las variables del archivo de configuración que comiencen con `BLOCK_DEVICE_` debido a que el dispositivo de bloque original se perdió con el host con error, asegúrese de que el nuevo dispositivo de bloque no tiene formato antes de intentar realizar más procedimientos de recuperación. El nuevo dispositivo de bloques no formateará si utiliza almacenamiento compartido y ha creado un volumen nuevo. Si no está seguro, ejecute el siguiente comando en cualquier archivo especial nuevo del dispositivo de almacenamiento en bloques.

> Ejecute el siguiente comando solo para nuevos dispositivos de almacenamiento en bloques. No ejecute este comando si cree que el almacenamiento de bloques aún contiene datos válidos para el nodo que se está recuperando, ya que se perderán los datos del dispositivo.
>
> ```
> sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
> ```

Inicie el servicio de host StorageGRID

Para iniciar los nodos de StorageGRID y asegurarse de que reinicien después del reinicio de un host, debe habilitar e iniciar el servicio de host StorageGRID.

Pasos

1. Ejecute los siguientes comandos en cada host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Ejecute el siguiente comando para asegurarse de que se sigue la implementación:

```
sudo storagegrid node status node-name
```

3. Si alguno de los nodos devuelve el estado «Sin ejecución» o «Detenido», ejecute el siguiente comando:

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

4. Si anteriormente habilitó e inició el servicio de host de StorageGRID (o si no está seguro de si el servicio se ha habilitado e iniciado), también debe ejecutar el siguiente comando:

```
sudo systemctl reload-or-restart storagegrid
```

Recupere los nodos que no se inician normalmente

Si un nodo StorageGRID no se vuelve a unir al grid normalmente y no se muestra como recuperable, es posible que esté dañado. Puede forzar el nodo en el modo de recuperación.

Pasos

1. Confirme que la configuración de red del nodo es correcta.

   Es posible que el nodo no haya podido volver a unirse a la cuadrícula porque las asignaciones de interfaz de red son incorrectas o porque la pasarela o una dirección IP de red de grid no son correctas.

2. Si la configuración de red es correcta, emita el `force-recovery` comando:

   `sudo storagegrid node force-recovery` *`node-name`*

3. Realice los pasos de recuperación adicionales para el nodo. Consulte "Lo siguiente: Si es necesario, realice pasos adicionales de recuperación".

Lo siguiente: Si es necesario, lleve a cabo pasos adicionales de recuperación

Según las acciones específicas que haya tomado para ejecutar los nodos StorageGRID en el host de reemplazo, es posible que deba realizar otros pasos de recuperación para cada nodo.

La recuperación de nodos está completa si no necesitaba tomar ninguna acción correctiva mientras sustituyó el host Linux o restauró el nodo de la cuadrícula con errores en el nuevo host.

Acciones correctivas y pasos siguientes

Durante el reemplazo de nodo, es posible que haya que realizar una de las siguientes acciones correctivas:

- Tenía que usar el `--force` indicador para importar el nodo.
- Para cualquiera `<PURPOSE>`, el valor de `BLOCK_DEVICE_<PURPOSE>` la variable del archivo de configuración hace referencia a un dispositivo de bloque que no contiene los mismos datos que antes del fallo del host.
- Emitió la emisión `storagegrid node force-recovery` *`node-name`* para el nodo.
- Ha agregado un nuevo dispositivo de bloque.

Si ha tomado **cualquiera** de estas acciones correctivas, debe realizar pasos adicionales de recuperación.

Tipo de recuperación	Paso siguiente
Nodo de administrador principal	"Configure el nodo de administración principal de reemplazo"
Nodo de administrador no primario	"Seleccione Start Recovery para configurar el nodo de administrador que no es primario"
Nodo de puerta de enlace	"Seleccione Start Recovery para configurar Gateway Node"
Nodo de archivado	"Seleccione Start Recovery para configurar Archive Node"
Nodo de almacenamiento (basado en software): • Si tenía que usar el `--force` indicador para importar el nodo o ha emitido `storagegrid node force-recovery node-name` • Si tenía que volver a instalar un nodo completo o tenía que restaurar /var/local	"Seleccione Start Recovery para configurar Storage Node"
Nodo de almacenamiento (basado en software): • Si ha agregado un nuevo dispositivo de bloque. • Si, por cualquiera `<PURPOSE>`, el valor de `BLOCK_DEVICE_<PURPOSE>` la variable del archivo de configuración hace referencia a un dispositivo de bloque que no contiene los mismos datos que antes del fallo del host.	"Recupérese de un fallo en el volumen de almacenamiento, donde la unidad del sistema está intacta"

Sustituya el nodo VMware

Cuando se recupera un nodo StorageGRID con fallos que se encontraba en VMware, se elimina el nodo fallido y se implementa un nodo de recuperación.

Antes de empezar

Ha determinado que la máquina virtual no se puede restaurar y debe reemplazarse.

Acerca de esta tarea

Se utiliza VMware vSphere Web Client para quitar primero la máquina virtual asociada con el nodo de grid que ha fallado. A continuación, puede implementar una nueva máquina virtual.

