Documentación de StorageGRID 11.6

StorageGRID

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-116/index.html on April 10, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Documentación de StorageGRID 11.6 . . . 1
Notas de la versión . . . 2
Manos a la obra . . . 3
- Imprimador de rejilla . . . 3
- Directrices sobre redes . . . 72

Instale y mantenga el hardware del dispositivo . . . 105
- Servicios de aplicaciones SG100 y SG1000 . . . 105
- Dispositivos de almacenamiento SG6000 . . . 219
- Dispositivos de almacenamiento SG5700 . . . 405
- Dispositivos de almacenamiento SG5600 . . . 542

Instale y actualice el software . . . 664
- Actualice el software StorageGRID . . . 664
- Instale Red Hat Enterprise Linux o CentOS . . . 700
- Instalar Ubuntu o Debian . . . 766
- Instale VMware . . . 832

Realizar la administración del sistema . . . 883
- Administre StorageGRID . . . 883
- Gestión de objetos con ILM . . . 1185
- Endurecimiento del sistema . . . 1351
- Configure FabricPool . . . 1359

Utilice StorageGRID . . . 1379
- Usar una cuenta de inquilino . . . 1379
- Use S3 . . . 1485
- Use Swift . . . 1619

Supervisar y mantener StorageGRID . . . 1652
- Supervisión y solución de problemas . . . 1652
- Amplíe su grid . . . 2007
- Recuperación y mantenimiento . . . 2064
- Revisar los registros de auditoría . . . 2317

Cómo habilitar StorageGRID en su entorno . . . 2411
Otras versiones de la documentación de StorageGRID de NetApp . . . 2412
Avisos legales . . . 2413
- Derechos de autor . . . 2413
- Marcas comerciales . . . 2413
- Estadounidenses . . . 2413
- Política de privacidad . . . 2413
- Código abierto . . . 2413

Documentación de StorageGRID 11.6

Notas de la versión

Obtener información específica de la versión sobre funciones nuevas, funciones eliminadas o obsoletas, problemas solucionados y problemas conocidos.

Inicie sesión en el sitio de soporte de NetApp en "Vea o descargue un archivo PDF" Contener las notas de la versión de StorageGRID 11.6.

Manos a la obra

Imprimador de rejilla

Imprimador de rejilla: Descripción general

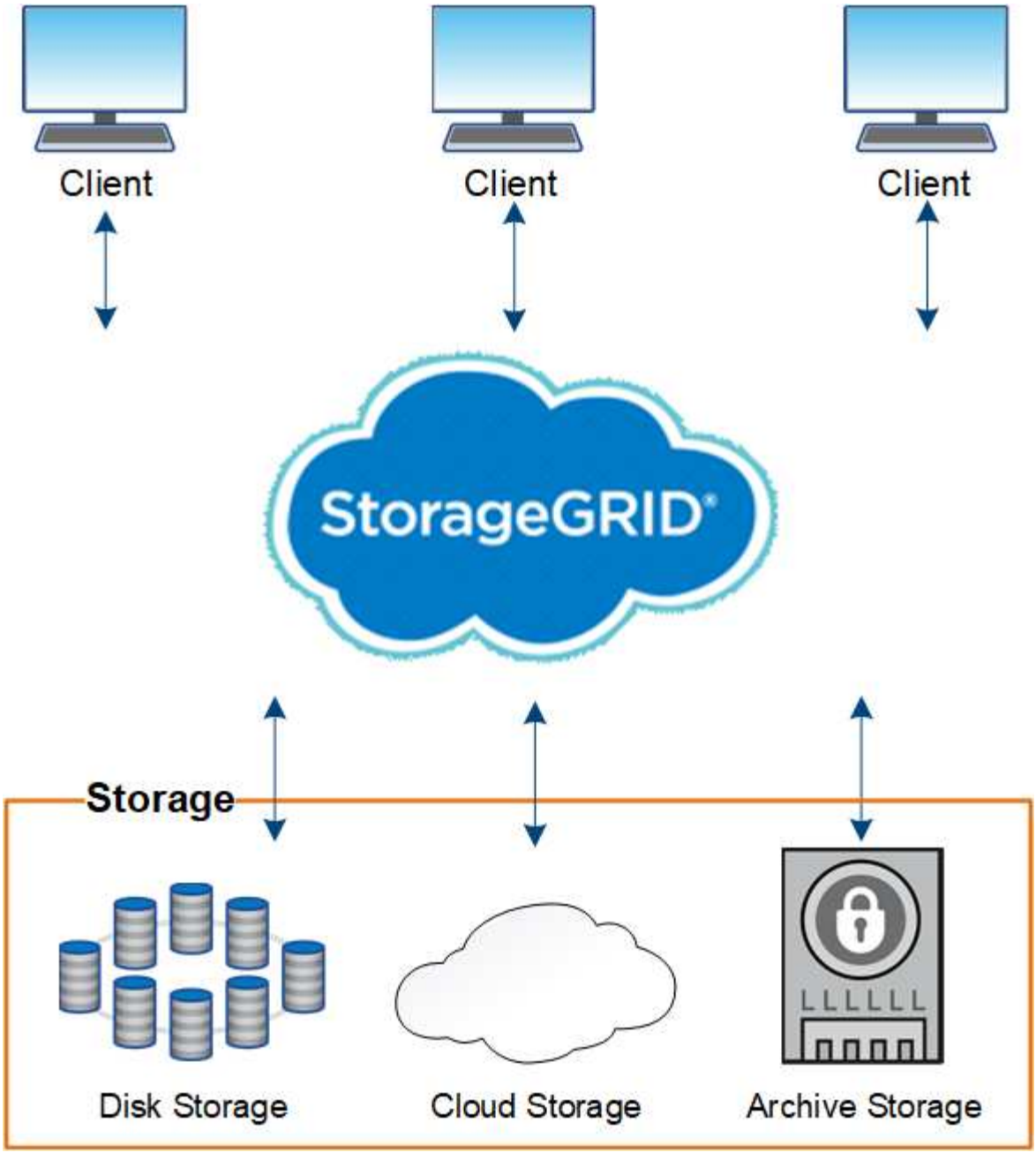
Use esta introducción para obtener información general del sistema StorageGRID y obtener información sobre la arquitectura de StorageGRID y la topología de redes, las funciones de gestión de datos y la interfaz de usuario.

¿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.



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
- 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. Se pueden crear reglas de ILM que gestionen el ciclo de vida de los datos en el nivel de los objetos y personalicen la ubicación de los datos, la durabilidad, el rendimiento, el coste y el tiempo de retención. La cinta está disponible como nivel de archivado integrado.
- 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

Puede utilizar StorageGRID en una configuración de cloud híbrido implementando gestión de datos condicionada por políticas para almacenar objetos en Cloud Storage Pools, aprovechando los servicios de plataforma StorageGRID y trasladando datos 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 prefiera mover objetos a los que se accede con poca frecuencia a un almacenamiento en cloud de menor coste, como Amazon S3 Glacier, S3 Glacier Deep Archive o el nivel de acceso Archive en el almacenamiento 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.

> 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 extremo externo que admite la recepción de eventos de servicio de notificación simple (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 con StorageGRID

Puede reducir el coste del almacenamiento de ONTAP organizando en niveles los datos en StorageGRID utilizando FabricPool. FabricPool es una tecnología Data Fabric de NetApp que permite la organización en niveles automatizada de los datos 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

- Administre StorageGRID
- Usar una cuenta de inquilino
- Gestión de objetos con ILM
- 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.

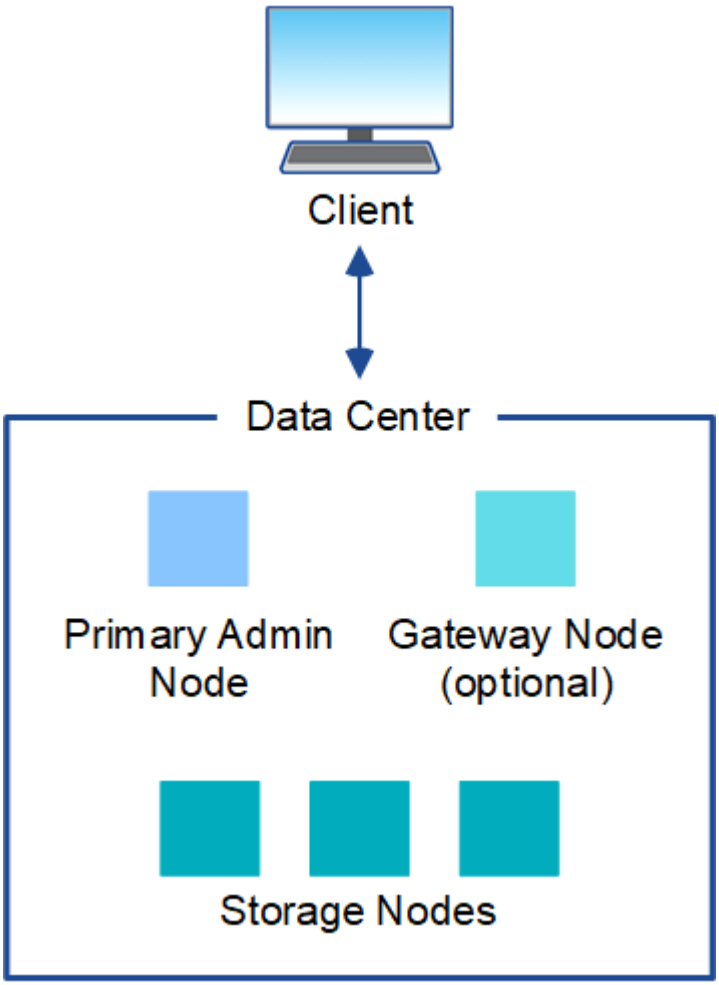
Para obtener información adicional sobre la topología de red, los requisitos y las comunicaciones de grid de StorageGRID, consulte Directrices sobre redes.

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

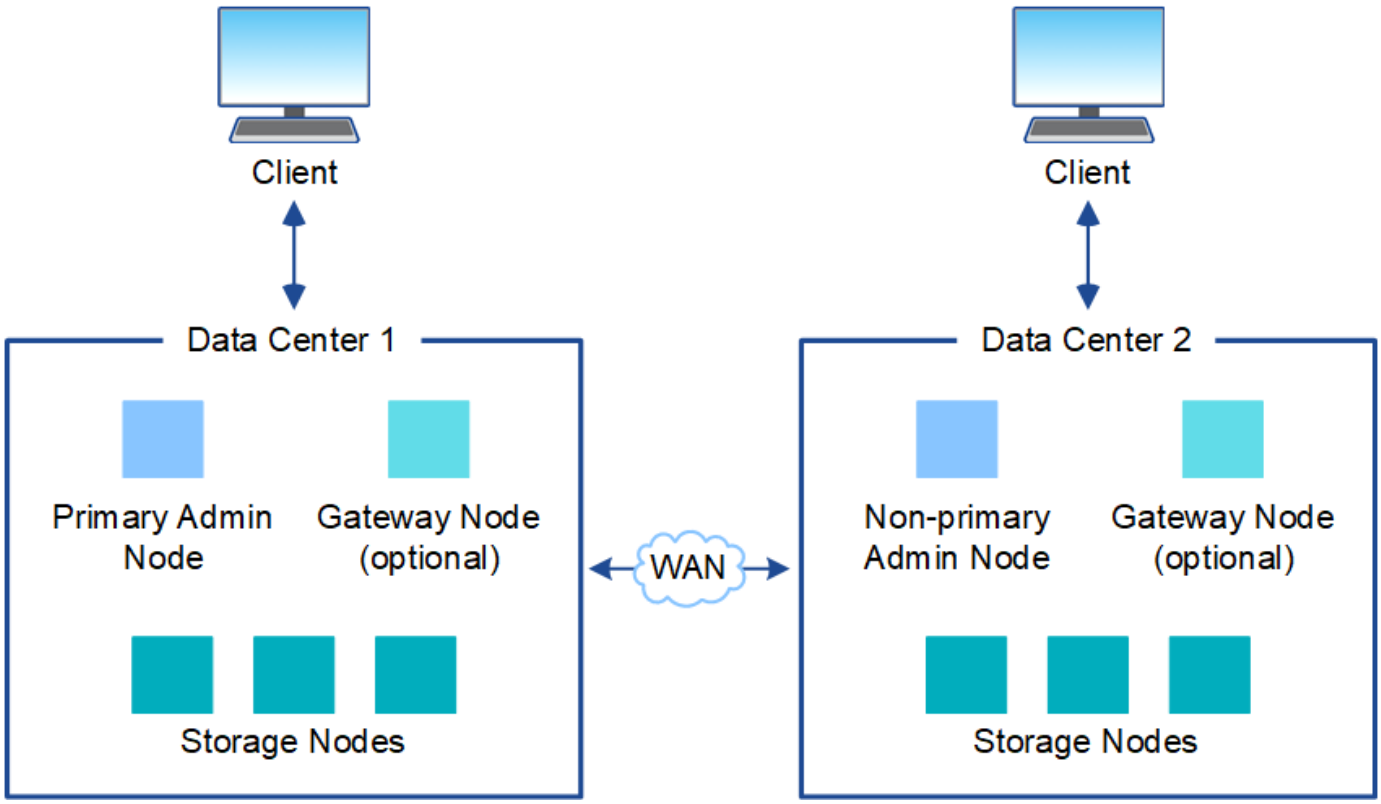
En una puesta en marcha con un único sitio, la infraestructura y las operaciones del sistema StorageGRID están centralizadas.



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.



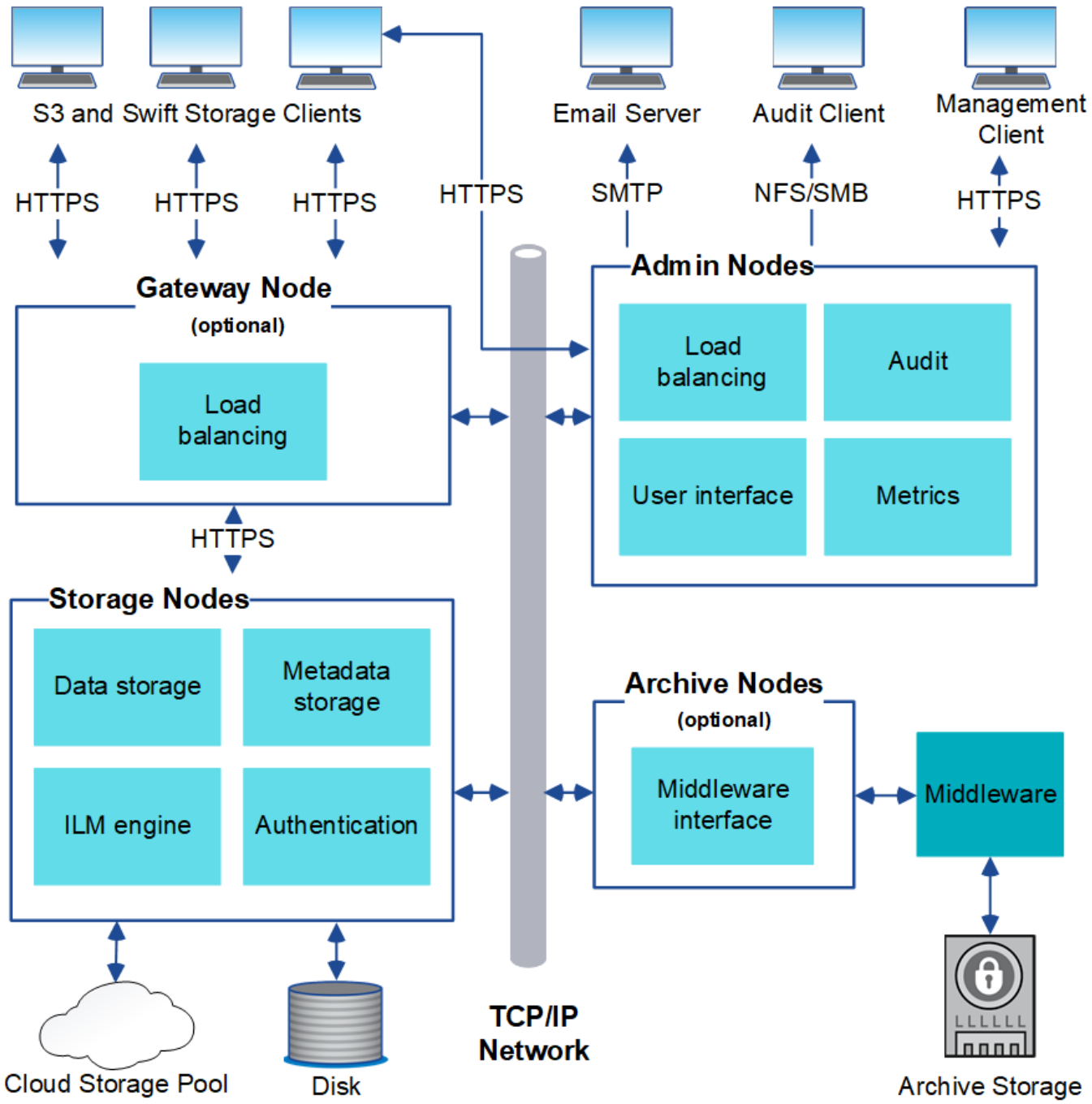
También pueden existir varios sitios lógicos en un único centro de datos y así permitir el uso de replicación distribuida y código de borrado para aumentar la disponibilidad y la resiliencia.

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 se pueden almacenar en StorageGRID en nodos de almacenamiento basados en software o hardware, en medios de archivado externos como cinta, o en pools de almacenamiento en cloud, que constan de bloques de S3 externos o contenedores de almacenamiento blob de Azure.

Nodos de grid y servicios

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.

El sistema StorageGRID utiliza cuatro tipos de nodos de grid:

- **Los nodos de administración** proporcionan servicios de administración tales como la configuración del sistema, la supervisión y el registro. 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.

- **Nodos de almacenamiento** gestionar y almacenar metadatos y datos de objetos. Cada sistema StorageGRID debe tener al menos tres nodos de almacenamiento. Si tiene varios sitios, cada sitio dentro del sistema StorageGRID también debe tener tres nodos de almacenamiento.
- **Los nodos de puerta de enlace (opcionales)** proporcionan una interfaz de equilibrio de carga que las aplicaciones cliente pueden 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. Puede utilizar una combinación de nodos de puerta de enlace y nodos de administración para el equilibrio de carga o puede implementar un equilibrador de carga HTTP de terceros.
- **Los nodos de archivo (opcionales)** proporcionan una interfaz a través de la cual los datos de objeto se pueden archivar en cinta.

Para obtener más información, consulte Administre StorageGRID.

Nodos basados en software

Los nodos de grid basados en software se pueden poner en marcha de las siguientes formas:

- Como máquinas virtuales en VMware vSphere
- Dentro de los motores de contenedor en los hosts Linux. Se admiten los sistemas operativos siguientes:
  - Red Hat Enterprise Linux
  - CentOS
  - Ubuntu
  - Debian

En la siguiente sección, se ofrece más información:

- Instale VMware
- Instale Red Hat Enterprise Linux o CentOS
- Instalar Ubuntu o Debian

Utilice la "Herramienta de matriz de interoperabilidad de NetApp" para obtener una lista de las versiones compatibles.

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.

Hay cuatro tipos de dispositivos StorageGRID disponibles:

- Los dispositivos **SG100 y SG1000 de servicios** son servidores de 1 unidad de bastidor (1U) que pueden funcionar como el nodo de administración principal, un nodo de administración no primario o un nodo de puerta de enlace. Ambos dispositivos pueden funcionar al mismo tiempo como nodos de puerta de enlace y nodos de administración (principal y no primario).
- El dispositivo de almacenamiento **SG6000** funciona como nodo de almacenamiento y combina el controlador de computación SG6000-CN 1U con una bandeja de controladoras de almacenamiento 2U o 4U. El SG6000 está disponible en tres modelos:
  - **SGF6024**: Combina el controlador informático SG6000-CN con una bandeja de controlador de almacenamiento 2U que incluye 24 unidades de estado sólido (SSD) y controladores de almacenamiento redundantes.
  - **SG6060 y SG606060X**: Combina el controlador de computación SG6000-CN con un alojamiento de 4U que incluye 58 unidades NL-SAS, 2 SSD y controladoras de almacenamiento redundantes. SG6060 y SG606060X admiten cada una una de las bandejas de expansión de 60 unidades, ofreciendo hasta 178 unidades dedicadas al almacenamiento de objetos.
- El dispositivo de almacenamiento **SG5700** es una plataforma de almacenamiento e informática integrada que funciona como nodo de almacenamiento. SG5700 está disponible en cuatro modelos:
  - **SG5712 y SG5712X**: Carcasa 2U que incluye 12 unidades NL-SAS y controladoras de almacenamiento e informática integradas.
  - **SG5760 y SG5760X**: Carcasa 4U que incluye 60 unidades NL-SAS y controladoras informáticas y de almacenamiento integradas.
- El dispositivo de almacenamiento * SG5600* es una plataforma de almacenamiento e informática integrada que funciona como nodo de almacenamiento. SG5600 está disponible en dos modelos:
  - **SG5612**: Un compartimento de 2U que incluye 12 unidades NL-SAS y controladoras de computación y almacenamiento integradas.
  - **SG5660**: Un compartimento de 4U que incluye 60 unidades NL-SAS y controladoras integradas de almacenamiento e informática.

En la siguiente sección, se ofrece más información:

- "Hardware Universe de NetApp"
- Servicios de aplicaciones SG100 y SG1000
- Dispositivos de almacenamiento SG6000
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG5600

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 auditorías (AMS)	Realiza un seguimiento de la actividad del sistema.
Nodo de gestión de configuraciones (CMN)	Gestiona la configuración en todo el sistema. Solo nodo de administrador principal.
Interfaz de programas de aplicaciones de gestión (API de gestión)	Procesa las solicitudes de la API de gestión de grid y la API de gestión de inquilinos.
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.
Sistema de gestión de redes (NMS)	Proporciona funcionalidad para Grid Manager.
Prometheus	Recopila y almacena métricas.
Monitor de estado del servidor (SSM)	Supervisa el sistema operativo y el hardware subyacente.

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.
Cassandra	Almacena y protege los metadatos de objetos.
Cassandra Reaper	Realiza reparaciones automáticas de metadatos de objetos.

Servicio	Función de la tecla
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.
Identidad (no)	Federe las identidades de usuario de LDAP y Active Directory.
Router de distribución local (LDR)	Procesa las solicitudes del protocolo de almacenamiento de objetos y gestiona los datos de objetos en el disco.
Máquina de estado replicada (RSM)	Garantiza que las solicitudes de servicio de la plataforma S3 se envíen a sus respectivos extremos.
Monitor de estado del servidor (SSM)	Supervisa el sistema operativo y el hardware subyacente.

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
Equilibrador de carga de conexión (CLB)	Proporciona un balanceo de carga de capas 3 y 4 del tráfico S3 y Swift de clientes a nodos de almacenamiento. Mecanismo de equilibrio de carga heredado. **Nota:** el servicio CLB está en desuso.
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.
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.

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.

Servicios de StorageGRID

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

- **Servicio de cuenta Forwarder**

  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. El servicio Load Balancer está presente en los nodos de administración y de puerta de enlace.

- **Servicio ADC (controlador de dominio administrativo)**

  Mantiene información de topología, proporciona servicios de autenticación y responde a las consultas de los servicios LDR y CMN. El servicio de ADC está presente en cada uno de los tres primeros nodos de almacenamiento instalados en un sitio.

- **Servicio AMS (sistema de Gestión de Auditoría)**

  Supervisa y registra todos los eventos y transacciones auditados del sistema en un archivo de registro de texto. El servicio AMS está presente en los nodos Admin.

- **Servicio ARC (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. El servicio ARC está presente en los nodos de archivado.

- **Cassandra Servicio Reaper**

  Realiza reparaciones automáticas de metadatos de objetos. El servicio Cassandra Reaper está presente en todos los nodos de almacenamiento.

- **Servicio de Chunk**

  Gestiona datos codificados de borrado y fragmentos de paridad. El servicio Chunk está presente en los nodos de almacenamiento.

- **Servicio CLB (equilibrador de carga de conexión)**

  Servicio obsoleto que proporciona una puerta de enlace a StorageGRID para aplicaciones cliente que se conectan a través de HTTP. El servicio CLB está presente en los nodos de puerta de enlace. El servicio

CLB quedó obsoleto y se quitará en un lanzamiento futuro de StorageGRID.

- **Servicio CMN (nodo de administración de configuración)**

  Gestiona las configuraciones de todo el sistema y las tareas de grid. Cada cuadrícula tiene un servicio CMN, que está presente en el nodo de administración principal.

- **Servicio DDS (almacén de datos distribuido)**

  Interactúa con la base de datos de Cassandra para gestionar los metadatos de objetos. El servicio DDS está presente en los nodos de almacenamiento.

- **Servicio DMV (Data Mover)**

  Mueve los datos a extremos de cloud. El servicio DMV está presente en los nodos de almacenamiento.

- **Servicio IP dinámico**

  Supervisa la cuadrícula para los cambios dinámicos de IP y actualiza las configuraciones locales. El servicio IP dinámica (dynip) está presente en todos los nodos.

- **Servicio Grafana**

  Se utiliza para la visualización de métricas en Grid Manager. El servicio Grafana se encuentra en los nodos de administración.

- **Servicio de alta disponibilidad**

  Administra IP virtuales de alta disponibilidad en nodos configurados en la página grupos de alta disponibilidad. El servicio de alta disponibilidad está presente en los nodos de administración y de puerta de enlace. Este servicio también se conoce como servicio de keepalived.

- **Servicio de identidad (idnt)**

  Federe las identidades de usuario de LDAP y Active Directory. El servicio de identidades (idnt) está presente en tres nodos de almacenamiento en cada sitio.

- **Servicio de Árbitros Lambda**

  Gestiona solicitudes S3 Select ObjectContent.

- **Servicio de equilibrador de carga**

  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. El servicio Load Balancer está presente en los nodos de administración y de puerta de enlace. Este servicio también se conoce como servicio nginx-gw.

- **Servicio LDR (router de distribución local)**

  Gestiona el almacenamiento y la transferencia de contenido dentro de la cuadrícula. El servicio LDR está presente en los nodos de almacenamiento.

- **Servicio de MDaemon 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. El servicio MISCd está presente en todos los nodos.

- **servicio 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. El servicio nginx está presente en todos los nodos.

- **servicio nginx-gw**

  Activa el servicio Load Balancer. El servicio nginx-gw está presente en los nodos Admin y Gateway.

- **Servicio NMS (sistema de administración de redes)**

  Activa las opciones de supervisión, generación de informes y configuración que se muestran a través de Grid Manager. El servicio NMS está presente en los nodos Admin.

- **Servicio de persistencia**

  Administra los archivos del disco raíz que deben persistir durante un reinicio. El servicio de persistencia está presente en todos los nodos.

- **Servicio Prometheus**

  Recopila métricas de series temporales de los servicios en todos los nodos. El servicio Prometheus está presente en los nodos de administración.

- **Servicio RSM (Servicio de máquina de estado replicado)**

  Garantiza que las solicitudes de servicio de la plataforma se envíen a sus respectivos extremos. El servicio RSM está presente en los nodos de almacenamiento que utilizan el servicio ADC.

- **Servicio SSM (Monitor de estado del servidor)**

  Supervisa las condiciones del hardware e informa al servicio NMS. En todos los nodos de cuadrícula hay una instancia del servicio SSM.

- **Servicio de colector de traza**

  Realiza la recogida de seguimiento para recopilar información que el soporte técnico utiliza. El servicio de colector de traza utiliza el software de código abierto Jäger y está presente en los nodos de administración.

Gestión de objetos

Cómo StorageGRID gestiona los datos

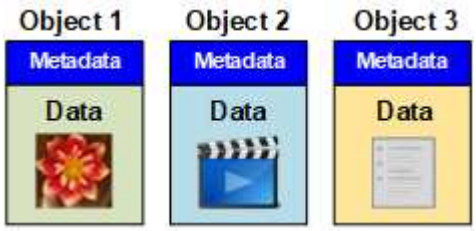
Cuando comience a trabajar con el sistema StorageGRID, es útil entender cómo gestiona los datos el sistema StorageGRID.

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.



Datos de objetos

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

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.

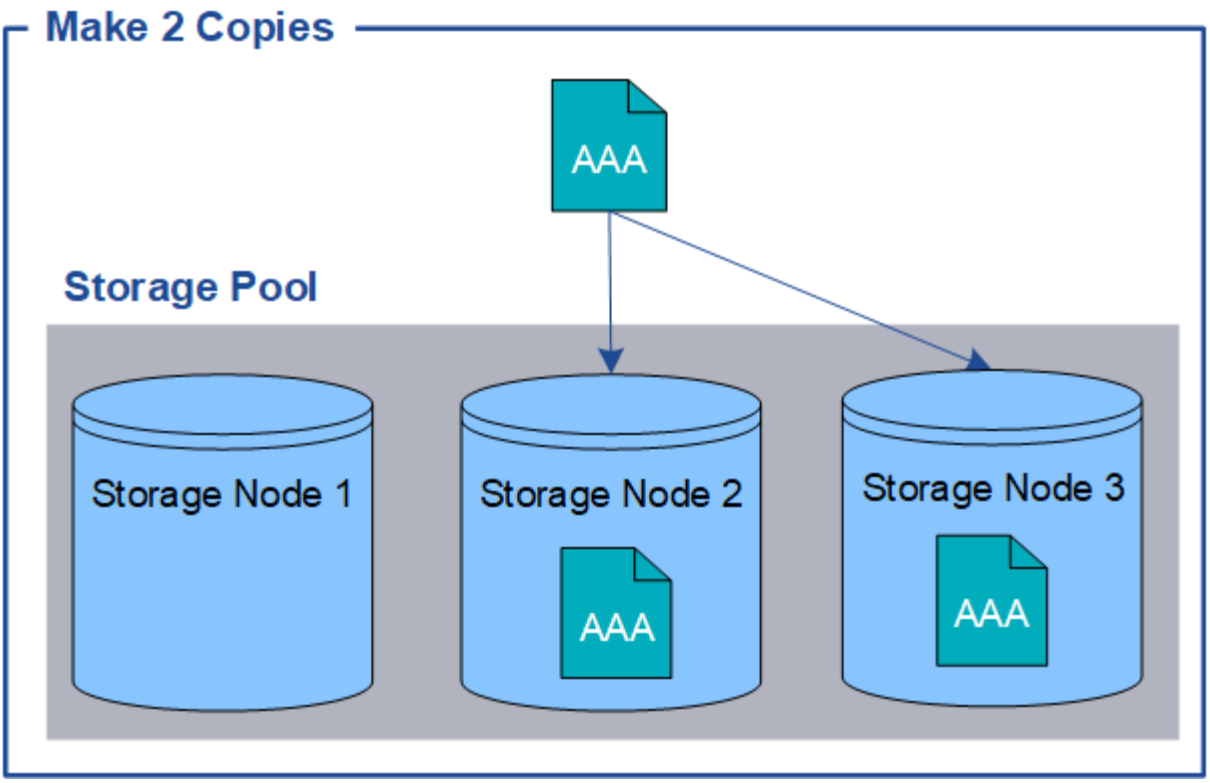
Cómo se protegen los datos de objetos

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.

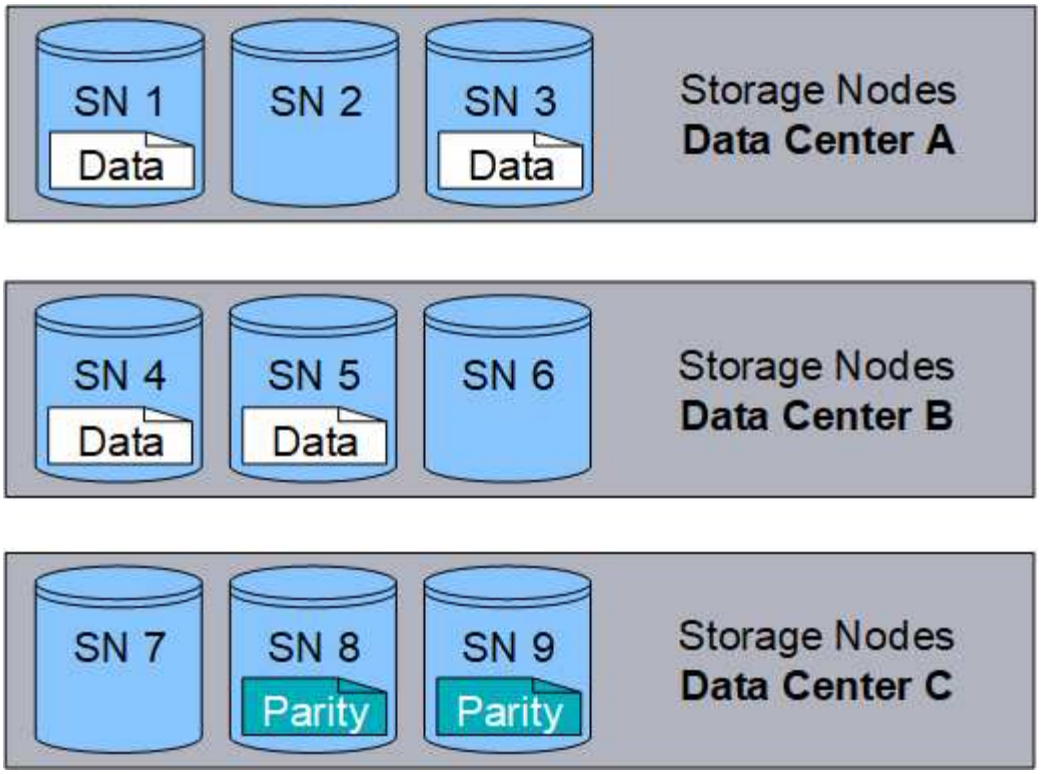
En el ejemplo siguiente, la regla make 2 copies especifica que se coloquen dos copias replicadas de cada objeto en un pool de almacenamiento que contenga tres nodos de almacenamiento.



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

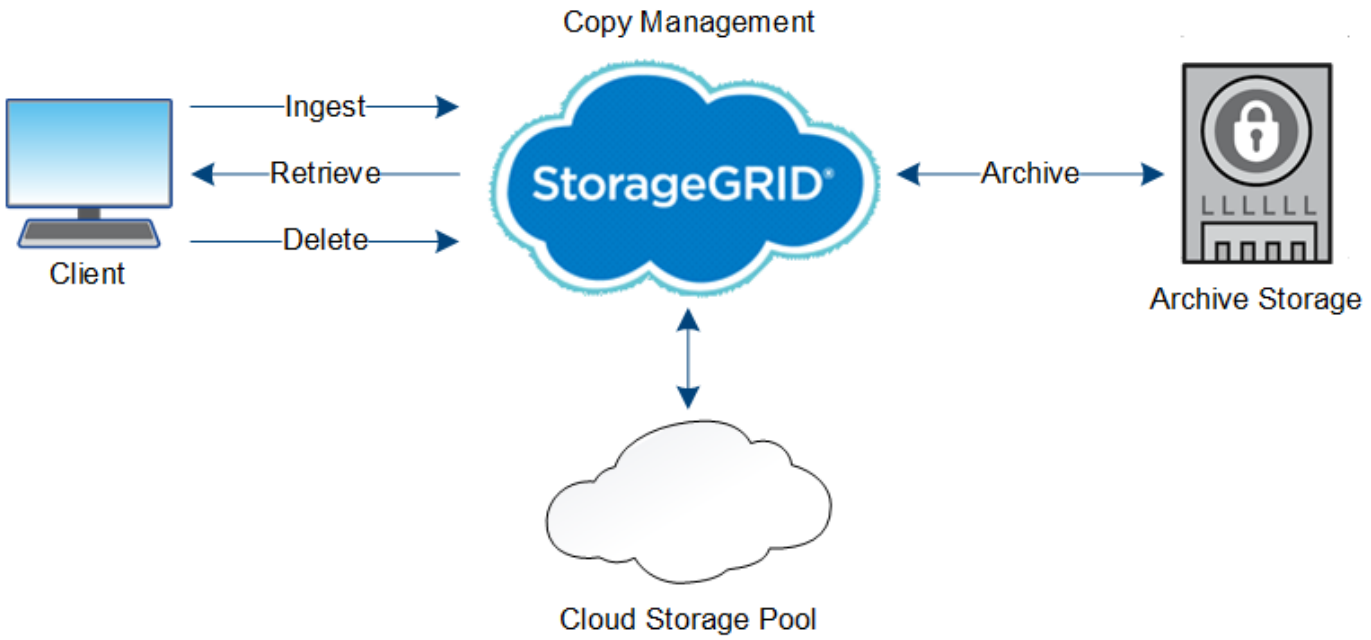
Ciclo de vida del objeto

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 codificadas por borrado en StorageGRID, como se describe en las reglas de ILM de la política activa de ILM. 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

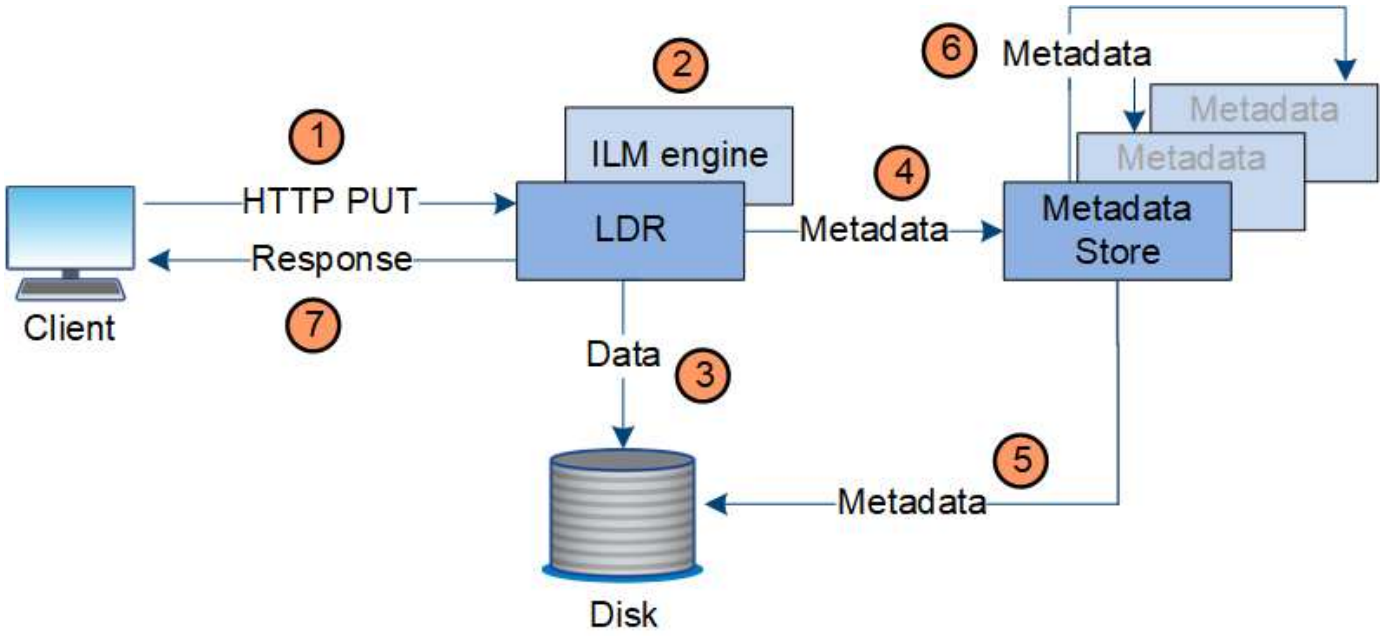
- Gestión de objetos con ILM
- Utilizar la gestión del ciclo de vida de la información

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 codificada por 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 la política de ILM activa y sus reglas de ILM. Las reglas de ILM hacen copias replicadas o codificadas de borrado para proteger los datos de los objetos ante pérdidas.

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.

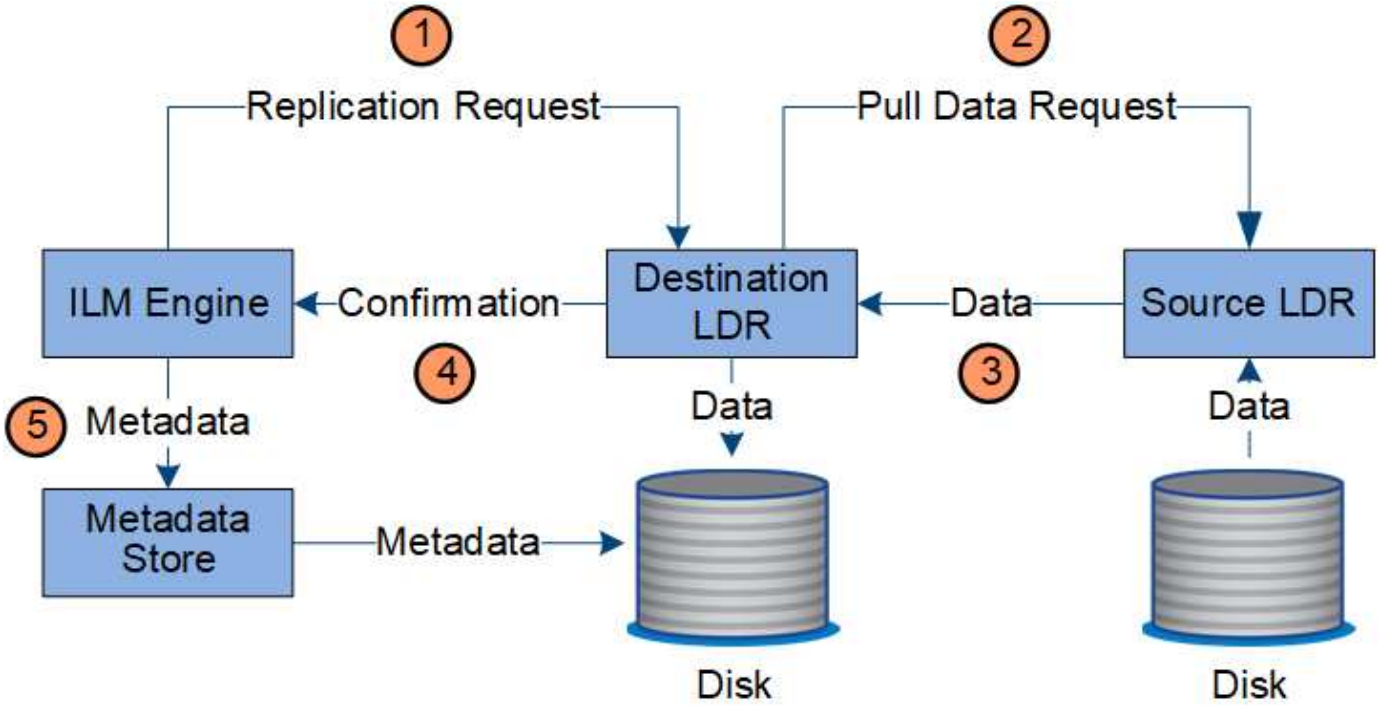
El servicio LDR gestiona los datos de objetos.

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.

Flujo de datos

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.



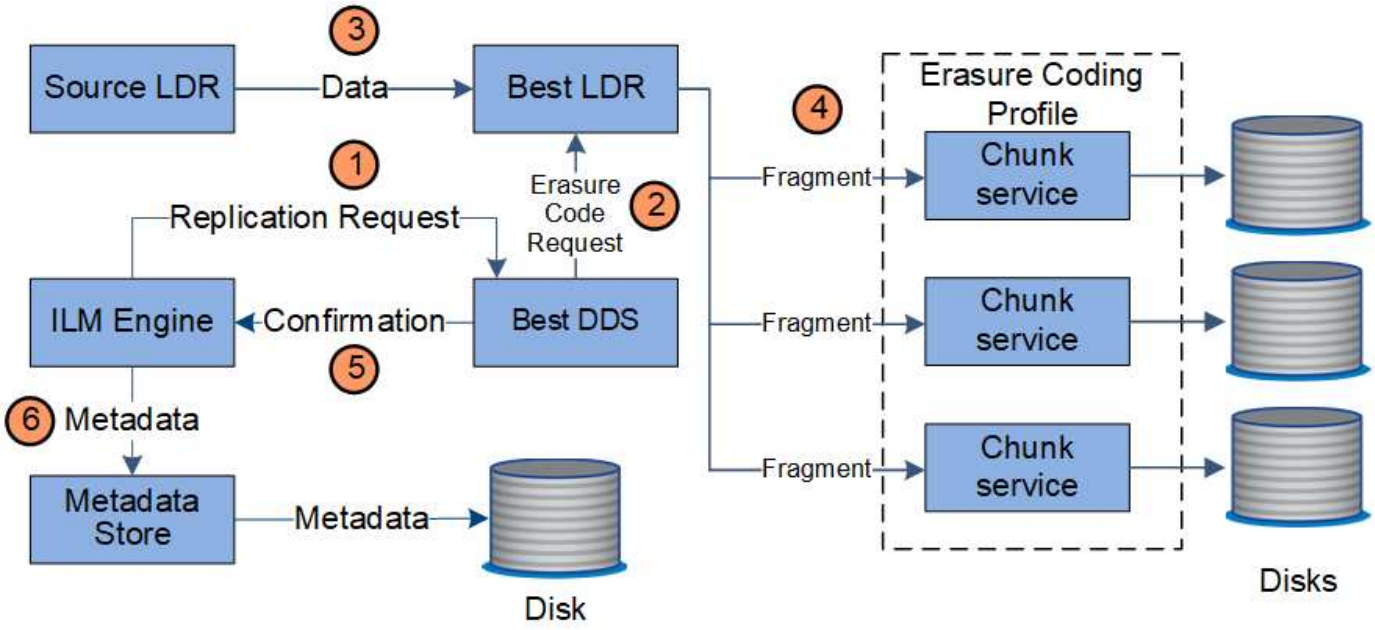
1. El motor de ILM consulta al servicio ADC para determinar el mejor servicio LDR de destino dentro del pool de almacenamiento especificado por la regla de ILM. A continuación, envía ese servicio LDR un comando para iniciar la replicación.
2. El servicio LDR de destino consulta al servicio ADC para obtener 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 realizar copias con código de borrado de los datos de objetos, el esquema de código de borrado aplicable separa los datos de los objetos en fragmentos de datos y de paridad, y distribuye estos fragmentos en los nodos de almacenamiento configurados en el perfil de código de borrado.

Flujo de datos

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



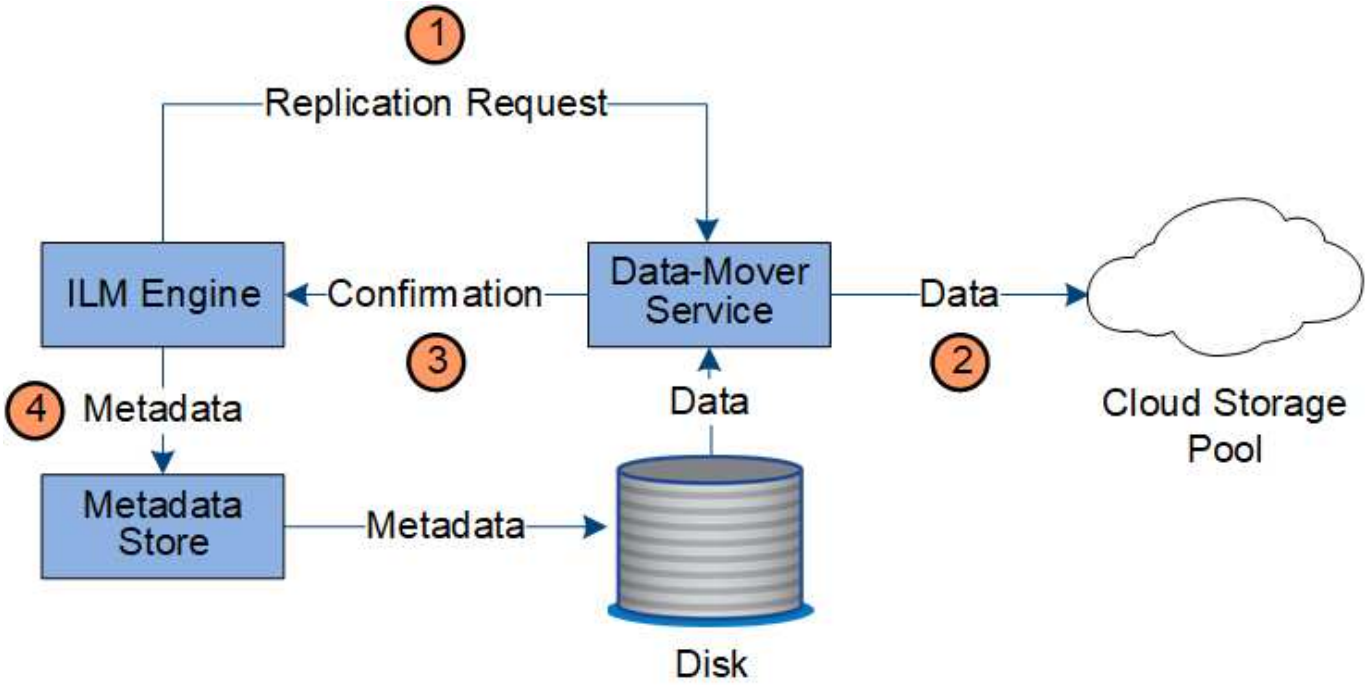
1. El motor ILM consulta al servicio ADC para determinar qué servicio DDS puede realizar mejor la operación de codificación de borrado. Una vez determinado, el motor de ILM envía una solicitud para "iniciar" a ese servicio.
2. El servicio DDS indica a un LDR que borre los datos del objeto.
3. El servicio LDR de origen envía una copia al servicio LDR seleccionado para codificación de borrado.
4. Una vez divididos en el número adecuado de fragmentos de paridad y datos, el servicio LDR distribuye estos fragmentos en los nodos de almacenamiento (servicios Chunk) que conforman el pool de almacenamiento del perfil de código 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.

Flujo de datos

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.