Este procedimiento es solo un paso del proceso de recuperación del nodo de cuadrícula. El procedimiento de retirada y puesta en marcha de nodos es el mismo para todos los nodos de VMware, incluidos los nodos de administrador, nodos de almacenamiento, nodos de puerta de enlace y archivado.

Pasos

1. Inicie sesión en VMware vSphere Web Client.
2. Acceda a la máquina virtual del nodo de grid donde se ha producido el error.
3. Tome nota de toda la información necesaria para poner en marcha el nodo de recuperación.
   a. Haga clic con el botón derecho del ratón en la máquina virtual, seleccione la ficha **Editar configuración** y anote la configuración en uso.
   b. Seleccione la ficha **vApp Options** para ver y registrar la configuración de red del nodo de cuadrícula.
4. Si el nodo de almacenamiento Grid en el que se ha producido el fallo es un nodo de almacenamiento, determine si alguno de los discos duros virtuales utilizados para el almacenamiento de datos no está dañado y conservarlos para volver a conectarlos al nodo de grid recuperado.
5. Apague la máquina virtual.
6. Seleccione **Acciones** > **Todas las acciones de vCenter** > **Eliminar del disco** para eliminar la máquina virtual.
7. Implemente una máquina virtual nueva para que sea el nodo de reemplazo y conéctelo a una o más redes StorageGRID. Para ver instrucciones, consulte "Poner en marcha un nodo de StorageGRID como máquina virtual".

   Al poner en marcha el nodo, tiene la opción de reasignar puertos de nodo o aumentar las opciones de CPU o memoria.

   > Después de implementar el nuevo nodo, puede agregar nuevos discos virtuales de acuerdo con sus requisitos de almacenamiento, volver a conectar los discos duros virtuales conservados desde el nodo de cuadrícula con error que se quitó anteriormente, o ambos.

8. Complete el procedimiento de recuperación de nodos, según el tipo de nodo que se está recuperando.

Tipo de nodo	Vaya a.
Nodo de administrador principal	"Configure el nodo de administración principal de reemplazo"
Nodo de administrador no primario	"Seleccione Start Recovery para configurar el nodo de administrador que no es primario"
Nodo de puerta de enlace	"Seleccione Start Recovery para configurar Gateway Node"
Nodo de almacenamiento	"Seleccione Start Recovery para configurar Storage Node"
Nodo de archivado	"Seleccione Start Recovery para configurar Archive Node"

Sustituya el nodo con fallos por el dispositivo de servicios

Sustituya el nodo con fallos por el dispositivo de servicios: Información general

Puede utilizar un dispositivo de servicios SG100 o SG1000 para recuperar un nodo de puerta de enlace fallido, un nodo de administración no primario fallido o un nodo de administración principal fallido alojado en VMware, un host Linux o un dispositivo de

servicios. Este procedimiento es un paso del procedimiento de recuperación de nodos de cuadrícula.

Antes de empezar

- Ha determinado que una de las siguientes situaciones es verdadera:
  - No se puede restaurar la máquina virtual que aloja el nodo.
  - El host Linux físico o virtual del nodo de grid ha dado error y es necesario reemplazarlo.
  - Se debe sustituir el dispositivo de servicios que aloja el nodo Grid.
- Ha confirmado que la versión del instalador de dispositivos StorageGRID en el dispositivo de servicios coincide con la versión de software de su sistema StorageGRID. Consulte "Comprobar y actualizar la versión de StorageGRID Appliance Installer".

> No ponga en marcha un dispositivo de servicio SG100 y SG1000 en el mismo sitio. El rendimiento puede ser impredecible.

Acerca de esta tarea

Puede utilizar un dispositivo de servicios SG100 o SG1000 para recuperar un nodo de red fallido en los casos siguientes:

- El nodo fallido se hospedó en VMware o Linux ("cambio de plataforma")
- El nodo con errores se hospedó en un dispositivo de servicios ("sustitución de plataformas")

Instalar el dispositivo de servicios (sólo cambio de plataforma)

Cuando va a recuperar un nodo de grid fallido que estaba alojado en VMware o un host Linux y utiliza un dispositivo de servicios para el nodo de reemplazo, primero debe instalar el hardware del dispositivo nuevo con el mismo nombre de nodo (nombre del sistema) que el nodo que ha fallado.

Antes de empezar

Tiene la siguiente información sobre el nodo con errores:

- **Nombre de nodo**: Debe instalar el dispositivo de servicios con el mismo nombre de nodo que el nodo que ha fallado. El nombre del nodo es el nombre de host (nombre del sistema).
- **Direcciones IP**: Puede asignar el dispositivo de servicios las mismas direcciones IP que el nodo que ha fallado, que es la opción preferida, o puede seleccionar una nueva dirección IP no utilizada en cada red.

Acerca de esta tarea

Realice este procedimiento solo si va a recuperar un nodo con errores alojado en VMware o Linux y lo va a reemplazar por un nodo alojado en un dispositivo de servicios.

Pasos

1. Siga las instrucciones para instalar un nuevo dispositivo de servicios SG100 o SG1000. Consulte "Inicio rápido para la instalación de hardware".
2. Cuando se le solicite el nombre de un nodo, utilice el nombre del nodo con errores.