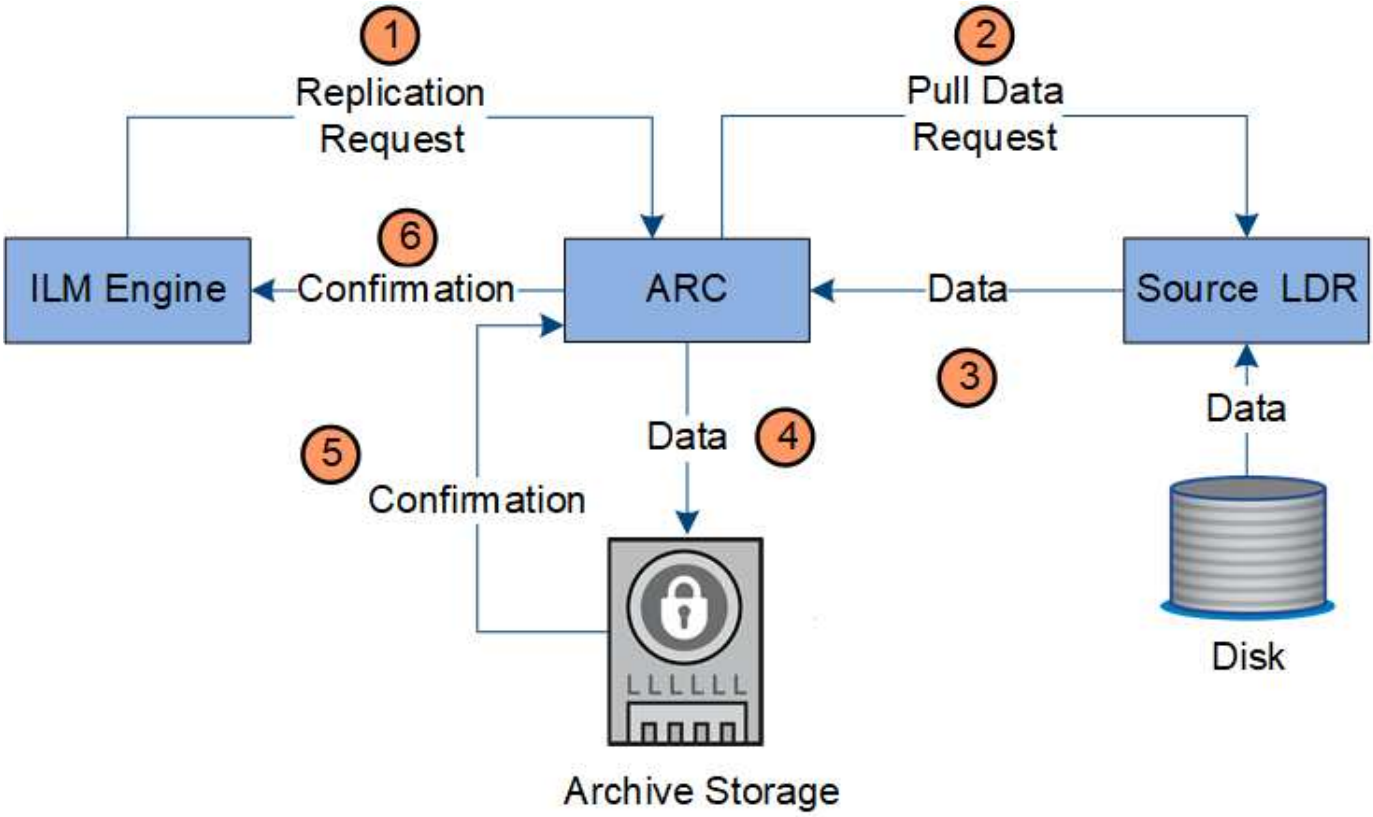


1. El motor de ILM selecciona un servicio Data mover para replicar en el Cloud Storage Pool.
2. El servicio Data mover envía los datos del objeto al Pool de almacenamiento en la nube.
3. El servicio Data mover notifica al motor ILM que los datos del objeto se han almacenado.
4. El motor de ILM actualiza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

Protección de contenido: archivo

Una operación de archivado consta de un flujo de datos definido entre el sistema StorageGRID y el cliente.

Si la política de ILM requiere archivar una copia de datos de objeto, el motor ILM, que es un componente del servicio LDR, envía una solicitud al nodo de archivado, que a su vez envía una copia de los datos de objeto al sistema de almacenamiento de archivado objetivo.



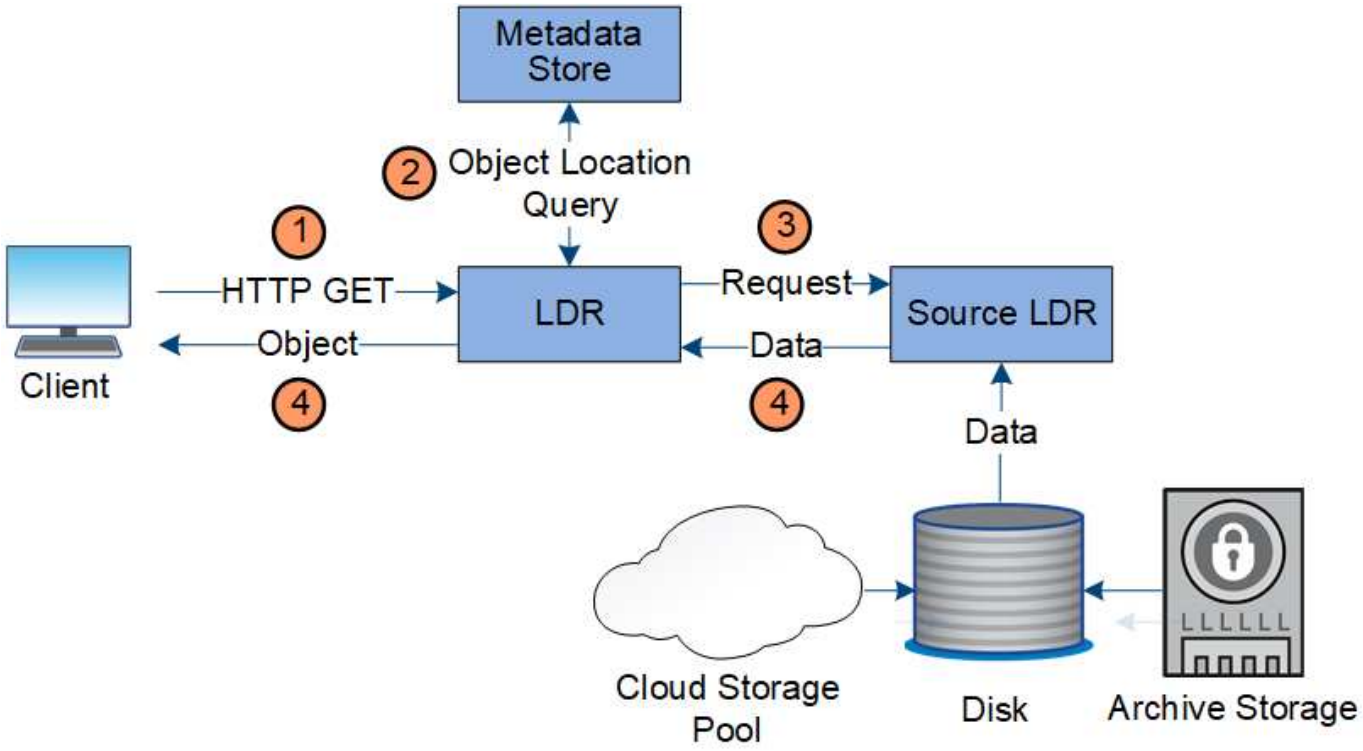
1. El motor ILM envía una solicitud al servicio ARC para almacenar una copia en los medios de archivado.
2. El servicio ARC consulta al servicio ADC para obtener la mejor ubicación de origen y envía una solicitud al servicio LDR de origen.
3. El servicio ARC recupera los datos de objeto del servicio LDR.
4. El servicio ARC envía los datos del objeto al destino del medio de archivado.
5. El medio de archivado notifica al servicio ARC que los datos del objeto se han almacenado.
6. El servicio ARC notifica al motor de ILM que los datos del objeto se han almacenado.

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 objetos está en el almacenamiento AWS Glacier o el nivel Azure Archive, la aplicación cliente debe emitir una solicitud DE restauración DE objetos S3 POSTERIOR para restaurar una copia recuperable al 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.
  - Cualquier método no puede eliminar una versión de objeto que esté bajo una retención legal.
  - Antes de que se alcance la fecha de retención de una versión de objeto, dicha versión no se puede eliminar mediante ningún método.
  - Los objetos en bloques con bloqueo de objetos S3 activado quedan retenidos por ILM "'eternamente'". Sin embargo, una vez alcanzada la fecha de retención hasta la fecha, una solicitud de cliente puede

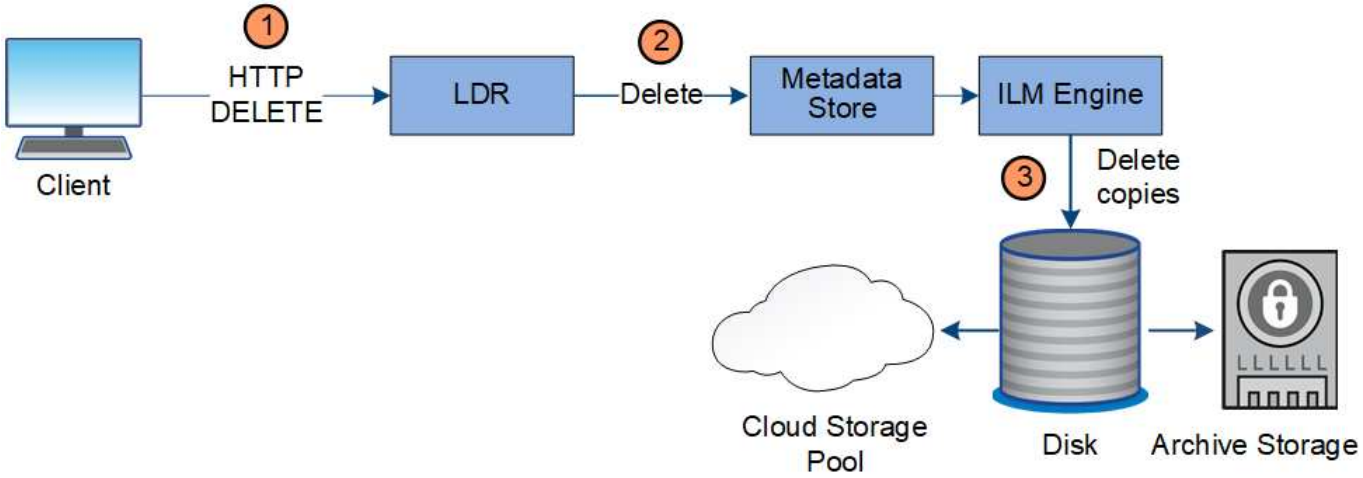
eliminar una versión de objeto o la expiración del ciclo de vida de la cuchara.

  - Si los clientes de S3 aplican una retención hasta la fecha predeterminada al bloque, no necesitan 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.
- **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.

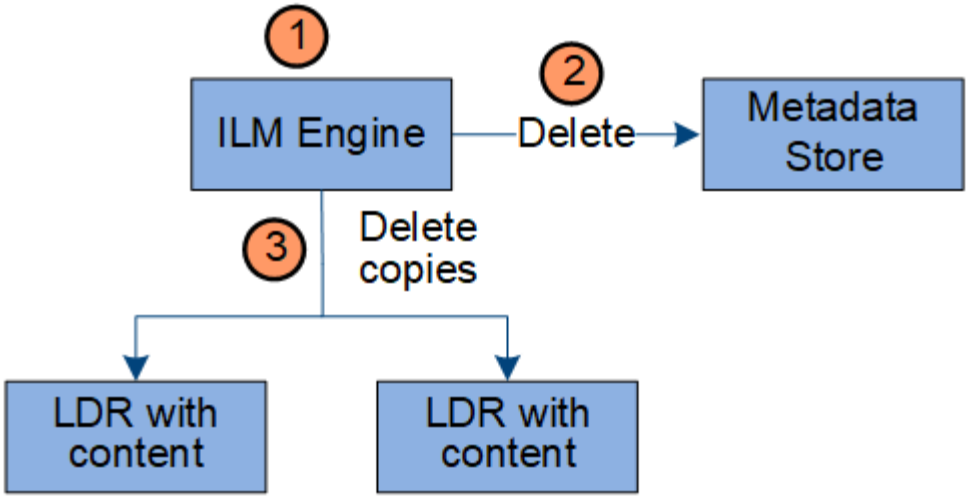
> La acción de caducidad en un ciclo de vida de bloque de S3 siempre anula la configuración de ILM. Como resultado, es posible que un objeto se conserve en la cuadrícula aunque hayan caducado las instrucciones de gestión del ciclo de vida de la información relativas a la ubicación del objeto.

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.

Cómo utilizar StorageGRID

Explore Grid Manager

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

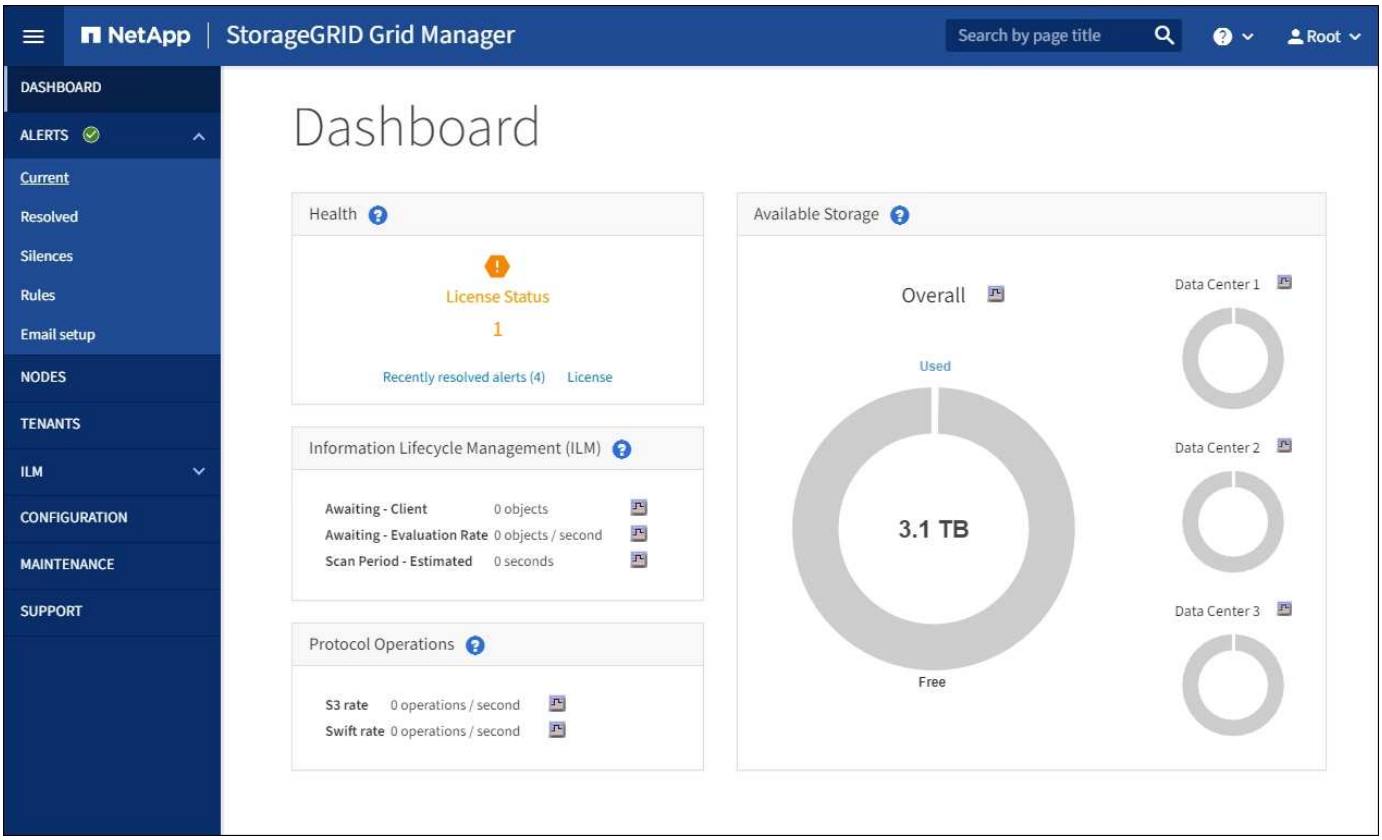
Cuando inicia sesión en Grid Manager, se conecta a un nodo de administración. Cada sistema StorageGRID incluye un nodo de administrador primario y cualquier número de nodos de administrador que no son primarios. Puede conectarse a cualquier nodo de administrador y cada nodo de administrador muestra una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

La consola incluye información resumida sobre el estado del sistema, el uso del almacenamiento, los procesos del ILM y las operaciones de S3 y Swift.



Para obtener una explicación de la información de cada panel, haga clic en el icono de ayuda para ese panel.

Leer más

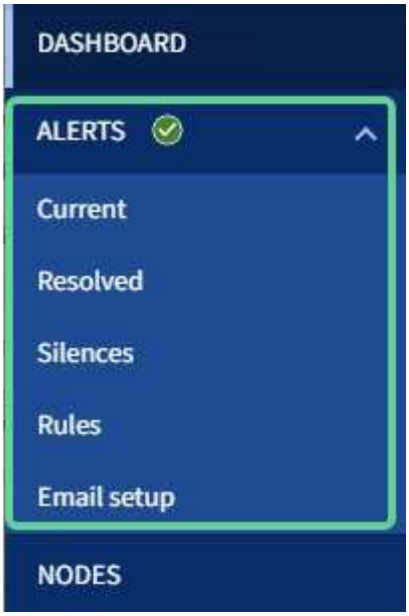
- Supervisión y solución de problemas

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 del 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 Alertas

El menú Alertas proporciona una interfaz fácil de usar para detectar, evaluar y resolver problemas que pueden producirse durante el funcionamiento de StorageGRID.



Desde el menú Alertas, puede hacer lo siguiente:

- 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

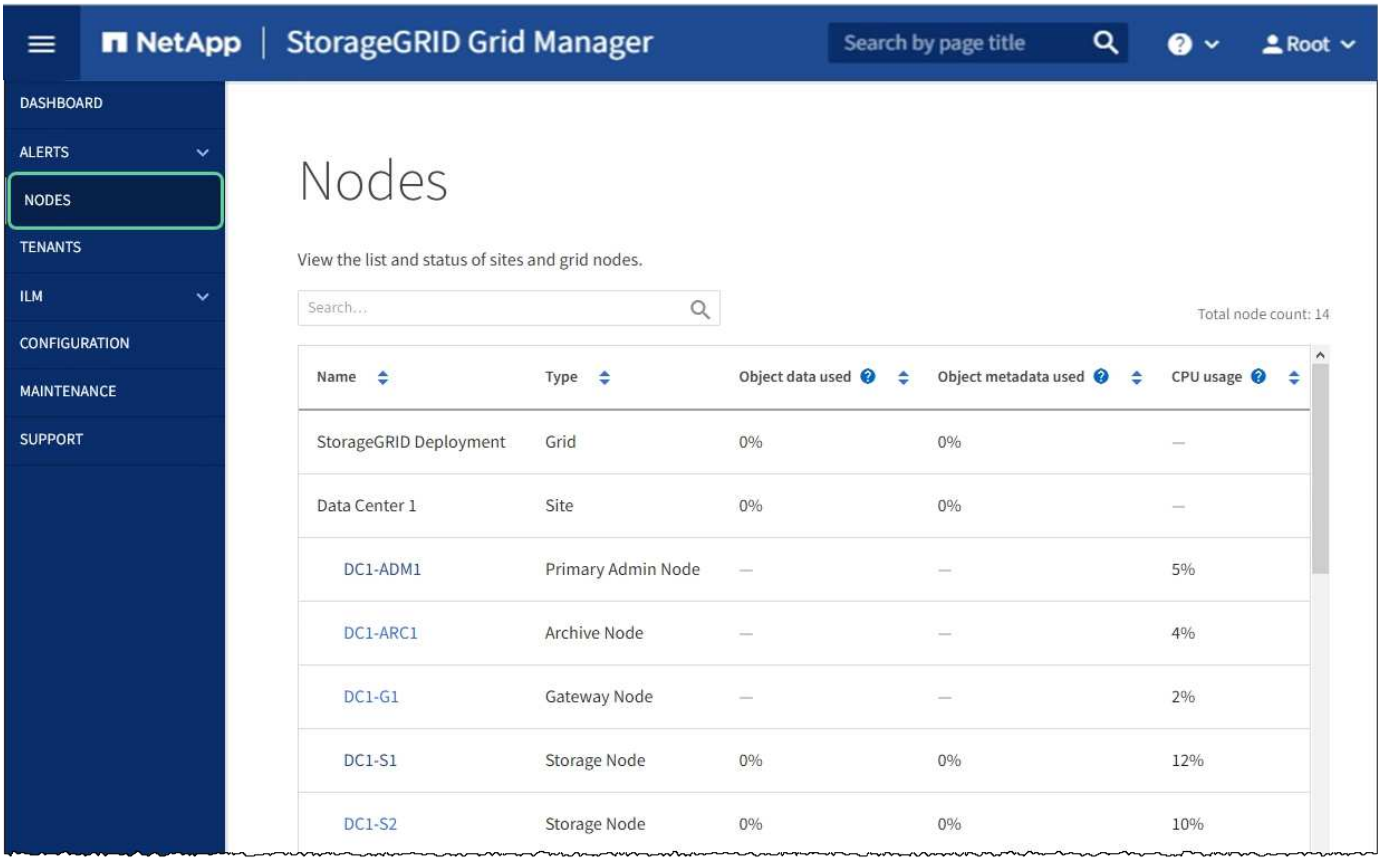
Leer más

- Supervisar y gestionar alertas
- Supervisión y solución de problemas

Nodos

La página nodos muestra información sobre la cuadrícula completa, 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.



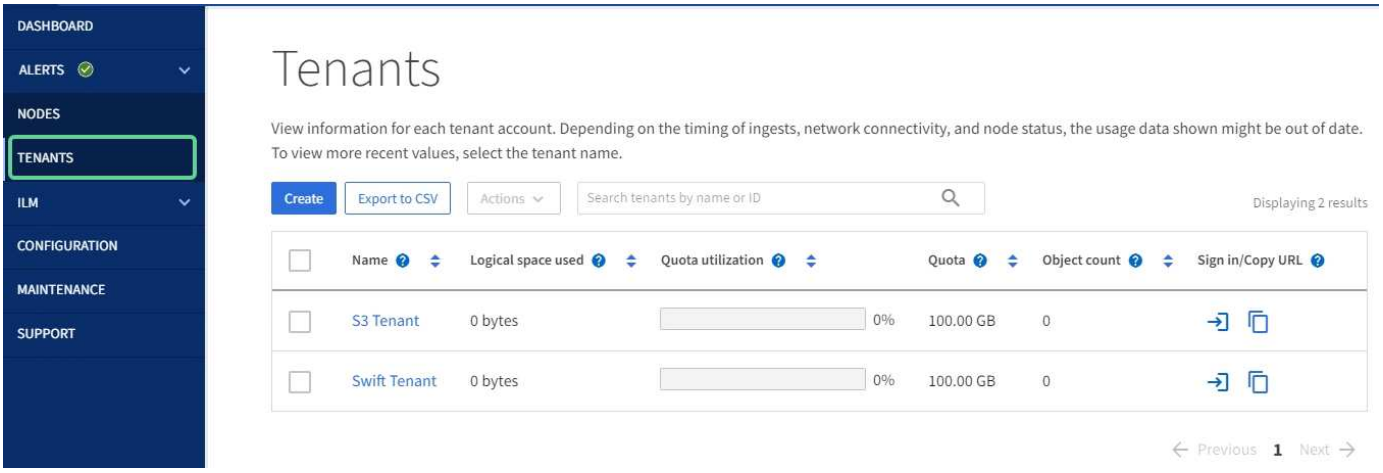
Leer más

- Vea la página Nodes
- Supervisión y solución de problemas

Inquilinos

La página Tenants permite crear y supervisar las cuentas de inquilinos de almacenamiento para el 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.