Preparar el aparato para su reinstalación (sólo sustitución de la plataforma)

Al recuperar un nodo de cuadrícula que se alojó en un dispositivo de servicios, primero debe preparar el dispositivo para la reinstalación del software StorageGRID.

Realice este procedimiento solo si va a reemplazar un nodo con errores alojado en un dispositivo de servicios. No siga estos pasos si el nodo que ha fallado estaba alojado originalmente en VMware o un host Linux.

Pasos

1. Inicie sesión en el nodo de la cuadrícula con errores:

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

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

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

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

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

2. Prepare el dispositivo para la instalación del software StorageGRID. Introduzca: `sgareinstall`

3. Cuando se le solicite continuar, introduzca: `y`

   El dispositivo se reinicia y la sesión SSH finaliza. Normalmente tarda unos 5 minutos en estar disponible el instalador de dispositivos de StorageGRID; aunque en algunos casos es posible que deba esperar hasta 30 minutos.

   El dispositivo de servicios se restablece y ya no se puede acceder a los datos en el nodo de grid. Las direcciones IP configuradas durante el proceso de instalación original deben permanecer intactas; sin embargo, se recomienda confirmarlo cuando finalice el procedimiento.

   Después de ejecutar el `sgareinstall` Comando, se eliminan todas las cuentas, contraseñas y claves SSH aprovisionados de StorageGRID, y se generan nuevas claves del host.

Inicie la instalación del software en el dispositivo de servicios

Para instalar un nodo de puerta de enlace o un nodo de administración en un dispositivo de servicios SG100 o SG1000, utilice el instalador de dispositivos StorageGRID, que se incluye en el dispositivo.

Antes de empezar

- El dispositivo se instala en un bastidor, se conecta a las redes y se enciende.
- Los enlaces de red y las direcciones IP se configuran para el dispositivo mediante el instalador de dispositivos de StorageGRID.
- Si va a instalar un nodo de puerta de enlace o un nodo de administrador que no sea primario, conoce la dirección IP del nodo de administrador principal de la cuadrícula de StorageGRID.
- Todas las subredes de red de grid enumeradas en la página Configuración de IP del instalador de dispositivos StorageGRID se definen en la lista de subredes de red de grid del nodo de administración principal.

  Consulte "Inicio rápido para la instalación de hardware".

- Está utilizando un "navegador web compatible".
- Tiene una de las direcciones IP asignadas al dispositivo. Puede utilizar la dirección IP para la red de administración, la red de red o la red de cliente.
- Si está instalando un nodo de administración principal, tiene disponibles los archivos de instalación de Ubuntu o Debian para esta versión de StorageGRID.

> Una versión reciente del software StorageGRID está precargada en el dispositivo de servicios durante la fabricación. Si la versión preinstalada del software coincide con la versión utilizada en la implementación de StorageGRID, no necesita los archivos de instalación.

Acerca de esta tarea

Para instalar el software StorageGRID en un dispositivo de servicios SG100 o SG1000:

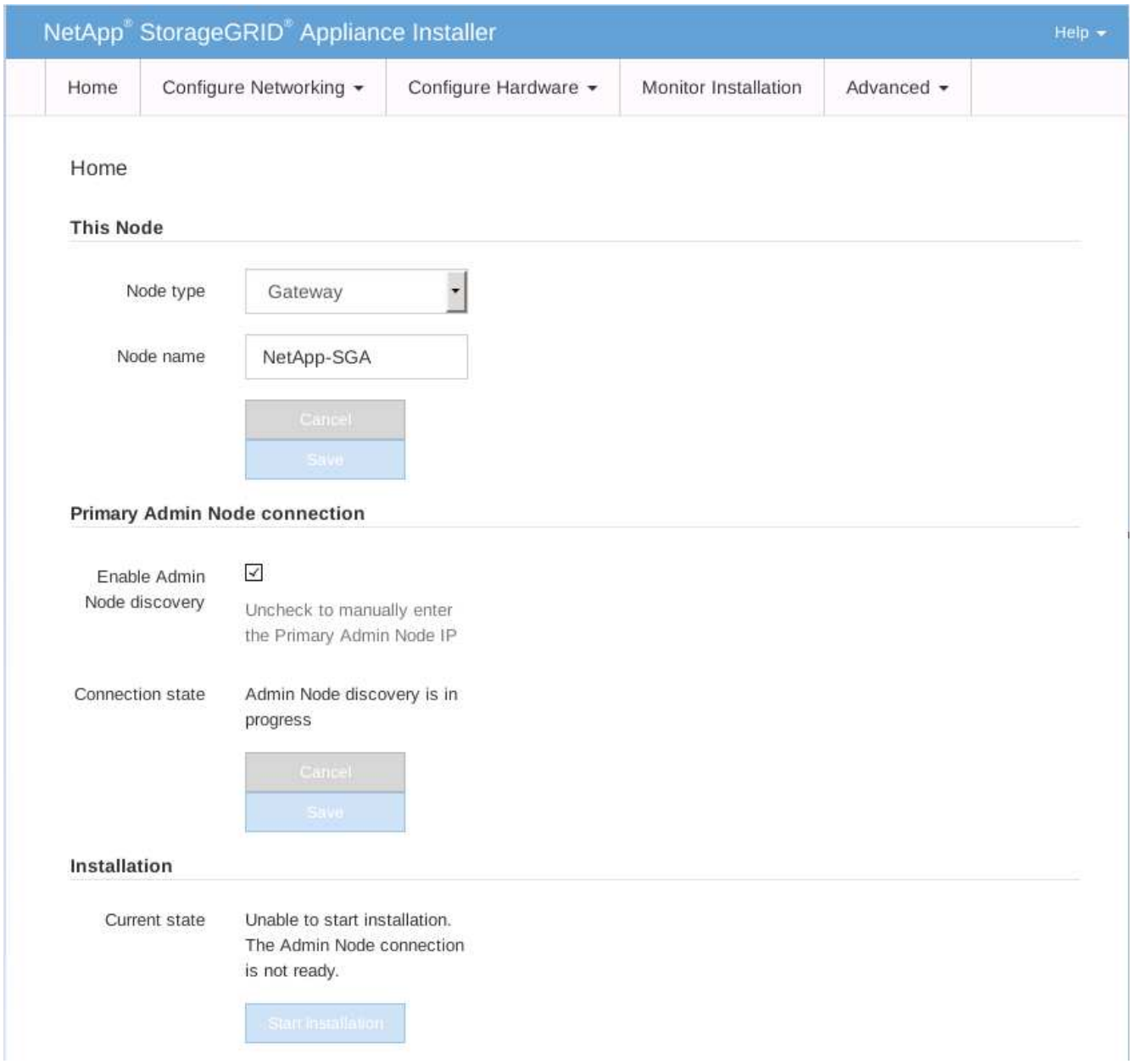
- Para un nodo de administración principal, debe especificar el nombre del nodo y luego cargar los paquetes de software adecuados (si es necesario).
- En el caso de un nodo de administrador que no sea primario o un nodo de puerta de enlace, debe especificar o confirmar la dirección IP del nodo de administración principal y el nombre del nodo.
- Inicia la instalación y espera a que los volúmenes estén configurados y el software esté instalado.
- Paso a través del proceso, la instalación se detiene. Para reanudar la instalación, debe iniciar sesión en Grid Manager y configurar el nodo pendiente como reemplazo del nodo que ha fallado.
- Una vez que haya configurado el nodo, se completa el proceso de instalación del dispositivo y el dispositivo se reinicia.

Pasos

1. Abra un explorador e introduzca una de las direcciones IP del dispositivo de servicios SG100 o SG1000.

   `https://Controller_IP:8443`

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.



2. Para instalar un nodo de administración principal:

   a. En la sección este nodo, para **Tipo de nodo**, seleccione **Administración primaria**.

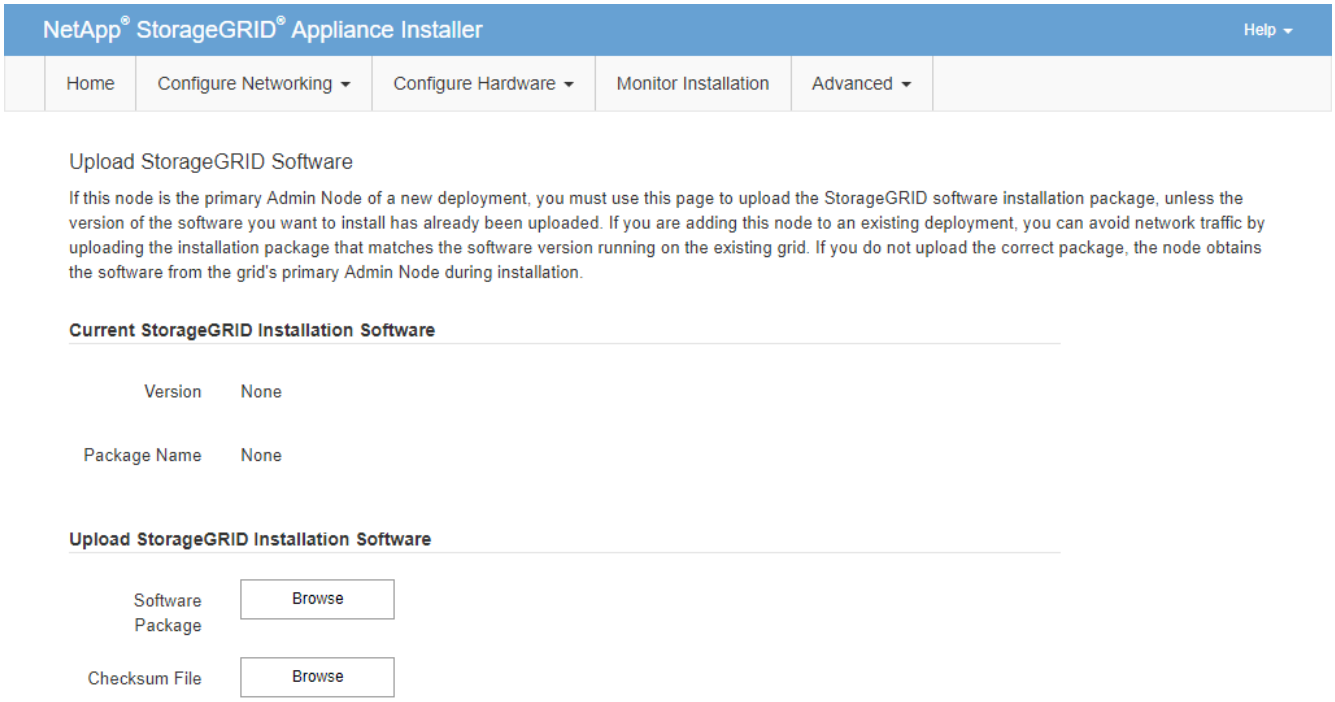
   b. En el campo **Nombre de nodo**, introduzca el mismo nombre que se utilizó para el nodo que está recuperando y haga clic en **Guardar**.