Leer más

- Gestione inquilinos y conexiones de clientes
- Administre StorageGRID
- Usar una cuenta de inquilino

Menú ILM

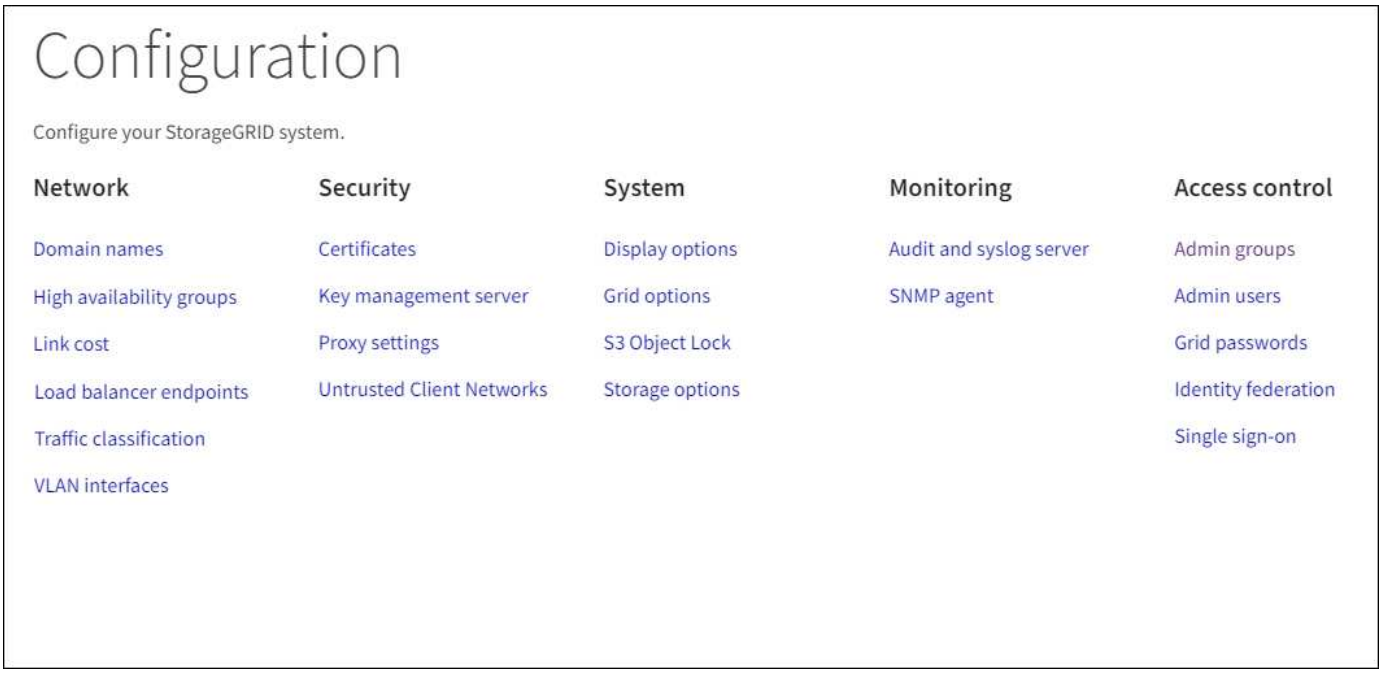
El menú ILM permite configurar las reglas y las políticas de gestión del ciclo de vida de la información (ILM) que rigen la durabilidad y la disponibilidad de los datos. También puede introducir un identificador de objeto para ver los metadatos de ese objeto.

Leer más

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

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.

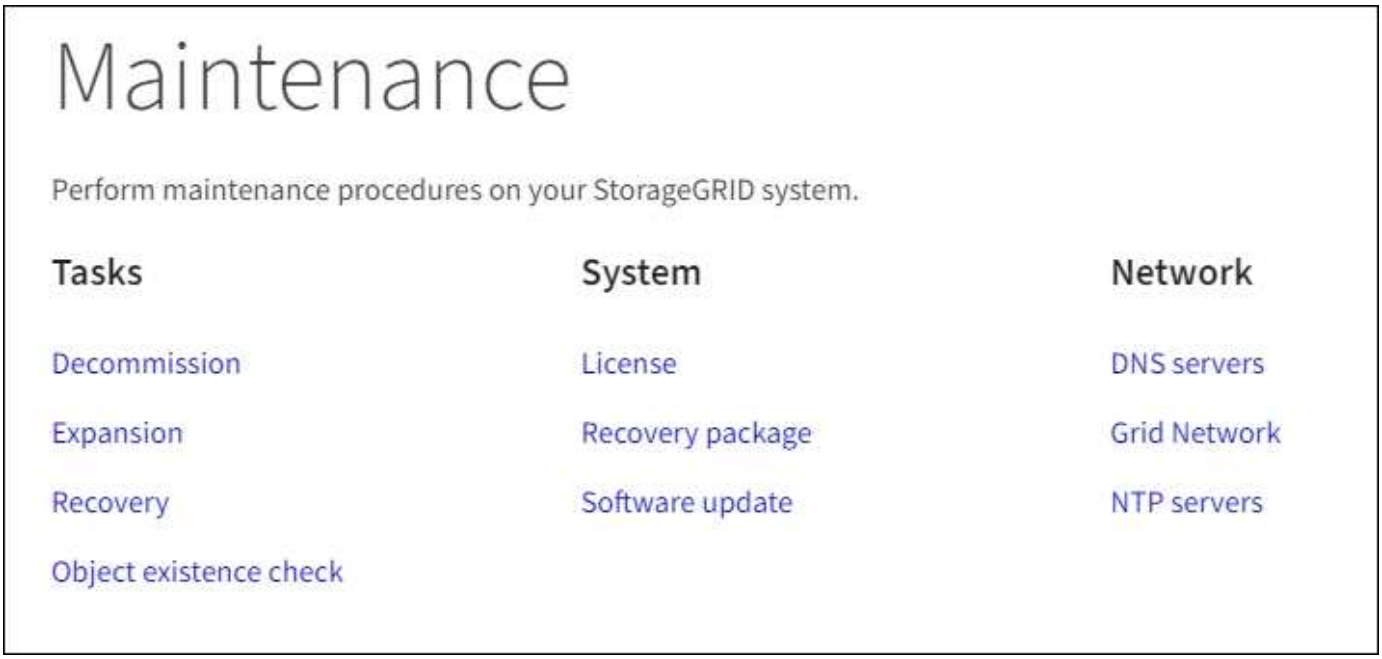


Leer más

- Configure los ajustes de red
- Gestione inquilinos y conexiones de clientes
- Revisar los mensajes de auditoría
- Control del acceso a StorageGRID
- Administre StorageGRID
- Supervisión y solución de problemas
- Revisar los registros de auditoría

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:

- Retirada de operaciones para eliminar sitios y nodos de grid no utilizados.
- Operaciones de ampliación para añadir nuevos sitios y nodos de grid.
- Operaciones de recuperación para reemplazar un nodo con fallos y restaurar datos.
- Comprobación de la existencia del objeto para verificar la existencia (aunque no la corrección) de los datos del objeto.

Sistema

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

- Consulta de detalles de la licencia de StorageGRID actual o carga de una nueva licencia.
- Generación de un paquete de recuperación.
- Realizar actualizaciones del software StorageGRID, incluidas actualizaciones de software, correcciones urgentes y actualizaciones del software de sistema operativo SANtricity en dispositivos seleccionados.

Red

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

- Edición de información sobre servidores DNS.
- Configurar las subredes utilizadas en la red de cuadrícula.
- Editar información sobre los servidores NTP.

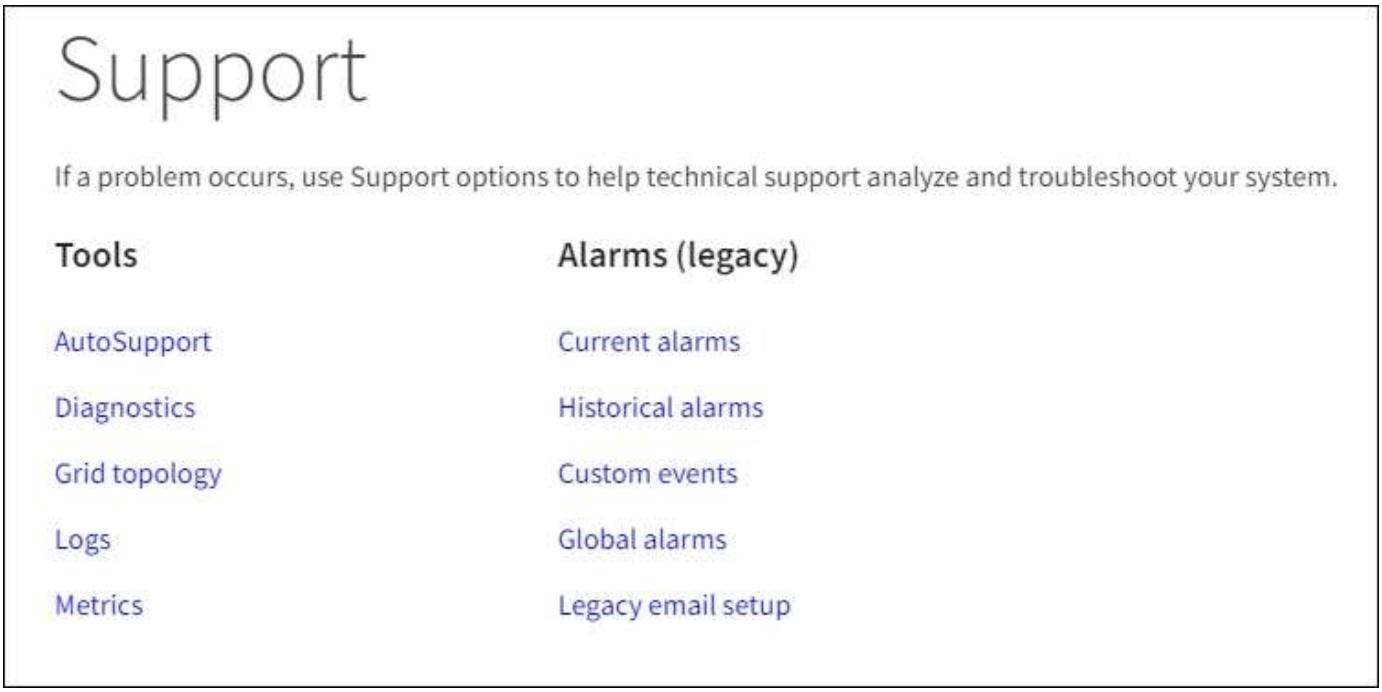
Leer más

- Realizar el mantenimiento
- Descargue el paquete de recuperación

- Amplíe su grid
- Actualizar el software de
- Recuperación y mantenimiento
- Dispositivos de almacenamiento SG6000
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG5600

Menú de soporte

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



Herramientas

En la sección Herramientas del menú Soporte, puede:

- Habilite AutoSupport.
- Realice un conjunto de comprobaciones de diagnóstico en el estado actual de la cuadrícula.
- Acceda al árbol de topología de la cuadrícula para ver información detallada sobre los nodos de la cuadrícula, los servicios y los atributos.
- Recuperar los archivos de registro y los datos del sistema.
- Revise las métricas y los gráficos detallados.

> 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)

En la sección Alarmas (heredadas) del menú Soporte, puede revisar las alarmas actuales, históricas y globales, configurar eventos personalizados y configurar notificaciones por correo electrónico para alarmas heredadas y AutoSupport.

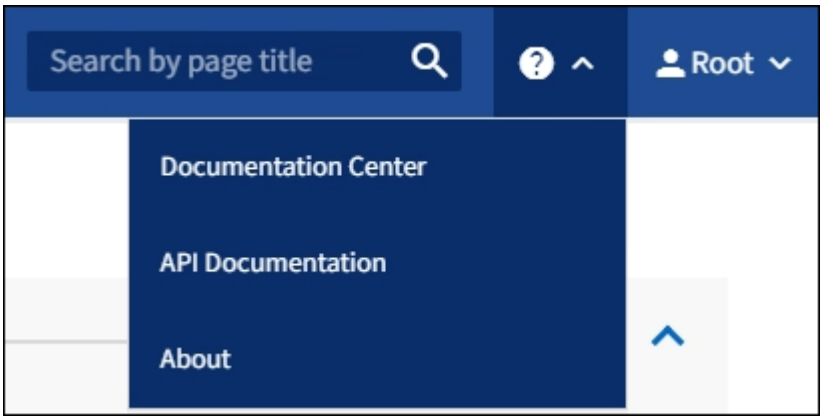
> Aunque el sistema de alarma heredado sigue siendo compatible, el sistema de alerta ofrece importantes ventajas y es más fácil de usar.

Leer más

- Arquitectura de StorageGRID y topología de red
- Atributos de la StorageGRID
- Use las opciones de soporte de StorageGRID
- Administre StorageGRID
- Supervisión y solución de problemas

Menú de ayuda

La opción Ayuda proporciona acceso al centro de documentación de StorageGRID para la versión actual y a la documentación de API. También puede determinar qué versión de StorageGRID está instalada actualmente.



Leer más

- Administre StorageGRID

Explore el responsable de inquilinos

El 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.

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

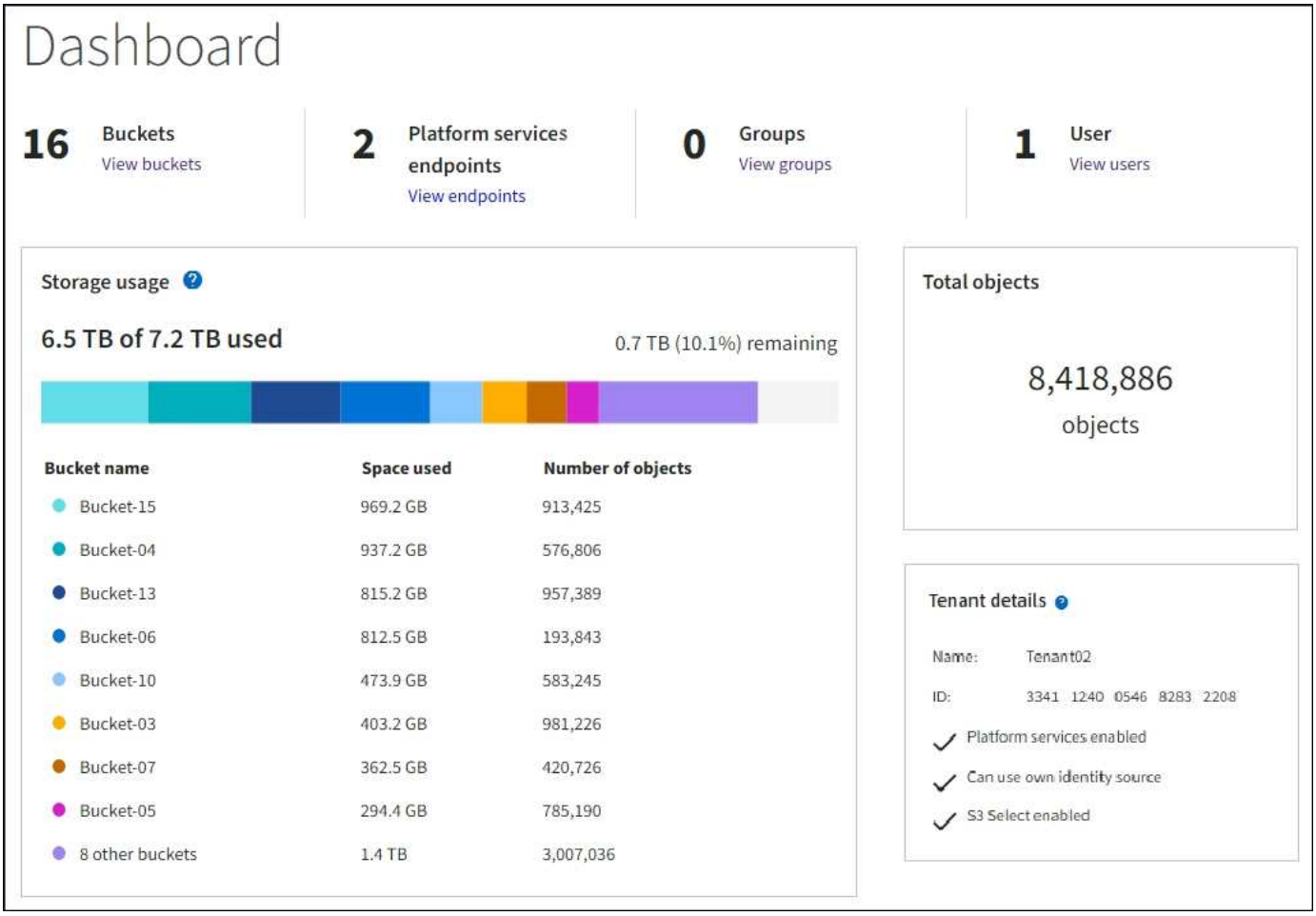
Consola de tenant Manager

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 Gestor de inquilinos permite a los usuarios inquilinos supervisar 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 de almacenamiento (solo inquilinos de S3)

El menú Storage se proporciona únicamente para cuentas de inquilinos de S3. Este menú permite a los usuarios de S3 gestionar claves de acceso, crear y eliminar bloques, y gestionar extremos de servicio de la plataforma.

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 gestionar sus propias credenciales de S3 pueden crear o quitar sus propias claves de acceso S3.
- Los usuarios que tienen el permiso Root Access pueden gestionar las claves de acceso de la cuenta raíz de S3, su propia cuenta y el resto de 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 del inquilino S3 con los permisos adecuados pueden realizar las siguientes tareas relacionadas con los 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 la configuración de los niveles de coherencia
- Aplicar una configuración de retención predeterminada
- Configurar el uso compartido de recursos de origen cruzado (CORS)
- Activar y desactivar la configuración de la última actualización de tiempo de acceso para los segmentos que pertenecen al arrendatario
- Eliminar cubos vacíos
- Gestione los objetos de un bloque mediante el Consola de S3 de experimental

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 compatible con AWS simple Notification Service™ (SNS).
- 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.

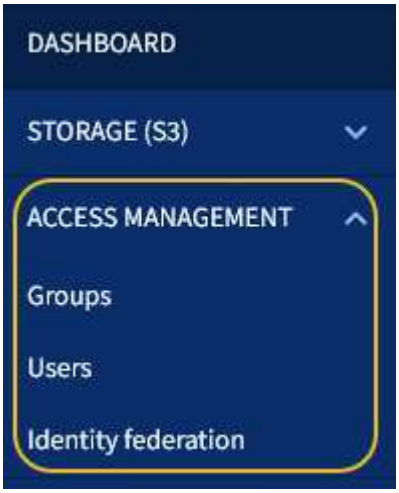
Extremos de servicios de plataforma

Si un administrador de grid habilitó 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 extremo de destino para cada servicio de plataforma.

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.



Información relacionada

- Explore Grid Manager
- Usar una cuenta de inquilino

Control del acceso a StorageGRID

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.

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. 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.

Para determinar qué tareas puede realizar cada usuario, asigne permisos diferentes 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 en la API de gestión 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). Cuando se habilita SSO, todos los usuarios deben estar autenticados por un proveedor de identidades externo antes de poder acceder a Grid Manager, al Gestor de inquilinos, a la API de gestión de grid o a la API de gestión de inquilinos. Los usuarios locales no pueden iniciar sesión en StorageGRID.

Cuando se habilita SSO y los usuarios inician sesión en StorageGRID, se redirigen a la página SSO de la organización para validar sus credenciales. Cuando los usuarios inician sesión en un nodo de administrador, se firman automáticamente todos los nodos de administración.

Cambiar contraseñas de cuadrícula

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 cambiar esta frase de contraseña según sea necesario.

Información relacionada

- Administre StorageGRID
- Usar una cuenta de inquilino

Gestione inquilinos y conexiones de clientes

Como administrador de grid, puede crear y gestionar las cuentas de inquilino que utilizan los clientes S3 y Swift para almacenar y recuperar objetos, así como gestionar las opciones de configuración que controlan la forma en la que se conectan los clientes con su sistema StorageGRID.

Cuentas de inquilino

Una cuenta de inquilino permite especificar quién puede usar su sistema de StorageGRID para almacenar y recuperar objetos, y qué funcionalidad está disponible para ellos. Las cuentas de inquilino permiten a las aplicaciones cliente que admiten la API DE REST de S3 o la API DE REST de Swift almacenar y recuperar objetos en StorageGRID. Cada cuenta de inquilino usa el protocolo de cliente S3 o el protocolo de cliente Swift.

Debe crear al menos una cuenta de inquilino para cada protocolo de cliente que se utilizará para almacenar los objetos en su sistema StorageGRID. Opcionalmente, puede crear cuentas de arrendatario adicionales si desea segregar los objetos almacenados en su sistema por entidades diferentes. Cada cuenta de inquilino tiene sus propios grupos y usuarios locales o federados, y sus propios bloques (contenedores para Swift) y objetos.

Puede utilizar Grid Manager o la API de gestión de grid para crear cuentas de inquilino. Al crear una cuenta de inquilino, especifique la siguiente información:

- Nombre para mostrar del arrendatario (el ID de cuenta del arrendatario se asigna automáticamente y no se puede modificar).
- Si la cuenta de inquilino usa S3 o Swift.
- Para las cuentas de inquilino de S3: Si la cuenta de inquilino está permitida para usar los servicios de la plataforma. Si se permite el uso de servicios de plataforma, la cuadrícula debe configurarse para que admita su uso.

- Opcionalmente, una cuota de almacenamiento para la cuenta de inquilino: El número máximo de gigabytes, terabytes o petabytes disponibles para los objetos del inquilino. La cuota de almacenamiento de un inquilino representa una cantidad lógica (tamaño de objeto), no una cantidad física (tamaño en disco).
- Si está habilitada la federación de identidades para el sistema StorageGRID, el grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.
- Si el sistema StorageGRID no utiliza el inicio de sesión único (SSO), tanto si la cuenta de inquilino usará su propio origen de identidad como si comparte el origen de identidad de la cuadrícula, así como la contraseña inicial del usuario raíz local del inquilino.

Si las cuentas de inquilinos S3 deben cumplir con los requisitos normativos, los administradores del grid pueden habilitar el valor global de bloqueo de objetos S3 para el sistema StorageGRID. Cuando se habilita S3 Object Lock para el sistema, todas las cuentas de inquilinos S3 pueden crear bloques con S3 Object Lock habilitado y, a continuación, especificar la configuración de retención y conservación legal para las versiones de objetos en ese bloque.

Después de crear una cuenta de inquilino, los usuarios de inquilino pueden iniciar sesión en el Administrador de inquilinos.

Conexiones cliente a los nodos StorageGRID

Para que los usuarios inquilinos puedan usar clientes S3 o Swift para almacenar y recuperar datos en StorageGRID, debe decidir cómo se conectan estos clientes a los nodos de StorageGRID.

Las aplicaciones cliente pueden almacenar o recuperar objetos conectándose a cualquiera de los siguientes elementos:

- El servicio Load Balancer en nodos de administrador o nodos de puerta de enlace. Esta es la conexión recomendada.
- El servicio CLB en los nodos de puerta de enlace.

  El servicio CLB está obsoleto.

- Nodos de almacenamiento, con o sin un equilibrador de carga externo.

Al configurar StorageGRID para que los clientes puedan utilizar el servicio Load Balancer, debe realizar los siguientes pasos:

1. Opcionalmente, configure los grupos de alta disponibilidad. Si crea un grupo de alta disponibilidad, las interfaces de varios nodos de administrador y nodos de puerta de enlace se colocan en una configuración de backup activo. Las conexiones de clientes se realizan mediante la dirección IP virtual del grupo de alta disponibilidad.
2. Configure los extremos para el servicio Load Balancer. El servicio Load Balancer en los nodos de administrador o de puerta de enlace distribuye conexiones de red entrantes desde aplicaciones cliente hasta los nodos de almacenamiento. Al crear un extremo de equilibrio de carga, especifica un número de puerto, si el extremo acepta conexiones HTTP o HTTPS, el tipo de cliente (S3 o Swift) que utilizará el extremo y el certificado que se utilizará para las conexiones HTTPS (si procede).
3. Opcionalmente, especifique que la red de cliente de un nodo no es de confianza para asegurarse de que todas las conexiones a la red de cliente del nodo se producen en los extremos del equilibrador de carga.

Información relacionada

- Administre StorageGRID

- Usar una cuenta de inquilino
- Use S3
- Use Swift
- Explore el responsable de inquilinos
- Configure los ajustes de red

Configure los ajustes de red

Puede configurar varios ajustes de red desde el Gestor de cuadrícula para ajustar el funcionamiento del sistema StorageGRID.

Nombres de dominio

Si piensa admitir solicitudes virtuales de estilo alojado en S3, debe configurar la lista de nombres de dominio de extremo a los que se conectan los clientes S3. Los ejemplos incluyen `s3.example.com`, `s3.example.co.uk`, y. `s3-east.example.com`.

Los certificados de servidor configurados deben coincidir con los nombres de dominio de extremo.

Grupos 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.

Cuando se crea un grupo de alta disponibilidad, se selecciona una interfaz de red para uno o varios nodos. Cada grupo de alta disponibilidad proporciona acceso a los servicios compartidos en los nodos seleccionados.

- Los grupos de ALTA DISPONIBILIDAD que incluyen interfaces en nodos de puerta de enlace, nodos de administrador o en ambos proporcionan conexiones de datos de alta disponibilidad para clientes S3 y Swift.
- Los grupos DE ALTA DISPONIBILIDAD que incluyen interfaces en los nodos de administración sólo proporcionan conexiones de alta disponibilidad con el administrador de grid y el administrador de inquilinos.

Las interfaces pueden pertenecer a la red de cuadrícula (eth0), a la red de cliente (eth2) o a una red VLAN.

Puede asignar hasta 10 direcciones IP virtuales (VIP) a cada grupo de alta disponibilidad. Se especifica una interfaz para que sea la interfaz principal y se clasifican las demás interfaces en orden de prioridad. La interfaz Primary es la interfaz activa a menos que se produzca un fallo. Si la interfaz activa falla, las direcciones 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.

Enlazar costes

Puede ajustar los costes de enlace para reflejar la latencia entre los sitios. Cuando existen dos o más centros de datos, los costes de enlace priorizan qué sitio del centro de datos debe proporcionar un servicio solicitado.

Puntos finales del equilibrador de carga

Puede utilizar un equilibrio de carga para gestionar cargas de trabajo de procesamiento y recuperación de clientes S3 y Swift. El equilibrio de carga maximiza la velocidad y la capacidad de conexión distribuyendo las cargas de trabajo y las conexiones entre varios nodos de almacenamiento.

Si desea utilizar el servicio de equilibrador de carga StorageGRID, que se incluye en los nodos de administración y de puerta de enlace, debe configurar uno o más puntos finales de equilibrador de carga. Cada extremo define un puerto de nodo de puerta de enlace o nodo de administrador para solicitudes S3 y Swift a nodos de almacenamiento.

Clasificación de tráfico

Puede crear políticas de clasificación de tráfico para identificar y manejar diferentes tipos de tráfico de red, incluido el tráfico relacionado con bloques específicos, inquilinos, subredes de clientes o extremos de equilibrador de carga. Estas políticas pueden ayudar a limitar y supervisar el tráfico.

Interfaces VLAN

Puede crear interfaces de LAN virtual (VLAN) para aislar y dividir el tráfico para obtener seguridad, flexibilidad y 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.

Por ejemplo, la red puede utilizar VLAN 100 para el tráfico FabricPool y VLAN 200 para una aplicación de archivado.

Información relacionada

- Administre StorageGRID
- Gestione inquilinos y conexiones de clientes

Configurar los ajustes de seguridad

Puede configurar varias opciones de seguridad desde Grid Manager para ayudar a proteger el sistema StorageGRID.

Certificados

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 solas. Los certificados de cliente no cifran datos.

Puede ver todos los certificados StorageGRID en la página **CONFIGURACIÓN** > **Seguridad** > **certificados**.

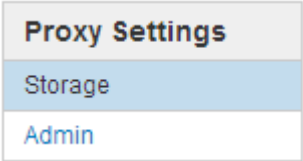
Servidores de gestión de claves

Puede configurar uno o más servidores de gestión de claves externos (KMS) para proporcionar claves de cifrado a los servicios de StorageGRID y a los dispositivos de almacenamiento. Cada clúster de KMS o KMS utiliza el protocolo de interoperabilidad de gestión de claves (KMIP) para proporcionar una clave de cifrado a los nodos de los dispositivos en el sitio StorageGRID asociado. El uso de servidores de gestión de claves le permite proteger los datos de StorageGRID aunque un dispositivo se haya eliminado del centro de datos. Una vez que los volúmenes del dispositivo se han cifrado, no podrá acceder a ningún dato en el 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.

Configuración de proxy

Si utiliza servicios de plataforma S3 o Cloud Storage Pools, puede configurar un servidor proxy no transparente entre los nodos de almacenamiento y los extremos externos de S3. Si envía mensajes de AutoSupport mediante HTTPS o HTTP, puede configurar un servidor proxy no transparente entre los nodos de administrador y el soporte técnico.



Redes de clientes no confiables

Si utiliza una red cliente, puede ayudar a proteger StorageGRID de ataques hostiles especificando que la red cliente de cada nodo no es de confianza. 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.

Por ejemplo, es posible que desee que un nodo de puerta de enlace rechace todo el tráfico entrante en la red cliente excepto las solicitudes HTTPS S3. O bien, es posible que desee habilitar el tráfico saliente del servicio de plataforma S3 desde un nodo de almacenamiento, al tiempo que se evitan las conexiones entrantes a ese nodo de almacenamiento en la red cliente.

Información relacionada

- Administre StorageGRID
- Gestione inquilinos y conexiones de clientes

Configure los ajustes del sistema

Puede configurar varios ajustes del sistema desde el Gestor de cuadrícula para ajustar el funcionamiento del sistema StorageGRID.

Opciones de visualización

Las opciones de visualización le permiten especificar el período de tiempo de espera para las sesiones de usuario y suprimir notificaciones por correo electrónico para las alarmas heredadas y los mensajes de AutoSupport activados por un evento.

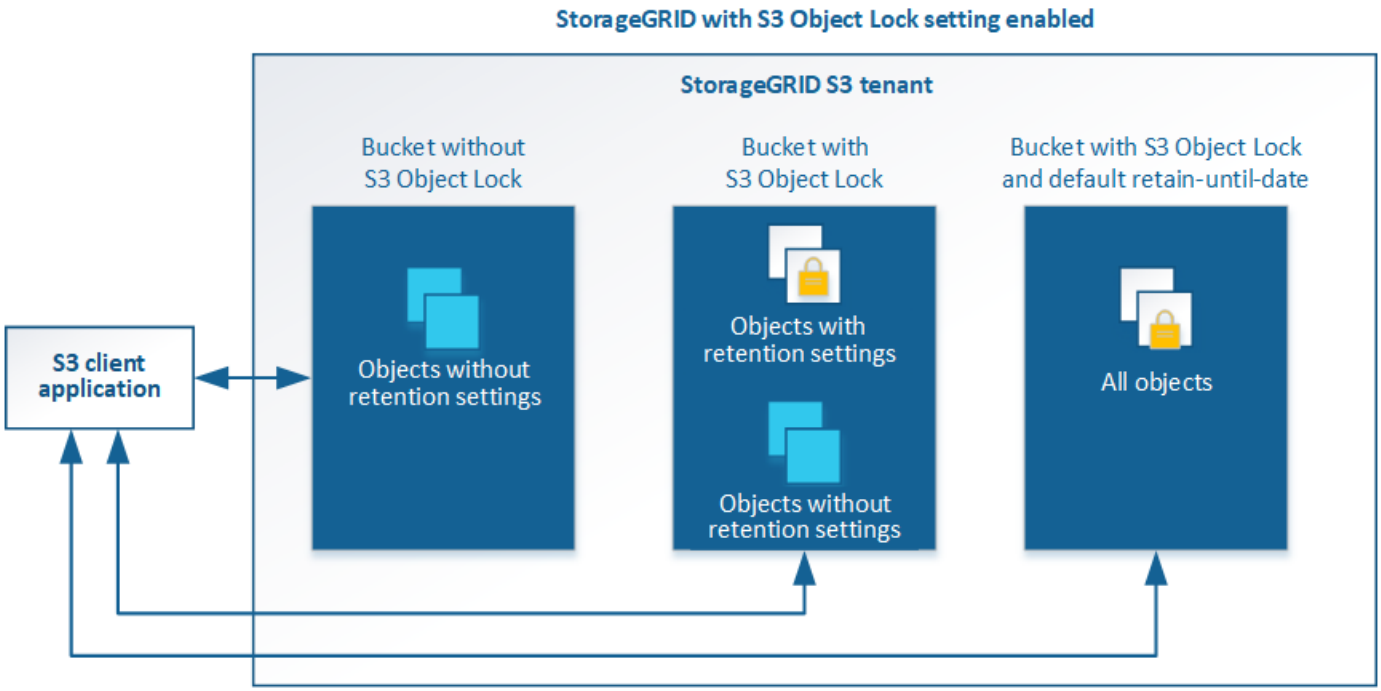
Opciones de cuadrícula

Puede utilizar Opciones de cuadrícula para configurar los valores de todos los objetos almacenados en el sistema StorageGRID, incluida la compresión de objetos almacenados, el cifrado de objetos almacenados. y hash de objetos almacenados.

También puede usar estas opciones para especificar la configuración global de las operaciones cliente de S3 y Swift.

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). Puede habilitar la configuración global de Object Lock para un sistema StorageGRID a fin de permitir que las cuentas de inquilinos S3 creen bloques con el bloqueo de objetos S3 habilitado. A continuación, el inquilino puede usar una aplicación cliente de S3 para especificar de forma opcional la configuración de retención (conservar hasta la fecha, la conservación legal o ambos) de los objetos en esos bloques. Además, cada bloque con el bloqueo de objetos S3 habilitado puede tener, de manera opcional, un modo de retención y un período de retención predeterminados, lo que se aplica si se agregan objetos al bloque sin su propia configuración de retención.



Opciones de almacenamiento

Las opciones de almacenamiento permiten controlar la segmentación de objetos y anular la configuración de Marca de agua del volumen de almacenamiento para gestionar el espacio de almacenamiento útil de un nodo de almacenamiento.

Utilizar la gestión del ciclo de vida de la información

La gestión del ciclo de vida de la información (ILM) se usa para controlar la ubicación, la duración y la protección de datos para 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.

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.

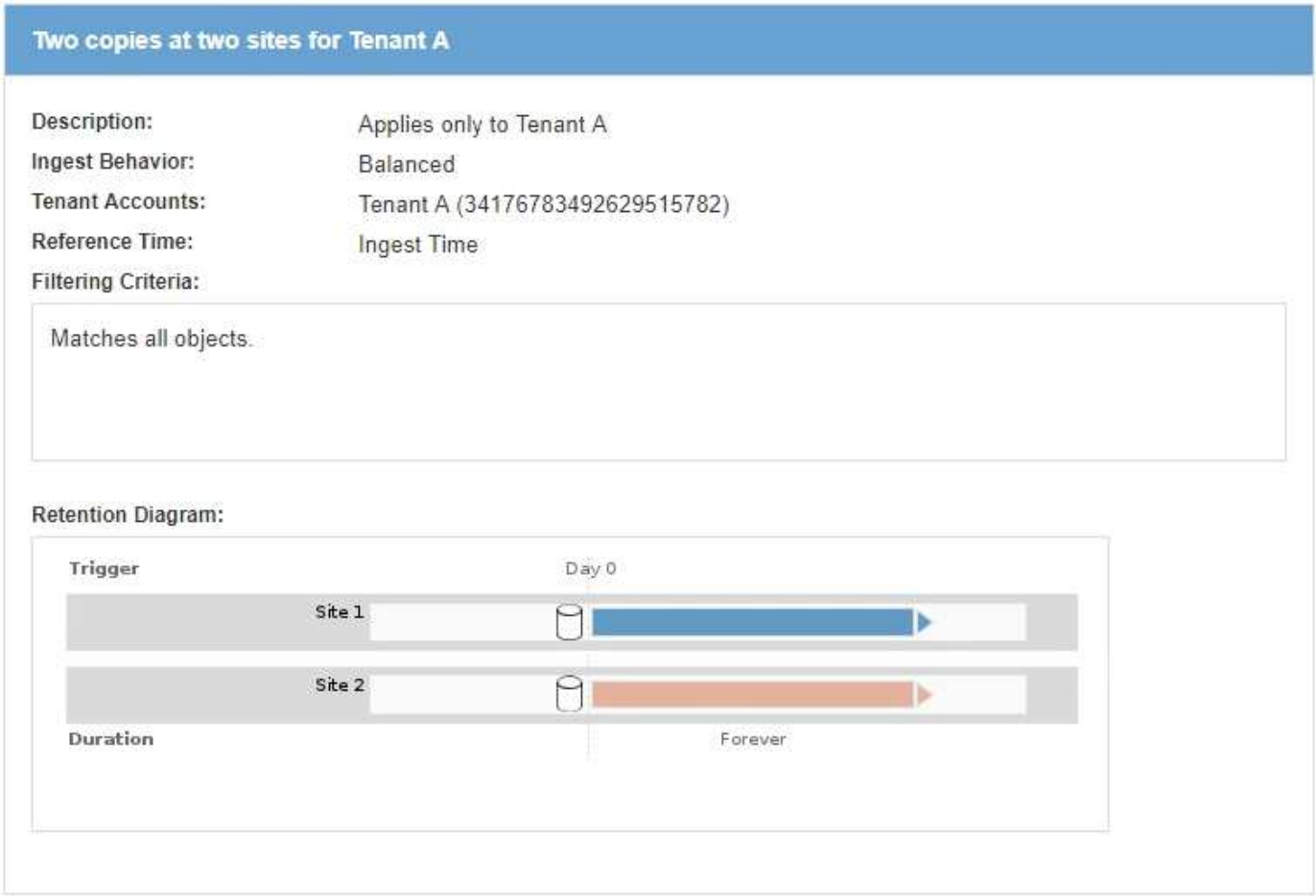
- El tipo de copias de objeto realizadas. Las copias se pueden replicar o codificar.
- Para las copias replicadas, el número de copias realizadas.
- Para las copias codificadas de borrado, se utiliza el esquema de codificación de borrado.
- Los cambios a lo largo del tiempo en la ubicación de almacenamiento 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. Las copias se distribuyen uniformemente por todos los nodos de almacenamiento.

Regla de ILM de ejemplo

Esta regla de ILM de ejemplo se aplica a los objetos que pertenecen al inquilino A. Realiza dos copias replicadas de esos objetos y almacena cada copia en un sitio diferente. Las dos copias se conservan «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.

Esta regla utiliza la opción equilibrada para el comportamiento de procesamiento: La instrucción de colocación de dos sitios se aplica tan pronto como el inquilino A guarda un objeto en StorageGRID, a menos que no sea posible realizar de inmediato ambas copias necesarias. 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

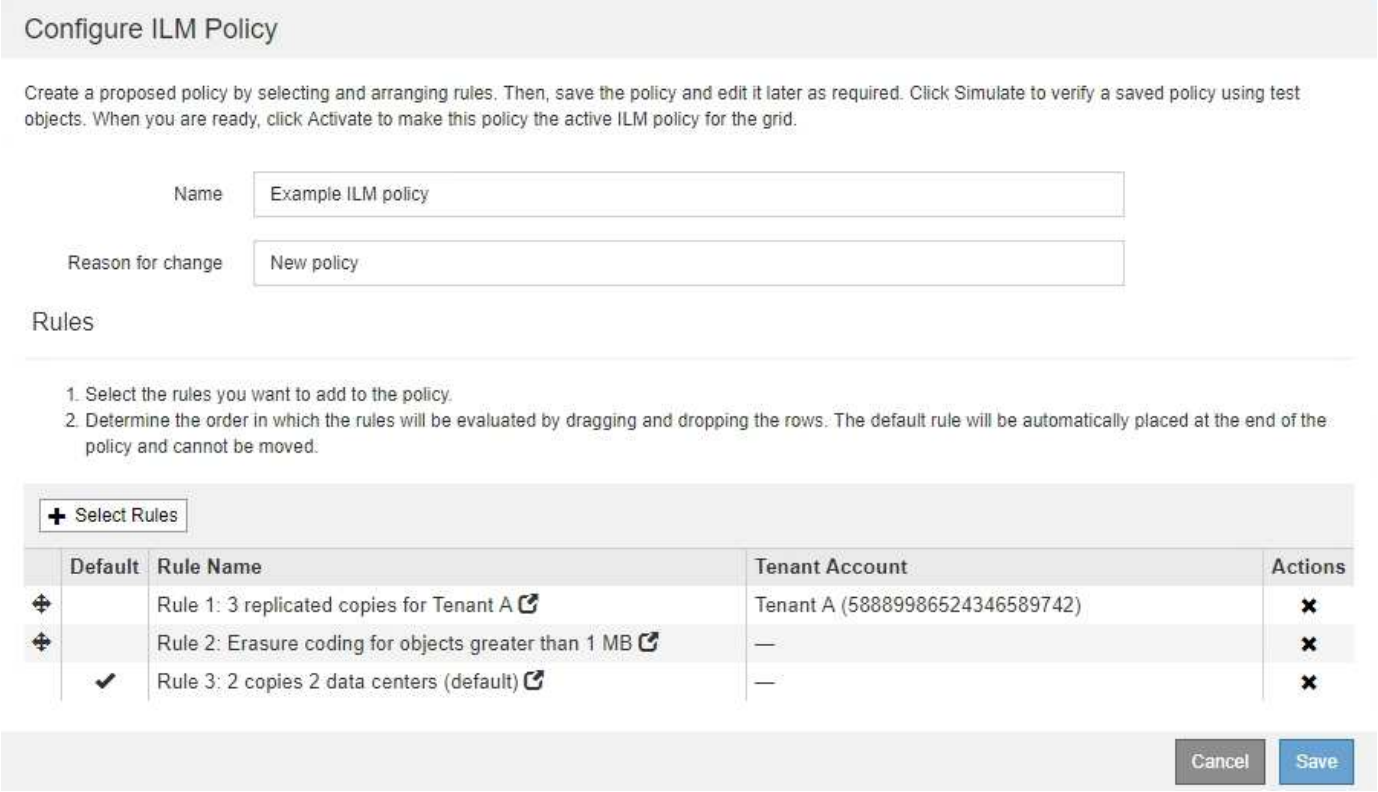
La política activa de ILM para su sistema StorageGRID controla la ubicación, la duración y la protección de datos de todos los objetos.

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 en función de cada regla posterior de la política hasta que se realice 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 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

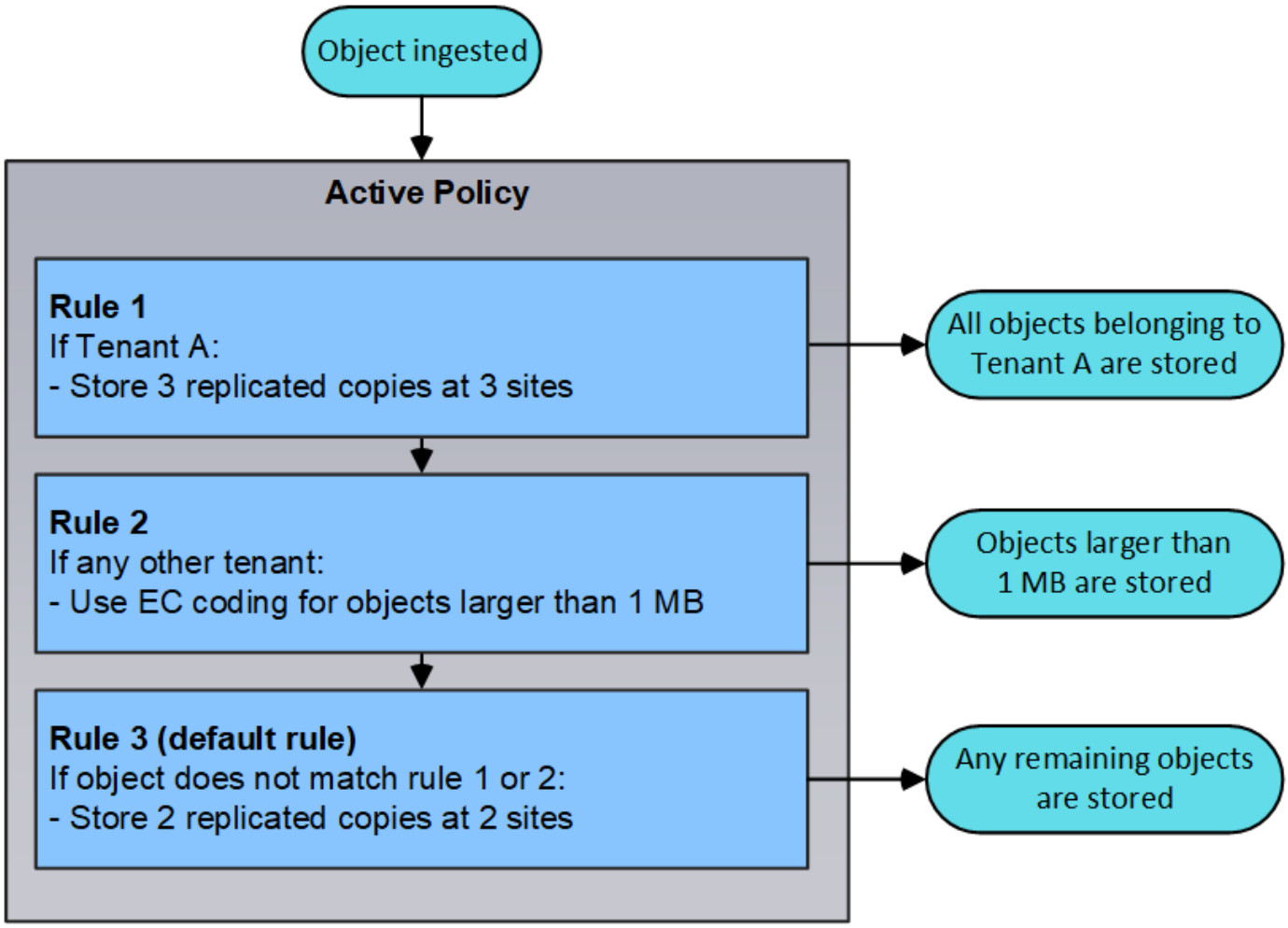
Este ejemplo de política de ILM usa tres reglas de ILM.



En este ejemplo, la regla 1 coincide con todos los objetos que pertenecen al arrendatario A. Estos objetos se almacenan como tres copias replicadas en tres sitios. Los objetos pertenecientes a otros arrendatarios no coinciden con la Regla 1, por lo que se evalúan en función de la Regla 2.

La regla 2 coincide con todos los objetos de otros arrendatarios, pero sólo si son superiores a 1 MB. Estos objetos de mayor tamaño se almacenan mediante codificación de borrado 6+3 en tres instalaciones. La regla 2 no coincide con los objetos de 1 MB o menos, por lo que estos objetos se evalúan en función de la regla 3.

La regla 3 es la última regla y la regla predeterminada de la política y no utiliza filtros. La regla 3 realiza dos copias replicadas de todos los objetos que no coinciden en la regla 1 o la regla 2 (objetos que no pertenecen al arrendatario A que son de 1 MB o menos).



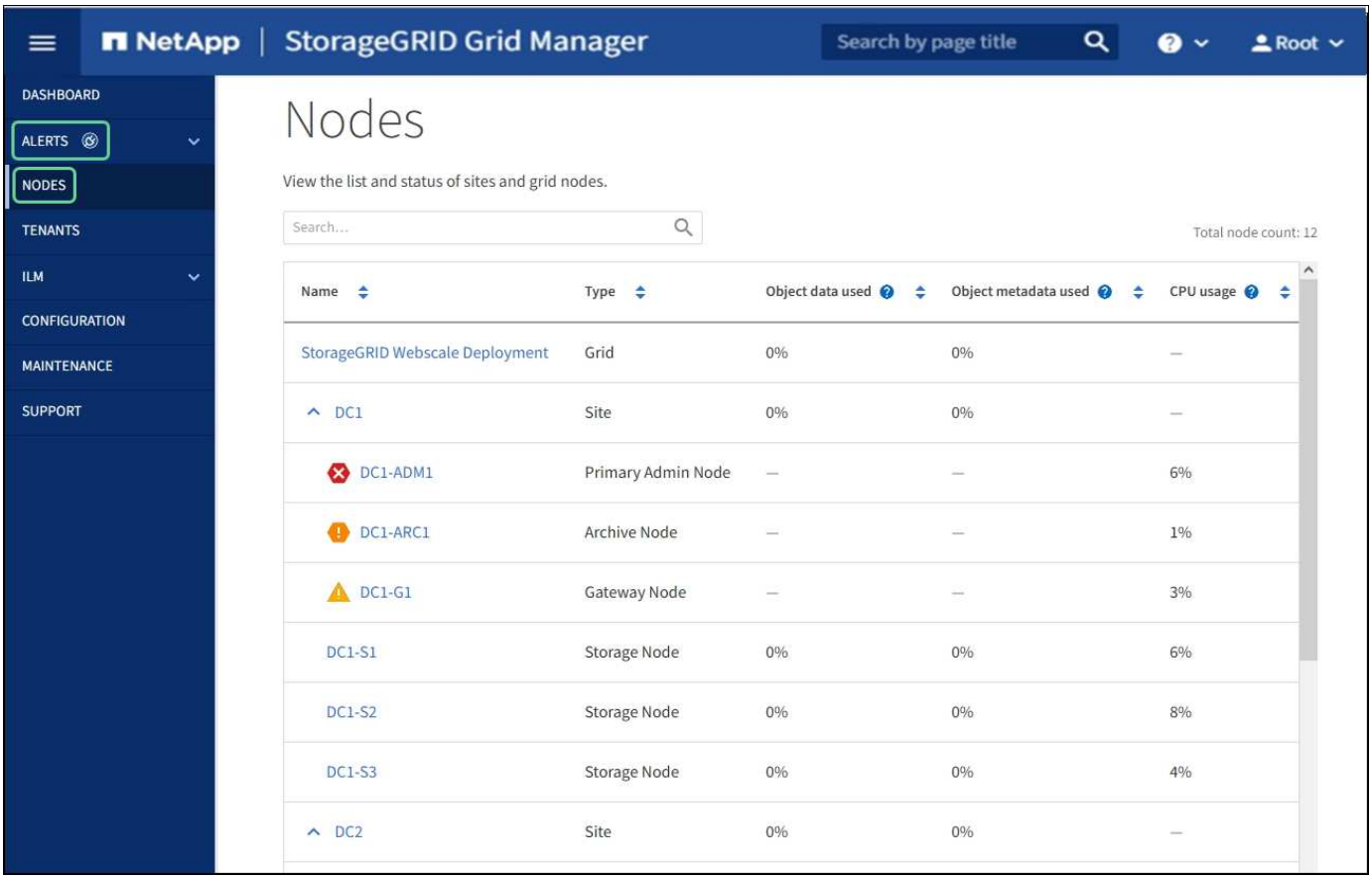
Información relacionada

- Gestión de objetos con ILM

Supervisar operaciones

Vea la página Nodes

Si necesita información más detallada sobre el sistema StorageGRID de la que proporciona la consola, puede usar la página nodos para ver métricas de toda la cuadrícula, cada sitio de la cuadrícula y cada nodo de un sitio.



En la tabla Nodes, se muestran todos los sitios y los nodos del sistema StorageGRID. La información de resumen se muestra para cada nodo. Si un nodo 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.

Iconos de estado de conexión

- **No conectado - Desconocido** : El nodo no está conectado a la cuadrícula por una razón desconocida. Por ejemplo, se ha perdido la conexión de red entre los nodos o se ha apagado el suministro eléctrico. 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.