   c. En la sección instalación, compruebe la versión de software que aparece en el estado actual

      Si la versión del software que está lista para instalar es correcta, vaya a la Paso de la instalación.

   d. Si necesita cargar una versión de software diferente, en el menú **Avanzado**, seleccione **cargar software StorageGRID**.

      Aparecerá la página Upload StorageGRID Software (cargar software de).



a. Haga clic en **examinar** para cargar el software **paquete de software** y **Archivo de suma de comprobación** para StorageGRID.

   Los archivos se cargan de forma automática después de seleccionarlos.

b. Haga clic en **Inicio** para volver a la página de inicio del instalador de dispositivos StorageGRID.

3. Para instalar un nodo de puerta de enlace o un nodo de administración que no sea principal:

   a. En la sección este nodo, para **Tipo de nodo**, seleccione **Puerta de enlace** o **Administración no primaria**, según el tipo de nodo que esté restaurando.

   b. En el campo **Nombre de nodo**, introduzca el mismo nombre que se utilizó para el nodo que está recuperando y haga clic en **Guardar**.

   c. En la sección Conexión del nodo de administración principal, determine si necesita especificar la dirección IP para el nodo de administración principal.

      El instalador de dispositivos de StorageGRID puede detectar esta dirección IP automáticamente, suponiendo que el nodo de administración principal o, al menos, otro nodo de grid con ADMIN_IP configurado, esté presente en la misma subred.

   d. Si no se muestra esta dirección IP o es necesario modificarla, especifique la dirección:

Opción	Descripción
Entrada IP manual	a. Desactive la casilla de verificación **Enable Admin Node discovery**. b. Introduzca la dirección IP de forma manual. c. Haga clic en **Guardar**. d. Espere hasta que el estado de conexión de la nueva dirección IP esté listo.

Opción	Descripción
Detección automática de todos los nodos principales de administración conectados	a. Seleccione la casilla de verificación **Enable Admin Node discovery**. b. En la lista de direcciones IP detectadas, seleccione el nodo de administración principal para la cuadrícula en la que se va a implementar este dispositivo de servicios. c. Haga clic en **Guardar**. d. Espere hasta que el estado de conexión de la nueva dirección IP esté listo.

4. en la sección instalación, confirme que el estado actual está preparado para iniciar la instalación del nombre del nodo y que el botón **Start Installation** está activado.

   Si el botón **Iniciar instalación** no está activado, es posible que deba cambiar la configuración de red o la configuración del puerto. Para obtener instrucciones, consulte las instrucciones de mantenimiento de su aparato.

5. En la página de inicio del instalador de dispositivos StorageGRID, haga clic en **Iniciar instalación**.

   El estado actual cambia a «Instalación en curso» y se muestra la página de instalación del monitor.

   > Si necesita acceder a la página de instalación del monitor manualmente, haga clic en **instalación del monitor** en la barra de menús.