- **No conectado - 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.

Si un nodo está desconectado de la cuadrícula, puede tener una alerta subyacente, pero sólo aparece 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

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. Deberá supervisar y resolver las alertas menores que no se despicen por sí mismas para asegurarse de que no provoquen un problema más grave.

Detalles de un sistema, sitio o nodo

Para ver la información disponible, seleccione el nombre de la cuadrícula, sitio o nodo de la siguiente manera:

- Seleccione el nombre de la cuadrícula para ver un resumen de las estadísticas de todo el sistema StorageGRID. (La captura de pantalla muestra un sistema denominado StorageGRID Deployment).
- 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.

Pestañas de la página Nodes

Las pestañas de la parte superior de la página Nodes se basan en lo que seleccione en el árbol de la izquierda.

Nombre de la ficha	Descripción	Incluido para
Descripción general	• Proporciona información básica sobre cada nodo. • Muestra las alertas activas que afectan al nodo.	Todos los nodos
Hardware subyacente	• Muestra el uso de CPU y de memoria para cada nodo • Para los nodos del dispositivo, proporciona información adicional de hardware.	Todos los nodos
Red	Muestra un gráfico que muestra el tráfico de red recibido y enviado a través de las interfaces de red. La vista de un único nodo muestra información adicional para el nodo.	Todos los nodos, cada sitio y el grid completo
Reducida	• Proporciona detalles para los dispositivos de disco y volúmenes de cada nodo. • Para los nodos de almacenamiento, cada sitio y todo el grid, incluye gráficos que muestran el almacenamiento de datos de objetos y el almacenamiento de metadatos usado con el tiempo.	Todos los nodos, cada sitio y el grid completo

Nombre de la ficha	Descripción	Incluido para
Objetos	• Proporciona información sobre las tasas de procesamiento y recuperación de S3 y Swift. • En el caso de los nodos de almacenamiento, proporciona información sobre el recuento de objetos y las consultas del almacén de metadatos y la verificación en segundo plano.	Nodos de almacenamiento, cada sitio y el grid completo
ILM	Proporciona información acerca de las operaciones de gestión del ciclo de vida de la información (ILM). • En el caso de los nodos de almacenamiento, se proporcionan detalles sobre la evaluación del ILM y la verificación en segundo plano para objetos codificados de borrado. • Muestra un gráfico de la cola de ILM a lo largo del tiempo de cada sitio y de la cuadrícula en su totalidad. • En todo el grid, ofrece el tiempo estimado para completar un análisis completo de ILM de todos los objetos.	Nodos de almacenamiento, cada sitio y el grid completo
Equilibrador de carga	Incluye gráficos de rendimiento y diagnóstico relacionados con el servicio Load Balancer. • Para cada sitio, proporciona un resumen agregado de las estadísticas para todos los nodos de ese sitio. • Para toda la cuadrícula, proporciona un resumen agregado de las estadísticas de todos los sitios.	Los nodos de administrador y de puerta de enlace, cada sitio y todo el grid
Servicios de plataforma	Proporciona información sobre cualquier operación de servicio de plataforma S3 en un sitio.	Cada sitio
System Manager de SANtricity	Ofrece acceso a SANtricity System Manager. En SANtricity System Manager, puede revisar la información de diagnóstico de hardware y entorno de la controladora de almacenamiento, así como los problemas relacionados con las unidades.	Nodos del dispositivo de almacenamiento **Nota**: La ficha Administrador del sistema de SANtricity no aparecerá si el firmware del controlador en el dispositivo de almacenamiento es anterior a 8.70 (11.70).

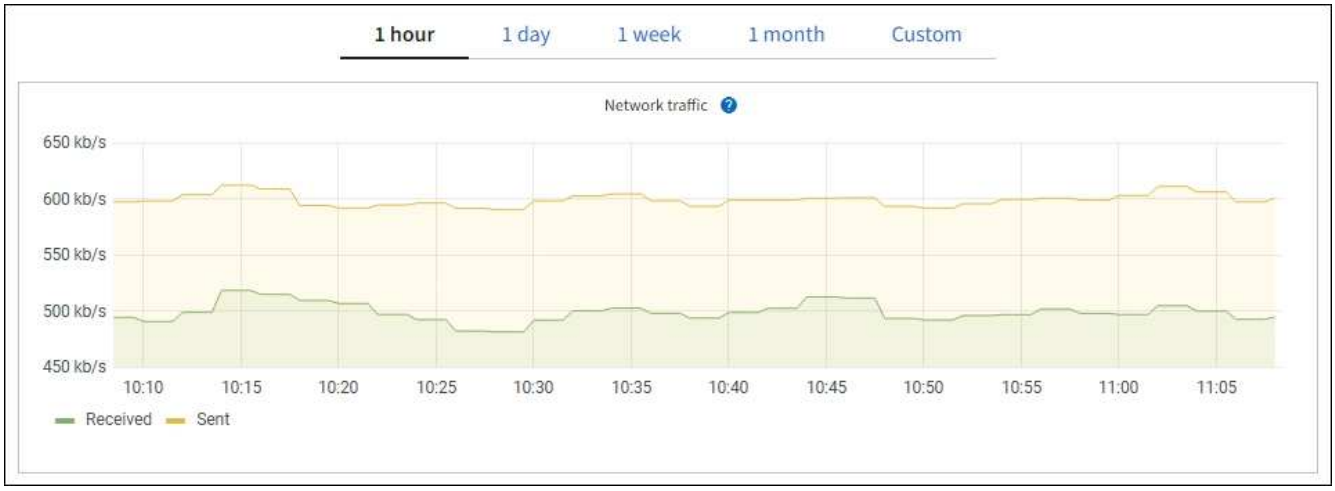
Métricas de Prometheus

El servicio Prometheus en nodos de administración recopila métricas de series temporales de los servicios de

todos los nodos.

La métrica recopilada por Prometheus se utiliza 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, seleccione el icono de ayuda y seleccione **Documentación de API** > **métricas**.) Si bien hay más de mil métricas disponibles, solo se requiere una cantidad relativamente pequeña para supervisar las operaciones de StorageGRID más importantes.

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

- La página **SUPPORT** > **Tools** > **Diagnostics** y la página **SUPPORT** > **Tools** > **Metrics**: Estas páginas, que están principalmente destinadas a ser utilizadas por el soporte técnico, proporcionan una serie de herramientas y gráficos que usan los valores de las métricas Prometheus.

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

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 StorageGRID se utilizan en varios lugares del Gestor de grid:

- **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.

Información relacionada

- Supervisión y solución de problemas
- Supervisar y gestionar alertas
- Use las opciones de soporte de StorageGRID

Supervisar y gestionar alertas

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

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 se centra en los problemas que pueden llevar a la práctica en el sistema. Se activan alertas para eventos que requieren su atención inmediata, no para eventos que se pueden ignorar de forma segura.
- Las páginas Alertas actuales y Alertas resueltas proporcionan una interfaz fácil de usar para ver los problemas actuales e históricos. Puede ordenar el listado por alertas individuales y grupos de alertas. Por ejemplo, podría ordenar todas las alertas por nodo/sitio para ver qué alertas afectan a un nodo concreto. O bien, se pueden ordenar las alertas de un grupo por tiempo activadas para encontrar la instancia más reciente de una alerta específica.
- Se agrupan varias alertas del mismo tipo en un correo electrónico para reducir el número de notificaciones. Además, se muestran varias alertas del mismo tipo como un grupo en las páginas Alertas y Alertas resueltas actuales. Puede expandir y contraer grupos de alertas para mostrar u ocultar las alertas individuales. Por ejemplo, si varios nodos informan de la alerta **no se puede comunicar con el nodo**, sólo se envía un correo electrónico y la alerta se muestra como un grupo en la página Alertas actuales.

Current Alerts Learn more

View the current alerts affecting your StorageGRID system.

Group alerts Active

Name	Severity	Time triggered	Site / Node	Status	Current values
Unable to communicate with node One or more services are unresponsive or cannot be reached by the metrics collection job.	2 Major	9 minutes ago *(newest)* 19 minutes ago *(oldest)*		2 Active	
Low root disk capacity The space available on the root disk is low.	Minor	25 minutes ago	Data Center 1 / DC1-S1-99-51	Active	Disk space available: 2.00 GB Total disk space: 21.00 GB
Expiration of server certificate for Storage API Endpoints The server certificate used for the storage API endpoints is about to expire.	Major	31 minutes ago	Data Center 1 / DC1-ADM1-99-49	Active	Days remaining: 14
Expiration of server certificate for Management Interface The server certificate used for the management interface is about to expire.	Minor	31 minutes ago	Data Center 1 / DC1-ADM1-99-49	Active	Days remaining: 30
Low installed node memory The amount of installed memory on a node is low.	8 Critical	a day ago *(newest)* a day ago *(oldest)*		8 Active	

- Las alertas utilizan nombres y descripciones intuitivos que le ayudan a entender más rápidamente el problema. Las notificaciones de alerta incluyen detalles sobre el nodo y el sitio afectado, la gravedad de alerta, la hora en la que se activó la regla de alerta y el valor actual de las métricas relacionadas con la alerta.
- Las notificaciones de alertas por correo electrónico y los listados de alertas de las páginas actuales de Alertas y Alertas resueltas ofrecen acciones recomendadas para resolver una alerta. Estas acciones recomendadas suelen incluir enlaces directos a documentación de StorageGRID para facilitar la búsqueda y el acceso a procedimientos más detallados para la solución de problemas.

Low installed node memory

The amount of installed memory on a node is low.

Recommended actions

Increase the amount of RAM available to the virtual machine or Linux host. Check the threshold value for the major alert to determine the default minimum requirement for a StorageGRID node.

See the instructions for your platform:

- VMware installation
- Red Hat Enterprise Linux or CentOS installation
- Ubuntu or Debian installation

Time triggered

2019-07-15 17:07:41 MDT *(2019-07-15 23:07:41 UTC)*

Status
Active (silence this alert)

Site / Node
Data Center 2 / DC2-S1-99-56

Severity
Critical

Total RAM size
8.38 GB

Condition
View conditions | Edit rule

Close

El sistema de alarma heredado está obsoleto. La interfaz de usuario y las API del sistema de alarma heredado se eliminarán en una versión futura. El sistema de alerta ofrece ventajas importantes y es más fácil de usar.

Gestionar alertas

Todos los usuarios de StorageGRID pueden ver alertas. Si tiene el permiso acceso raíz o Administrar alertas, también puede administrar alertas, como se indica a continuación:

- Si necesita suprimir temporalmente las notificaciones de una alerta en uno o más niveles de gravedad, puede silenciar fácilmente una regla de alerta específica durante una duración determinada. Puede silenciar una regla de alerta de toda la cuadrícula, un solo sitio o un único nodo.
- Puede editar las reglas de alerta predeterminadas si es necesario. Puede deshabilitar una regla de alerta por completo o cambiar sus condiciones de activación y duración.
- Puede crear reglas de alerta personalizadas para tener en cuenta las condiciones específicas que son relevantes para su situación y para proporcionar sus propias acciones recomendadas. Para definir las condiciones de una alerta personalizada, debe crear expresiones mediante las métricas Prometheus disponibles en la sección Metrics de la API de gestión de grid.