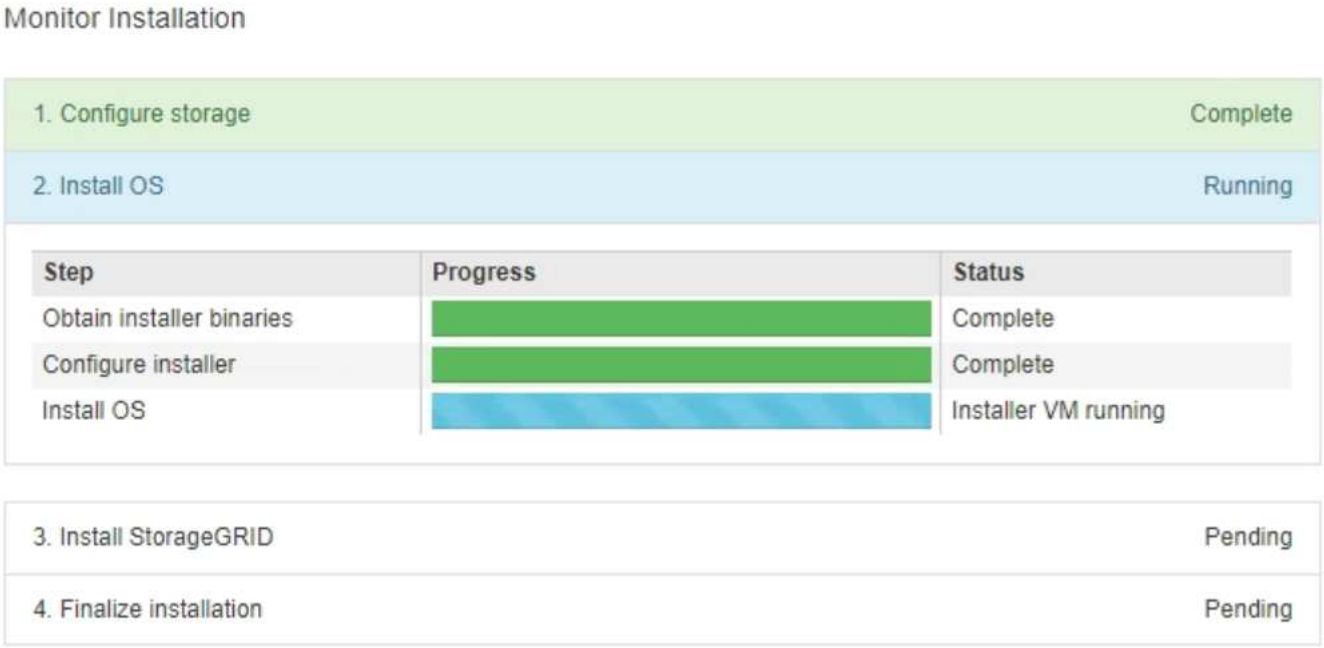
Supervisar la instalación del dispositivo de servicios

El instalador del dispositivo StorageGRID proporciona el estado hasta que se completa la instalación. Una vez finalizada la instalación del software, el dispositivo se reinicia.

Pasos

1. Para supervisar el progreso de la instalación, haga clic en **instalación del monitor** en la barra de menús.

   La página Monitor Installation (instalación del monitor) muestra el progreso de la instalación.



La barra de estado azul indica qué tarea está en curso actualmente. Las barras de estado verdes indican tareas que se han completado correctamente.

> Installer garantiza que las tareas completadas en una instalación anterior no se vuelvan a ejecutar. Si vuelve a ejecutar una instalación, las tareas que no necesitan volver a ejecutarse se muestran con una barra de estado verde y el estado “Omitida”.

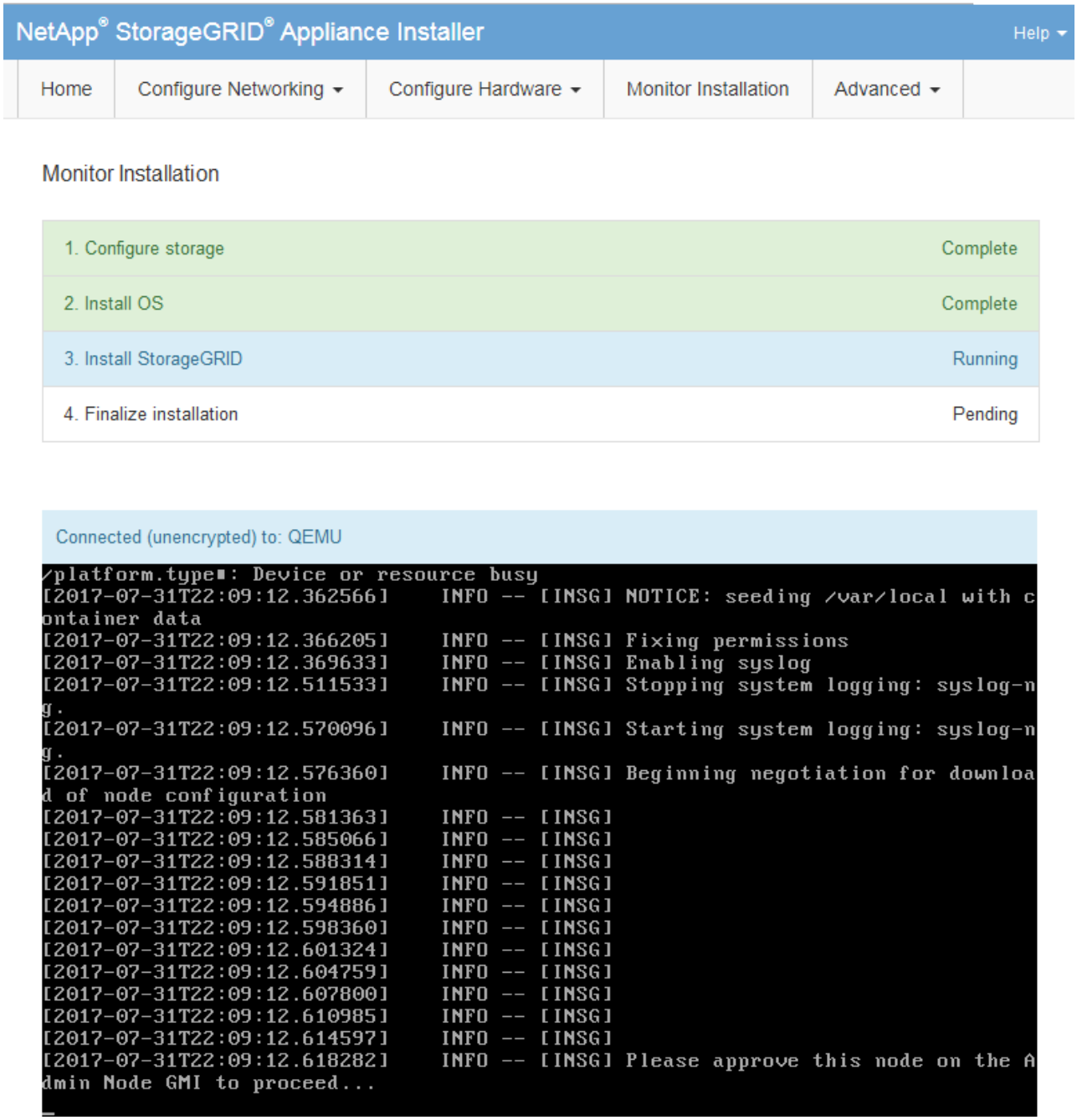
2. Revise el progreso de las dos primeras etapas de instalación.
   - **1. Configurar almacenamiento**

     Durante esta fase, el instalador borra toda la configuración existente de las unidades y configura la configuración del host.

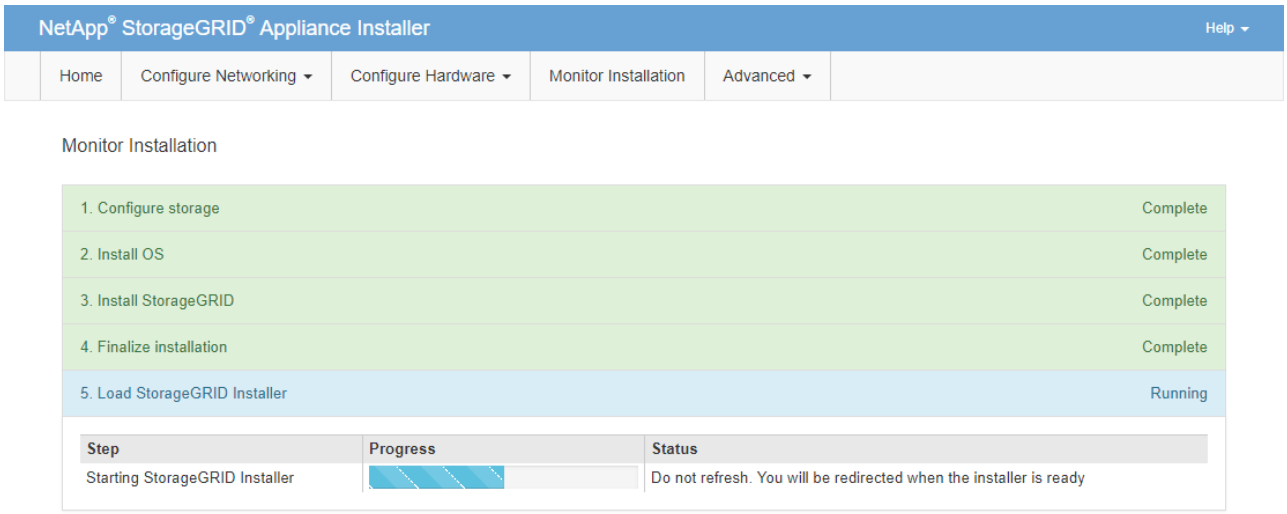
   - **2. Instalar OS**

     Durante esta fase, el instalador copia la imagen del sistema operativo base para StorageGRID desde el nodo de administración principal al dispositivo o instala el sistema operativo base desde el paquete de instalación del nodo de administración principal.

3. Continúe supervisando el progreso de la instalación hasta que se produzca una de las siguientes situaciones:
   - Para los nodos de puerta de enlace del dispositivo o los nodos de administración de dispositivos no primarios, la etapa **instalar StorageGRID** se detiene y aparece un mensaje en la consola integrada, solicitándole que apruebe este nodo en el nodo de administración mediante el Administrador de grid.



- En el caso de los nodos de administración principales del dispositivo, aparece una quinta fase (Load StorageGRID Installer). Si la quinta fase está en curso durante más de 10 minutos, actualice la página manualmente.



4. Vaya al siguiente paso del proceso de recuperación para el tipo de nodo de grid del dispositivo que está recuperando.

Tipo de recuperación	Referencia
Nodo de puerta de enlace	"Seleccione Start Recovery para configurar Gateway Node"
Nodo de administrador no primario	"Seleccione Start Recovery para configurar el nodo de administrador que no es primario"
Nodo de administrador principal	"Configure el nodo de administración principal de reemplazo"

Cómo el soporte técnico recupera un sitio

Si un sitio de StorageGRID en su totalidad falla o ocurre un error en varios nodos de almacenamiento, debe ponerse en contacto con el soporte técnico. El soporte técnico evaluará su situación, desarrollará un plan de recuperación y, a continuación, recuperará los nodos o instalaciones en los que se haya producido un error que cumpla con sus objetivos empresariales, optimizará el tiempo de recuperación y evitará la pérdida innecesaria de datos.