  Por ejemplo, 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 < 24000000000
  ```

Información relacionada

Supervisión y solución de problemas

Usar supervisión de SNMP

Si desea supervisar StorageGRID mediante el Protocolo simple de administración de red (SNMP), puede utilizar el Administrador de grid para configurar el agente SNMP.

Cada nodo StorageGRID ejecuta un agente SNMP, o un daemon, que proporciona una base de datos de información de gestión (MIB). El MIB de StorageGRID contiene definiciones de tablas y notificaciones para alertas y alarmas. Cada nodo StorageGRID también admite un subconjunto de objetos MIB-II.

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. El agente proporciona acceso MIB de solo lectura para consultas, y puede enviar dos tipos de notificaciones condicionadas por eventos a un sistema de gestión:

- **Trampas** son notificaciones enviadas por el agente SNMP que no requieren el reconocimiento del sistema de administración. 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** es similar a las trampas, pero requieren el reconocimiento del sistema de administración. 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 en los siguientes casos:

- Una alerta predeterminada o personalizada se activa en cualquier nivel de gravedad. Para suprimir las notificaciones SNMP de una alerta, debe configurar un silencio para la alerta. Las notificaciones de alerta se envían mediante el nodo de administrador que esté configurado para que sea el remitente preferido.
- Ciertas alarmas (sistema heredado) se activan a niveles de gravedad especificados o superiores.

  Las notificaciones SNMP no se envían para cada alarma ni para cada gravedad de alarma.

Información relacionada

- Supervisión y solución de problemas

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. Además, cada nodo de su grid almacena una cantidad limitada de mensajes de auditoría en un archivo de registro local (localaudit.log).

Para facilitar el acceso a los registros de auditoría, es posible configurar el acceso de clientes al recurso compartido de auditoría para NFS y CIFS (CIFS está obsoleto). 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 enviar información de auditoría almacenada en los nodos administrador y local a un servidor de syslog externo. El uso de un servidor de syslog externo puede facilitar la gestión de la información de auditoría y reducir el tráfico de red. Consulte Configurar los mensajes de auditoría y los destinos de registro si quiere más información.

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 que se encuentran disponibles para analizar los mensajes de auditoría, consulte la instrucciones para los mensajes de auditoría. Para obtener información sobre cómo configurar el acceso al cliente de auditoría, consulte Configure el acceso de los clientes de auditoría.

Información relacionada

- Revisar los registros de auditoría
- Administre StorageGRID

Realizar el mantenimiento

Realiza varios procedimientos de mantenimiento para mantener el sistema StorageGRID actualizado y garantizar que el rendimiento se realiza de forma eficiente. Grid Manager proporciona herramientas y opciones para facilitar el proceso de realización de tareas de mantenimiento.

Actualizaciones de software

Puede realizar tres tipos de actualizaciones de software desde la página actualización de software de Grid Manager:

- Actualización de software StorageGRID
- Revisión StorageGRID
- Actualización de SANtricity OS

Actualizaciones de software StorageGRID

Cuando existe una nueva versión de la función StorageGRID disponible, la página actualización de software le guiará durante el proceso de cargar el archivo necesario y actualizar el sistema StorageGRID. Debe actualizar todos los nodos de grid para todos los sitios del centro de datos desde el nodo de administración principal.

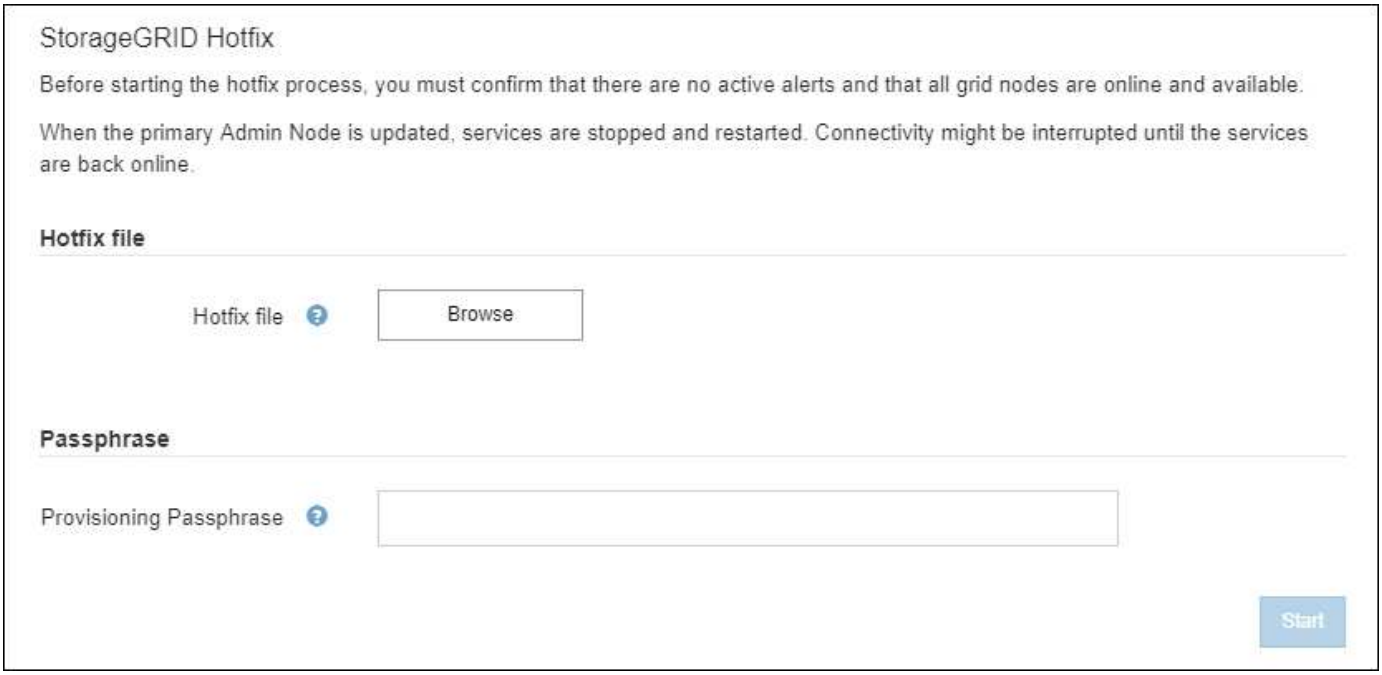
Durante una actualización del software StorageGRID, las aplicaciones cliente pueden seguir procesamiento y recuperación de datos de objetos.

Revisiones

Si se detectan y resuelven problemas con el software entre versiones de características, es posible que deba aplicar una revisión al sistema StorageGRID.

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.

La página de corrección de StorageGRID, que se muestra a continuación, permite cargar un archivo de revisión.



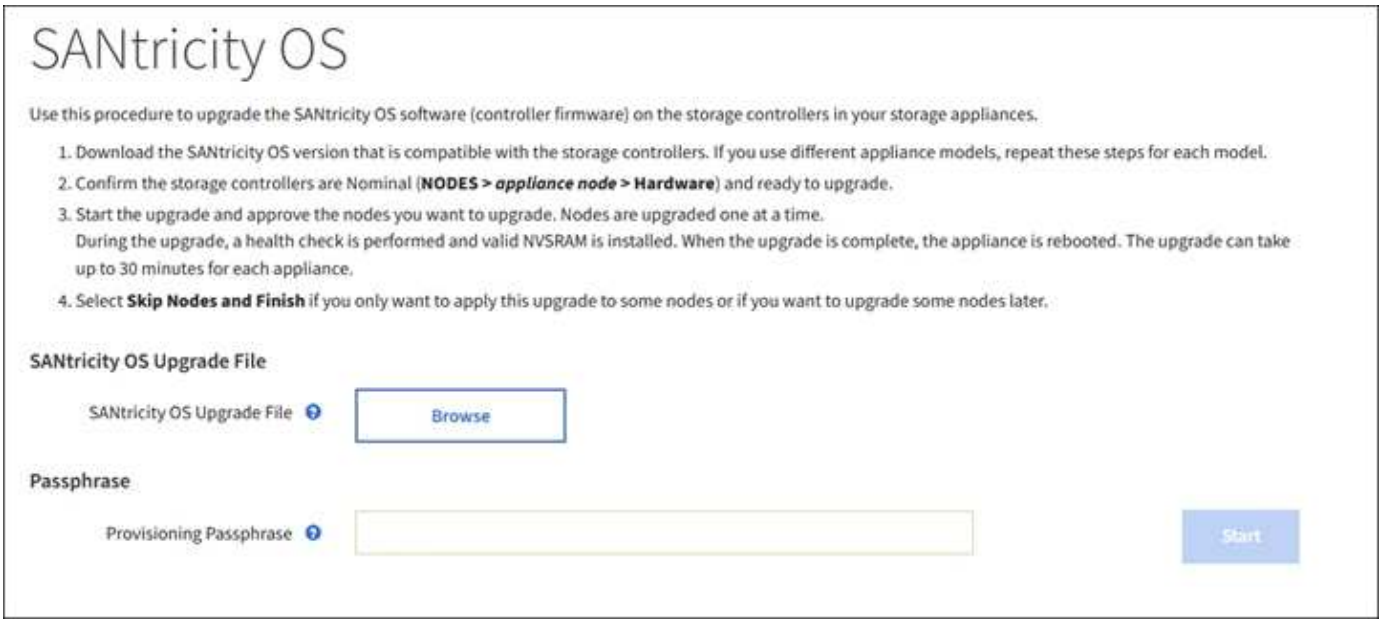
La revisión se aplica primero al nodo de administración principal. A continuación, debe aprobar la aplicación de la revisión a otros nodos de cuadrícula hasta que todos los nodos de su sistema StorageGRID ejecuten la misma versión de software. Puede personalizar la secuencia de aprobación seleccionando aprobar nodos de cuadrícula individuales, grupos de nodos de cuadrícula o todos los nodos de cuadrícula.

Mientras todos los nodos de cuadrícula se actualizan con la nueva versión de revisión, los cambios reales en una revisión sólo pueden afectar a servicios específicos de tipos de nodos específicos. Por ejemplo, una revisión sólo podría afectar al servicio LDR en nodos de almacenamiento.

Actualizaciones del sistema operativo SANtricity

Es posible que necesite actualizar el software de sistema operativo SANtricity en las controladoras de almacenamiento de sus dispositivos de almacenamiento si las controladoras no funcionan de forma óptima. Puede cargar el archivo del sistema operativo SANtricity en el nodo de administración principal del sistema StorageGRID y aplicar la actualización desde el Administrador de grid.

La página SANtricity, que se muestra a continuación, permite cargar el archivo de actualización del sistema operativo SANtricity.

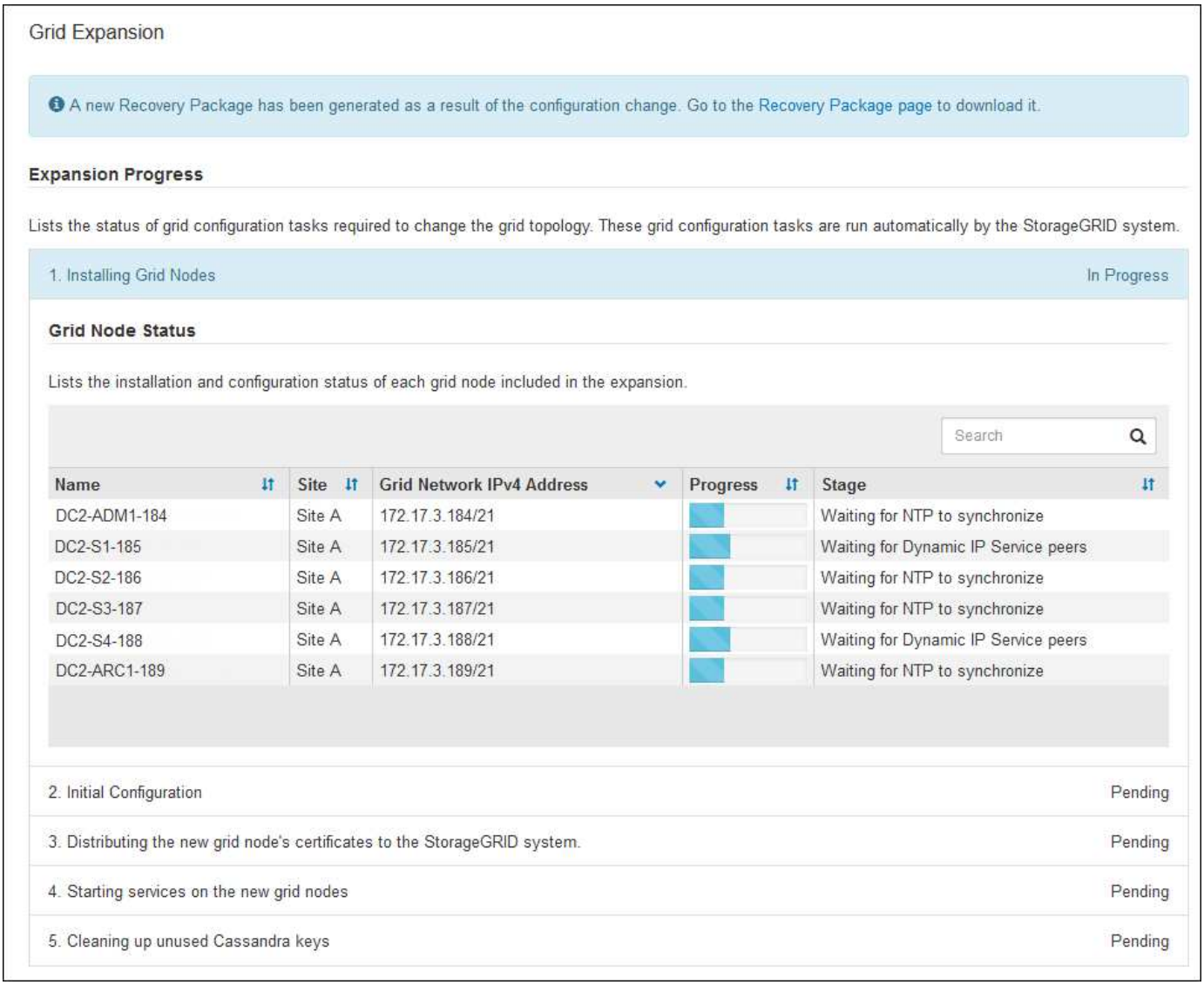


Después de cargar el archivo, puede aprobar la actualización en nodos de almacenamiento individuales o en todos los nodos. La capacidad para aprobar nodos de forma selectiva facilita la programación de la actualización. Después de aprobar un nodo para la actualización, el sistema realiza una comprobación del estado e instala la actualización si es aplicable al nodo.

Procedimientos de expansión

Puede expandir un sistema StorageGRID añadiendo volúmenes de almacenamiento a nodos de almacenamiento, agregando nuevos nodos grid a un sitio existente o añadiendo un nuevo sitio de centro de datos. Si tiene nodos de almacenamiento que usan el dispositivo de almacenamiento SG6060 o SG6060X, puede añadir una o dos bandejas de expansión al doble o triple de la capacidad de almacenamiento del nodo.

Puede realizar ampliaciones sin interrumpir el funcionamiento del sistema actual. Cuando agrega nodos o un sitio, primero implementa los nuevos nodos y después ejecuta el procedimiento de expansión desde la página expansión de cuadrícula.

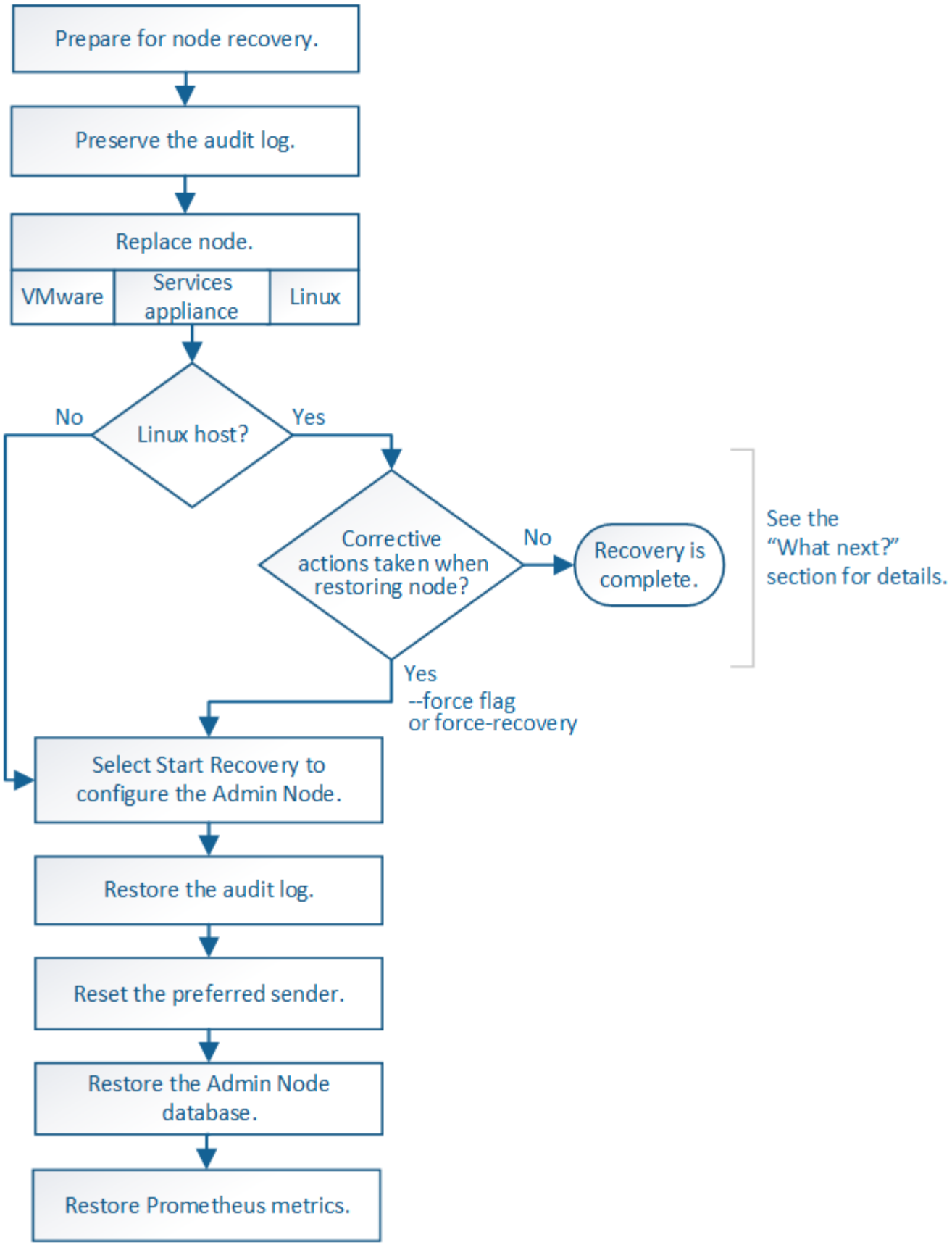


Procedimientos de recuperación de nodos

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.

Los pasos para recuperar un nodo de cuadrícula dependen de la plataforma en la que se aloje el nodo de grid y del tipo de nodo de cuadrícula. Cada tipo de nodo de cuadrícula tiene un procedimiento de recuperación específico, que se debe seguir exactamente. En general, intenta conservar los datos del nodo de cuadrícula con errores cuando es posible, reparar o reemplazar el nodo con errores, utilizar la página recuperación para configurar el nodo de sustitución y restaurar los datos del nodo.

Por ejemplo, este diagrama de flujo muestra el procedimiento de recuperación si un nodo de administración ha fallado.



Procedimientos de retirada

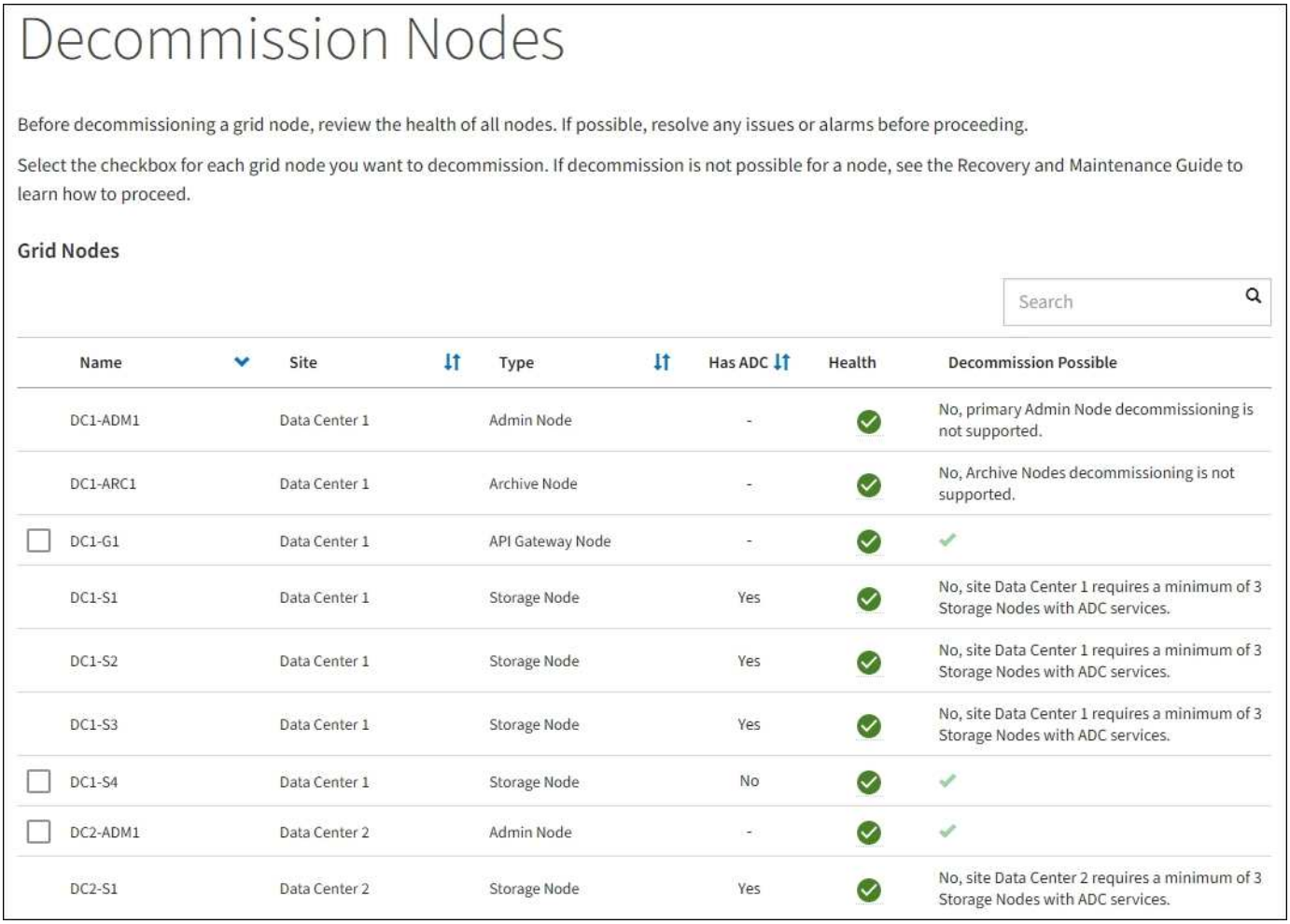
Tal vez desee eliminar de forma permanente nodos grid o un sitio de centro de datos completo de su sistema StorageGRID.

Por ejemplo, podría retirar uno o varios nodos de grid en estos casos:

- Añadió un nodo de almacenamiento de mayor tamaño al sistema y desea quitar uno o más nodos de almacenamiento más pequeños mientras conserva los objetos al mismo tiempo.
- Necesita menos almacenamiento total.
- Ya no necesita un nodo de puerta de enlace ni un nodo de administrador que no sea primario.
- El grid incluye un nodo desconectado que no se puede recuperar ni volver a conectar.

Puede utilizar la página nodos de misión no deseados en Grid Manager para eliminar los siguientes tipos de nodos de cuadrícula:

- Los nodos de almacenamiento, a menos que no haya suficientes nodos, permanecerán en el sitio para admitir ciertos requisitos
- Nodos de puerta de enlace
- Nodos de administrador no primario



Puede utilizar la página Sitio de retirada en Grid Manager para quitar un sitio. La retirada de un sitio conectado quita un sitio operativo y conserva los datos. Una retirada de sitio desconectada quita un sitio que ha fallado pero no conserva los datos. El asistente del sitio de retirada le guía a través del proceso de selección del sitio, visualización de detalles del sitio, revisión de la política de ILM, eliminación de referencias del sitio de las reglas de ILM y resolución de conflictos de nodos.

Procedimientos de mantenimiento de red

Algunos de los procedimientos de mantenimiento de red que debe realizar son los siguientes:

- Actualización de las subredes en la red de cuadrícula
- Uso de la herramienta Change IP para cambiar la configuración de red establecida inicialmente durante la implementación de grid
- Agregar, quitar o actualizar servidores de sistema de nombres de dominio (DNS)
- Agregar, eliminar o actualizar servidores de protocolo de tiempo de redes (NTP) para garantizar que los datos se sincronizan con precisión entre los nodos de grid
- Restauración de conectividad de red a los nodos que pueden haberse aislado del resto del grid

Procedimientos de middleware y a nivel de host

Algunos procedimientos de mantenimiento son específicos de los nodos StorageGRID que se implementan en Linux o VMware, o bien son específicos de otros componentes de la solución de StorageGRID. Por ejemplo, puede que desee migrar un nodo de cuadrícula a un host Linux diferente o realizar tareas de mantenimiento en un nodo de archivado conectado a Tivoli Storage Manager (TSM).

Clonado de nodos de dispositivos

El clonado de nodos de dispositivos le permite sustituir fácilmente un nodo de dispositivos existente en el grid por un dispositivo de diseño más reciente o mayores funcionalidades que forman parte del mismo sitio lógico de StorageGRID. El proceso transfiere todos los datos al dispositivo nuevo, situándolos en servicio para sustituir el nodo de dispositivo antiguo y dejar el dispositivo antiguo en estado previo a la instalación. La clonación ofrece un proceso de actualización de hardware que es fácil de ejecutar y proporciona un método alternativo para reemplazar dispositivos.

Procedimientos de los nodos de grid

Es posible que deba realizar ciertos procedimientos en un nodo de grid específico. Por ejemplo, es posible que deba reiniciar un nodo de grid o detener y reiniciar manualmente un servicio de nodo de grid específico. Algunos procedimientos de nodo de cuadrícula se pueden realizar desde Grid Manager; otros requieren que inicie sesión en el nodo de cuadrícula y que utilice la línea de comandos del nodo.

Información relacionada

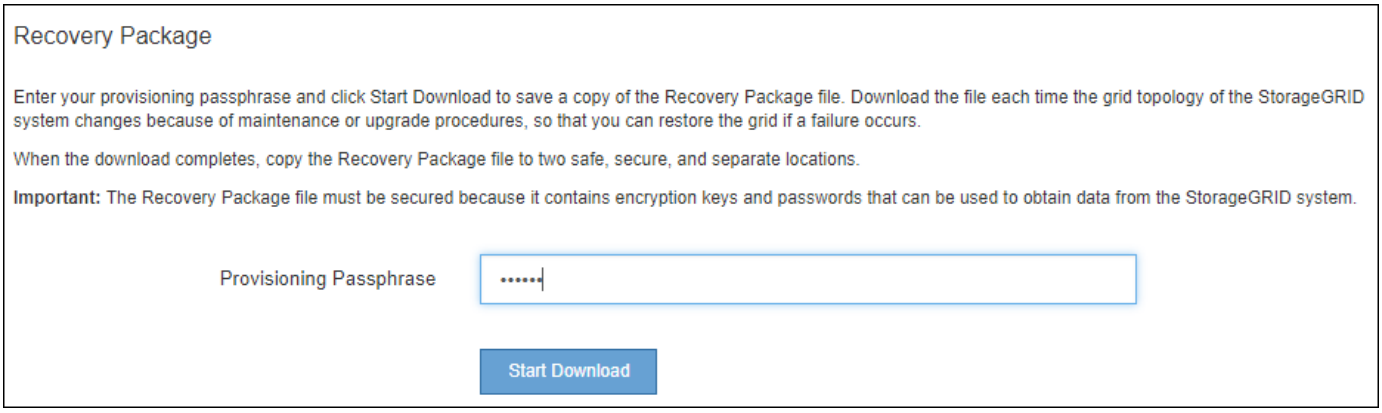
- Administre StorageGRID
- Actualizar el software de
- Amplíe su grid
- Recuperación y mantenimiento

Descargue el paquete de recuperación