Solo el soporte técnico puede realizar la recuperación del sitio.

Los sistemas StorageGRID se adaptan a una gran variedad de fallos y es posible realizar muchos de los procedimientos de recuperación y mantenimiento por su cuenta. Sin embargo, es difícil crear un procedimiento de recuperación del sitio, generalizado porque los pasos detallados dependen de factores que son específicos de su situación. Por ejemplo:

- **Sus objetivos de negocio**: Después de la pérdida completa de un sitio StorageGRID, usted debe evaluar la mejor manera de cumplir sus objetivos de negocio. Por ejemplo, ¿desea reconstruir el sitio perdido en el lugar? ¿Desea sustituir el sitio StorageGRID perdido en una nueva ubicación? Cada situación de cliente es diferente y su plan de recuperación debe estar diseñado para responder a sus prioridades.
- **Naturaleza exacta del fallo**: Antes de comenzar una recuperación del sitio, establezca si algún nodo en el

sitio fallido está intacto o si algún nodo de almacenamiento contiene objetos recuperables. Si reconstruye nodos o volúmenes de almacenamiento que contienen datos válidos, podría producirse una pérdida de datos innecesaria.

- * Políticas de ILM activas*: El número, tipo y ubicación de las copias de objetos en su red es controlado por sus políticas de ILM activas. Los detalles de las políticas de ILM pueden afectar a la cantidad de datos recuperables, así como a las técnicas específicas necesarias para la recuperación.

  Si un sitio contiene la única copia de un objeto y el sitio se pierde, el objeto se pierde.

- **Consistencia de cubo (o contenedor)**: La consistencia aplicada a un depósito (o contenedor) afecta si StorageGRID replica completamente los metadatos de objeto en todos los nodos y sitios antes de decirle a un cliente que la ingesta de objetos se realizó correctamente. Si el valor de consistencia permite una coherencia eventual, es posible que algunos metadatos de objeto se hayan perdido en el fallo del sitio. Esto puede afectar a la cantidad de datos recuperables y a los detalles del procedimiento de recuperación.
- **Historial de cambios recientes**: Los detalles de su procedimiento de recuperación pueden verse afectados por si hubo algún procedimiento de mantenimiento en curso en el momento del fallo o si se realizaron cambios recientes en sus políticas de ILM. El soporte técnico debe evaluar el historial reciente de la red, así como la situación actual, antes de iniciar la recuperación del centro.

Solo el soporte técnico puede realizar la recuperación del sitio.

Esta es una descripción general del proceso que el soporte técnico utiliza para recuperar un sitio donde se ha producido un fallo:

1. Soporte técnico:
   a. Realiza una evaluación detallada del fallo.
   b. Trabaja contigo para revisar tus objetivos de negocio.
   c. Desarrolla un plan de recuperación adaptado a la situación.
2. Si el nodo de administración principal falla, el soporte técnico lo recupera.
3. El soporte técnico recupera todos los nodos de almacenamiento, siguiendo este esquema:
   a. Sustituya el hardware o las máquinas virtuales del nodo de almacenamiento según sea necesario.
   b. Restaure los metadatos de objetos al sitio con errores.
   c. Restaurar datos de objetos en los nodos de almacenamiento recuperados.

   Se perderán datos si se utilizan los procedimientos de recuperación de un único nodo de almacenamiento fallido.

   Cuando falla todo un sitio, el soporte técnico utiliza comandos especializados para restaurar correctamente objetos y metadatos de objetos.

4. El soporte técnico recupera otros nodos con errores.

   Después de recuperar los metadatos y los datos del objeto, el soporte técnico utiliza procedimientos estándar para recuperar nodos de pasarela con errores, nodos de administración no principales o nodos de archivado.

Información relacionada

"Retirada de sitios"

Cómo habilitar StorageGRID en su entorno

Vaya a. "Cómo habilitar StorageGRID en su entorno" Para obtener más información sobre cómo probar y habilitar las aplicaciones en su entorno StorageGRID.

El sitio de documentación **storagegrid-enable** proporciona ejemplos y libros de cocina que se expanden sobre la documentación del producto en este sitio, y describe algunos pasos siguientes para evaluar e integrar con StorageGRID.

Parte de la información incluía:

- Listas de soluciones de terceros validadas para versiones anteriores y actuales de StorageGRID.
- Guías de características de productos. Por ejemplo, estas guías proporcionan toda la información que necesita para crear pools de almacenamiento en la nube.
- Guías de herramientas y aplicaciones.
- Ejemplos de API para usar funciones de StorageGRID como el cifrado S3 y el bloqueo de objetos S3.

Otras versiones de la documentación de StorageGRID de NetApp

Encontrará documentación para otras versiones del software NetApp StorageGRID aquí:

- "Documentación de StorageGRID 11,7"
- "Documentación de StorageGRID 11,6"
- "Documentación de StorageGRID 11,5"
- "Centro de documentación de StorageGRID 11,4"
- "Centro de documentación de StorageGRID 11,3"
- "Centro de documentación de StorageGRID 11,2"

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

https://library.netapp.com/ecm/ecm_download_file/ECMLP2886898