El paquete de recuperación es un archivo .zip descargable que contiene archivos y software específicos de la implementación necesarios para instalar, ampliar, actualizar y mantener un sistema StorageGRID.

El archivo Recovery Package también contiene información de integración y configuración específica del sistema, incluidos los nombres de host del servidor y las direcciones IP, y contraseñas altamente confidenciales necesarias durante el mantenimiento, la actualización y la expansión del sistema. El paquete de recuperación es necesario para recuperarse de un error del nodo de administración principal.

Al instalar un sistema StorageGRID, es necesario descargar el archivo del paquete de recuperación y confirmar que puede acceder correctamente al contenido de este archivo. También se debe descargar el archivo cada vez que la topología de cuadrícula de los cambios del sistema StorageGRID se debe a los procedimientos de mantenimiento o actualización.



Después de descargar el archivo del paquete de recuperación y confirmar que puede extraer el contenido, copie el archivo del paquete de recuperación 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.

Información relacionada

- Actualizar el software de
- Amplíe su grid
- Recuperación y mantenimiento

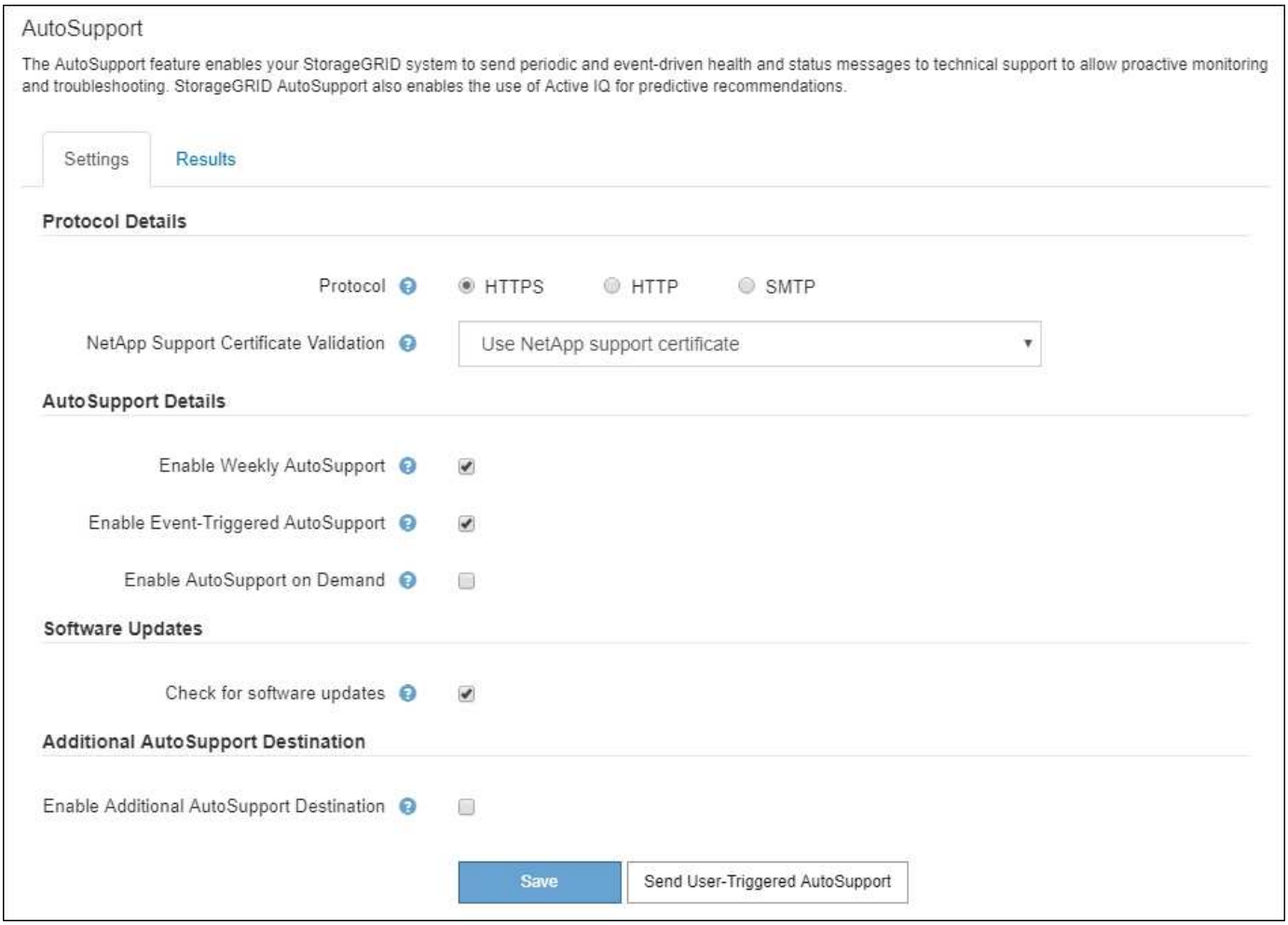
Use las opciones de soporte de StorageGRID

Grid Manager ofrece opciones para ayudarle a trabajar con el soporte técnico en caso de que surja un problema con el sistema StorageGRID.

Configure AutoSupport

La función AutoSupport permite que el sistema StorageGRID envíe mensajes de estado y estado al soporte técnico. El uso de AutoSupport puede acelerar significativamente la detección 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 los mensajes de AutoSupport para que se envíen a un destino adicional.

La configuración de AutoSupport se realiza mediante el Administrador de cuadrícula (**SUPPORT** > **Tools** > **AutoSupport**). La página **AutoSupport** tiene dos fichas: **Ajustes** y **resultados**.



Información incluida en los mensajes de AutoSupport

Los mensajes de AutoSupport incluyen información como la siguiente:

- Versión del software StorageGRID
- Versión del sistema operativo
- Información de atributos a nivel de sistema y ubicación
- Alertas y alarmas recientes (sistema heredado)
- Estado actual de todas las tareas de cuadrícula, incluidos los datos históricos
- Uso de la base de datos del nodo de administrador
- Número de objetos perdidos o faltantes
- Ajustes de configuración de cuadrícula
- Entidades NMS
- Política de ILM activa
- Archivo de especificación de grid aprovisionado
- Métricas de diagnóstico

Puede habilitar la función AutoSupport y las opciones individuales de AutoSupport cuando instale StorageGRID por primera vez, o bien puede habilitarlas más adelante. Si AutoSupport no está habilitado, aparecerá un mensaje en el Panel 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.

Utilice 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.

Debe habilitar AutoSupport si desea usar las consolas y la funcionalidad de Active IQ del sitio de soporte de NetApp.

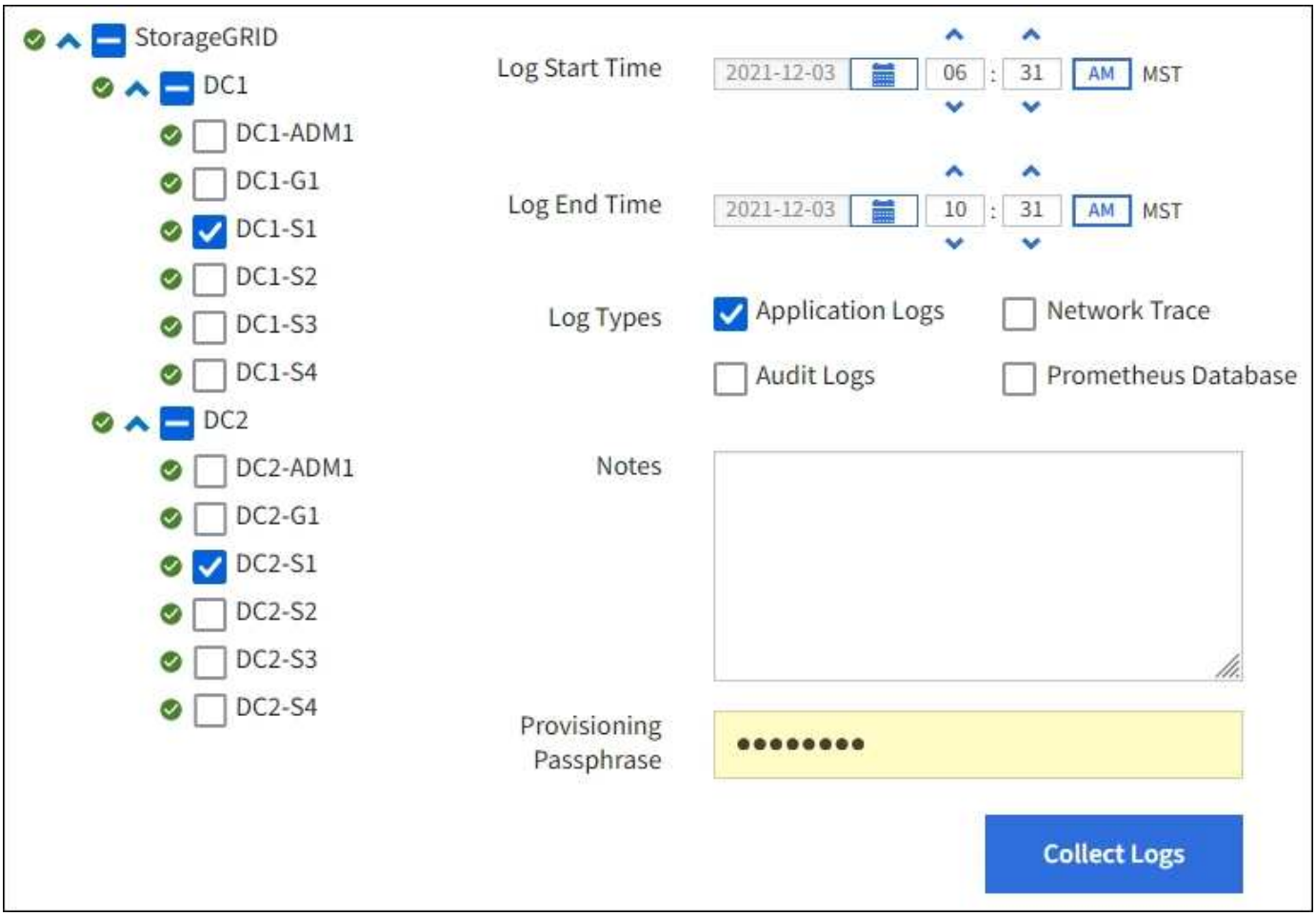
"Documentación del asesor digital de Active IQ"

Recopile registros de StorageGRID

Para ayudar a resolver un problema, es posible que deba recoger archivos de registro y reponerlos al soporte de.

StorageGRID utiliza los archivos de registro para capturar eventos, mensajes de diagnóstico y condiciones de error. El archivo bycast.log se mantiene para cada nodo de grid y es el archivo principal de solución de problemas. StorageGRID también crea archivos de registro para servicios StorageGRID individuales, archivos de registro relacionados con actividades de implementación y mantenimiento y archivos de registro relacionados con aplicaciones de terceros.

Los usuarios que dispongan de los permisos adecuados y que conozcan la contraseña de acceso de aprovisionamiento para el sistema StorageGRID pueden utilizar la página registros en el administrador de grid para recopilar archivos de registro, datos del sistema y datos de configuración. Cuando recoja registros, seleccione un nodo o nodos y especifique un período de tiempo. Los datos se recogen y archivan en un `.tar.gz` archivo, que puede descargar en un equipo local. Dentro de este archivo hay un archivo de registro para cada nodo de cuadrícula.



Utilice métricas y ejecute diagnósticos

Al solucionar problemas, puede trabajar con el soporte técnico para revisar métricas y gráficos detallados para su sistema StorageGRID. También puede ejecutar consultas de diagnóstico prediseñadas para evaluar de forma proactiva valores clave en su sistema StorageGRID.

Página de métricas

La página Metrics proporciona acceso a las interfaces de usuario de 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.

Metrics

Access charts and metrics to help troubleshoot issues.

The tools available on this page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

Prometheus

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time.

Access the Prometheus UI using the link below. You must be signed in to the Grid Manager.

- https://[illegible]/metrics/graph

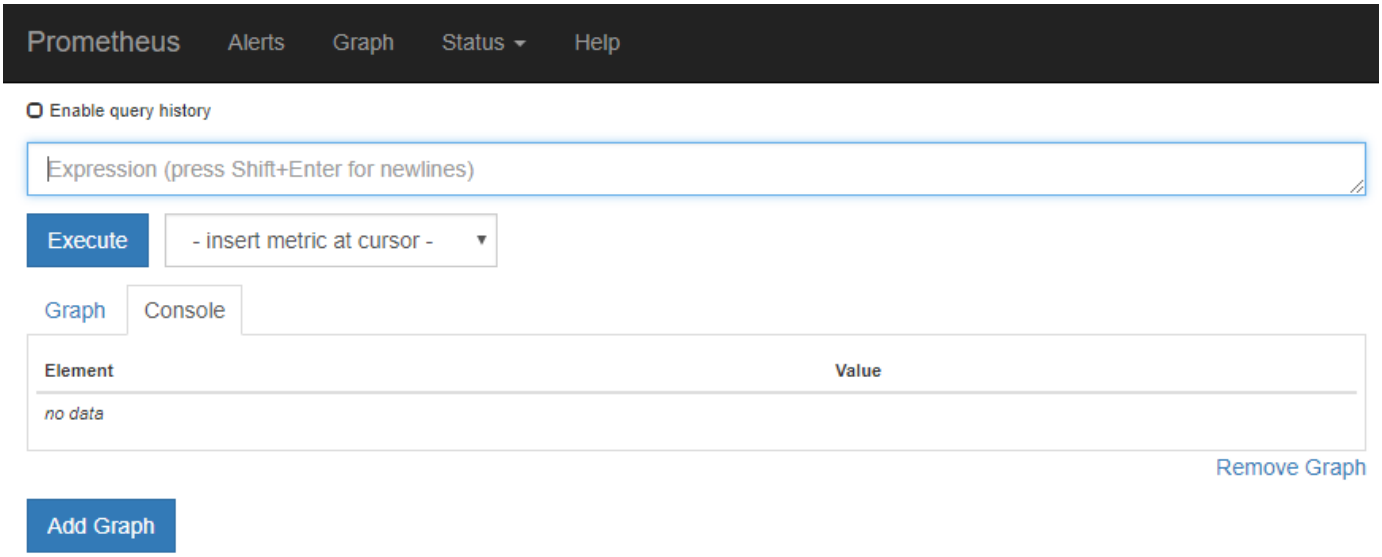
Grafana

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values over time.

Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

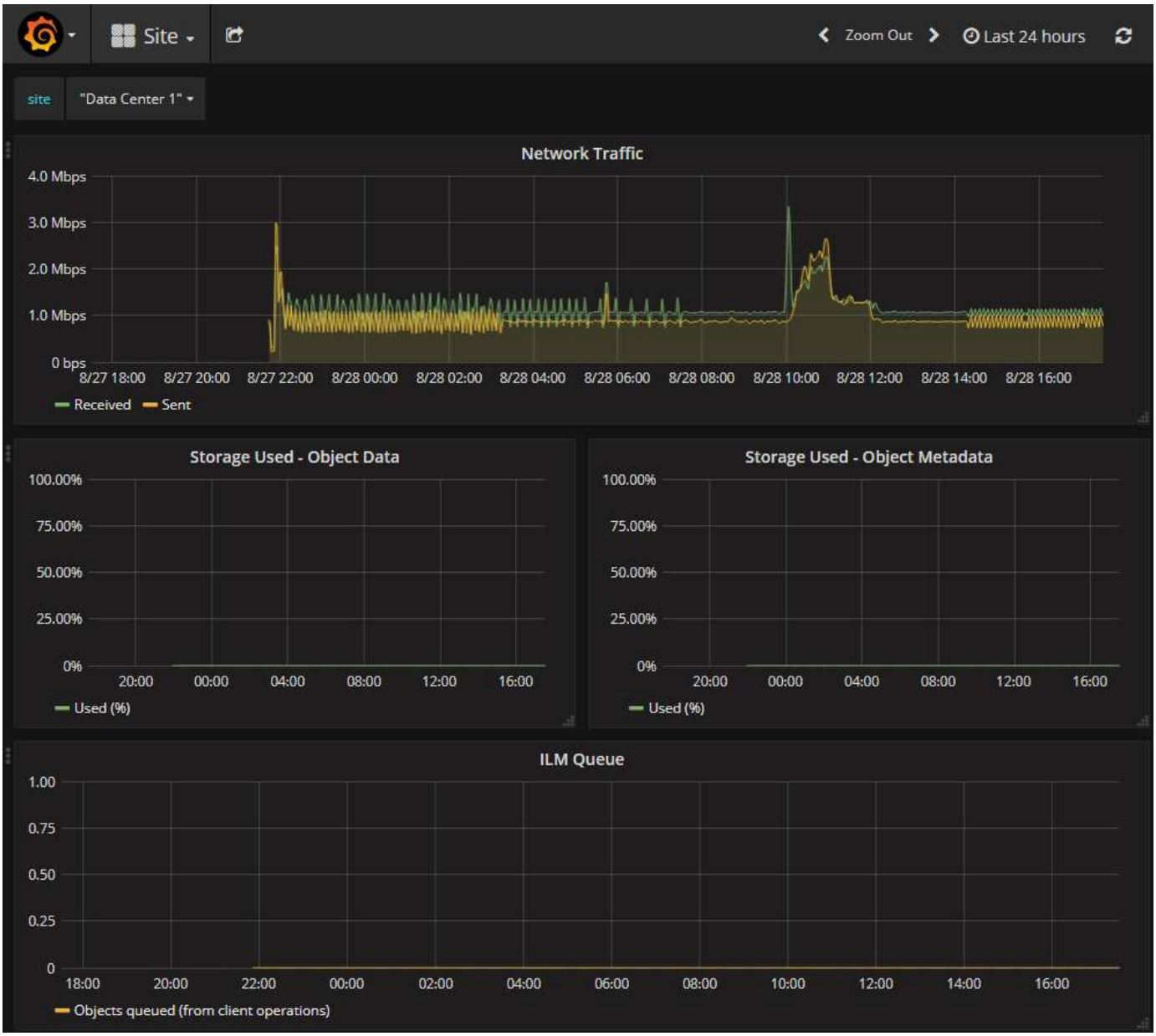
ADE	Grid	S3 - Node
Account Service Overview	ILM	S3 Overview
Alertmanager	Identity Service Overview	S3 Select
Audit Overview	Ingests	Site
Cassandra Cluster Overview	Node	Support
Cassandra Network Overview	Node (Internal Use)	Traces
Cassandra Node Overview	OSL - AsyncIO	Traffic Classification Policy
Cloud Storage Pool Overview	Platform Services Commits	Usage Processing
EC - ADE	Platform Services Overview	Virtual Memory (vmstat)
EC - Chunk Service	Platform Services Processing	
EC Overview	Replicated Read Path Overview	

El enlace de la sección Prometheus de la página Metrics le permite consultar los valores actuales de las métricas de StorageGRID y ver gráficos de los valores 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.

Los enlaces de la sección Grafana de la página Metrics le permiten acceder a paneles preconstruidos que contienen gráficos de métricas de StorageGRID a lo largo del tiempo.



Página Diagnóstico

La página Diagnósticos realiza un conjunto de comprobaciones de diagnóstico preconstruidas sobre el estado actual de la cuadrícula. En el ejemplo, todos los diagnósticos tienen un estado normal.

Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. A diagnostic check can have one of three statuses:

- **Normal**: All values are within the normal range.
- **Attention**: One or more of the values are outside of the normal range.
- **Caution**: One or more of the values are significantly outside of the normal range.

Diagnostic statuses are independent of current alerts and might not indicate operational issues with the grid. For example, a diagnostic check might show Caution status even if no alert has been triggered.

Run Diagnostics

- Cassandra blocked task queue too large
- Cassandra commit log latency
- Cassandra commit log queue depth
- Cassandra compaction queue too large

Al hacer clic en un diagnóstico específico puede ver detalles sobre el diagnóstico y sus resultados actuales.

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.

CPU utilization

Checks the current CPU utilization on each node.

To view charts of CPU utilization and other per-node metrics, access the **Node** Grafana dashboard.

Status Normal

Prometheus query `sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode)(node_cpu_seconds_total{mode!="idle"}))`

View in Prometheus

Thresholds Attention >= 75%
Caution >= 95%

Status	Instance	CPU Utilization
✔	DC1-ADM1	2.598%
✔	DC1-ARC1	0.937%
✔	DC1-G1	2.119%
✔	DC1-S1	8.708%
✔	DC1-S2	8.142%
✔	DC1-S3	9.669%
✔	DC2-ADM1	2.515%
✔	DC2-ARC1	1.152%
✔	DC2-S1	8.204%
✔	DC2-S2	5.000%
✔	DC2-S3	10.469%

Información relacionada

- Administre StorageGRID
- Configure los ajustes de red

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 las redes, familiarícese con la arquitectura StorageGRID tal y como se describe en Imprimador de rejilla.

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 nodos basados en software

- Instale Red Hat Enterprise Linux o CentOS
- Instalar Ubuntu o Debian

- Instale VMware

Instale los nodos del dispositivo

- Servicios de aplicaciones SG100 y SG1000
- Dispositivos de almacenamiento SG6000
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG5600

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

- Instale Red Hat Enterprise Linux o CentOS
- Instalar Ubuntu o Debian
- Instale VMware

Nodos del dispositivo

- Servicios de aplicaciones SG100 y SG1000
- Dispositivos de almacenamiento SG6000
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG5600

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. No es necesario que todos los nodos estén en la misma red de cliente y los nodos nunca se comunicarán entre sí a través de la red de 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 Administrar redes de clientes que no son de confianza 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. No obstante, 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 cuadrícula (eth0) o la interfaz de red de cliente (eth2) para que sea una conexión troncal, o bien puede usar interfaces troncales adicionales para el 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 obtener acceso de cliente o administrador a los nodos de almacenamiento ni 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.

Información relacionada

- Requisitos de red

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.

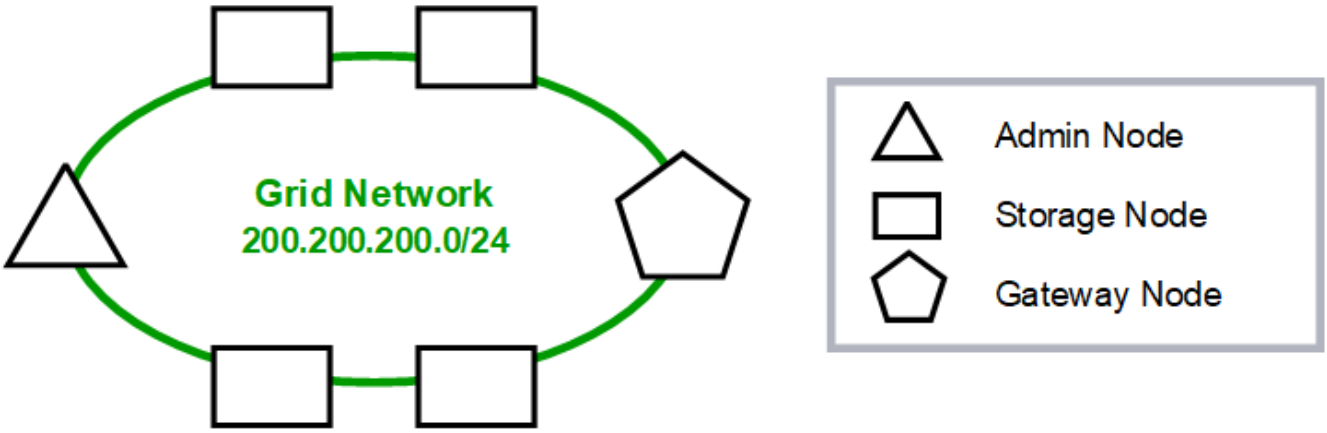
Durante la configuración, debe agregar todas las subredes de red de cuadrícula a la Lista de subredes de red de cuadrícula (GNSL). Esta lista incluye todas las subredes de todos los sitios y podría incluir también subredes externas que proporcionan acceso a servicios críticos como NTP, DNS o LDAP.

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 resulta adecuada para puestas en marcha en un único sitio que no están disponibles externamente, pruebas de concepto o puestas en marcha 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.

Topology example: Grid Network only



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

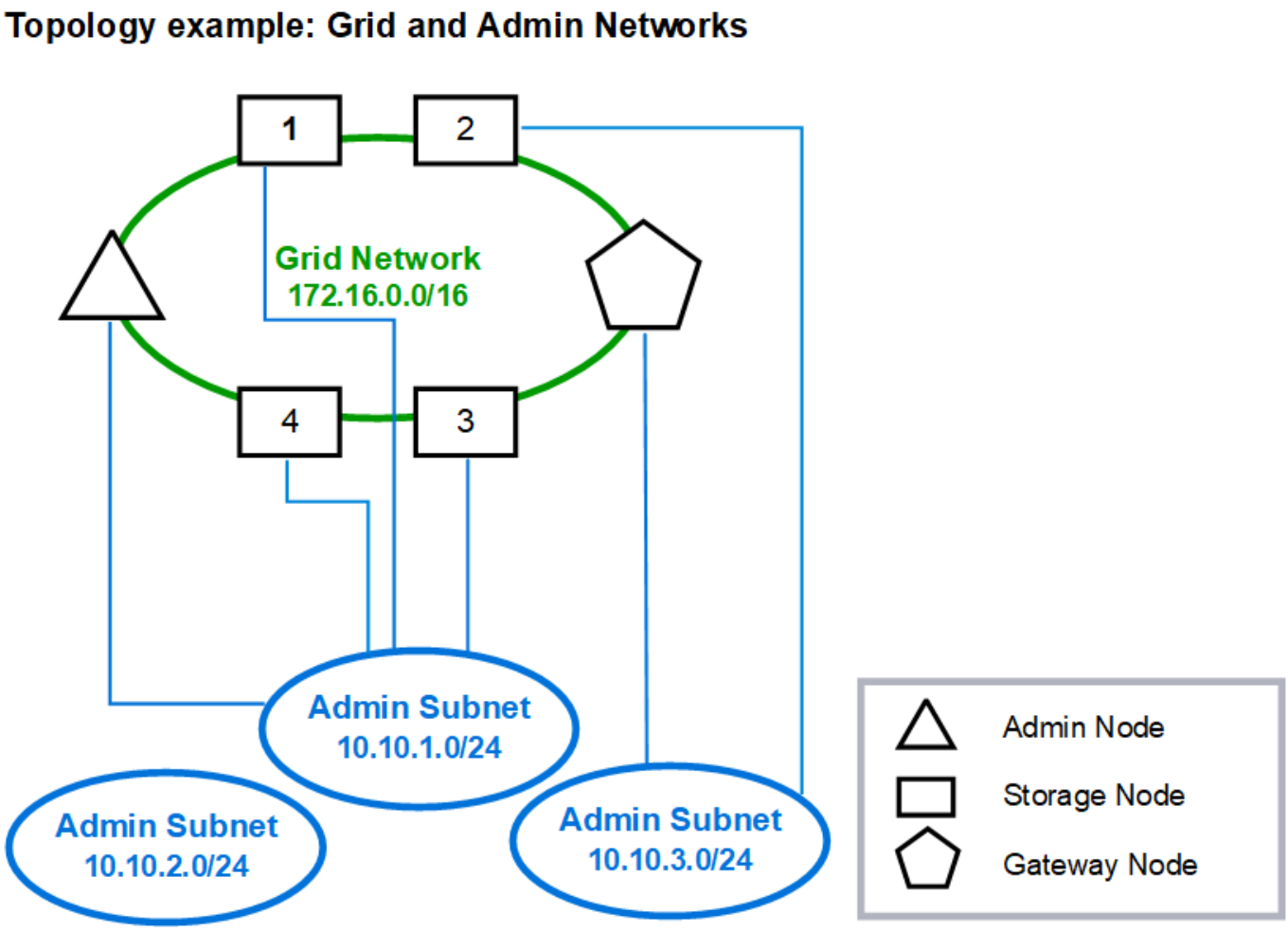
Topología de red de administrador

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.



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

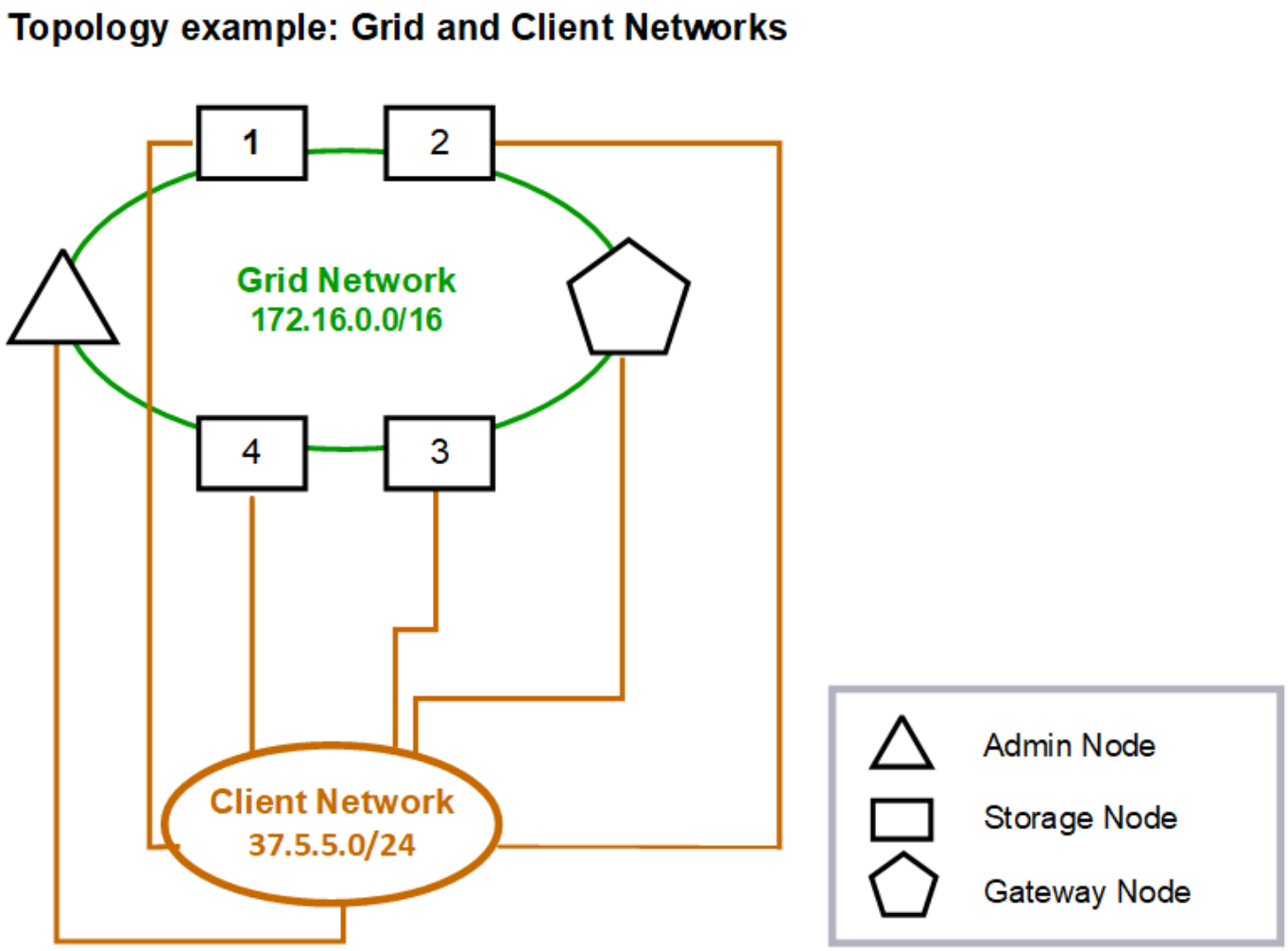
Tener una red cliente es opcional. Al usar una red de cliente, el tráfico de red de cliente (por ejemplo, S3 y Swift) se puede separar del tráfico interno de la cuadrícula, lo que permite que las redes de grid estén más seguras. El tráfico administrativo puede ser gestionado por el cliente o la red de 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

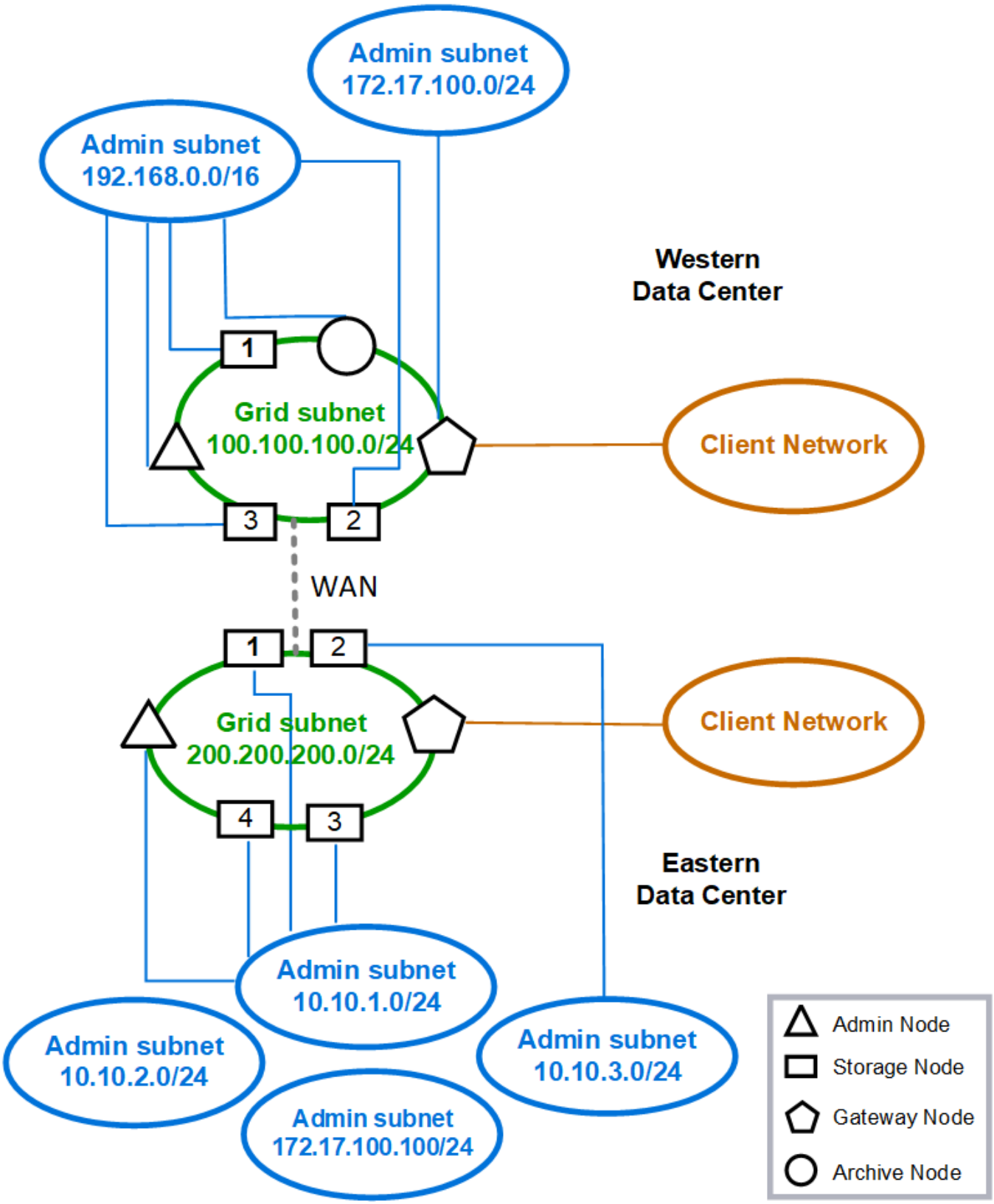
Topología para las tres redes

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 establecer contacto con ninguno de los servidores NTP o DNS aprovisionados mediante las reglas de enrutamiento predeterminadas, intentará establecer automáticamente el contacto en todas las redes (Grid, Admin y Client) siempre que 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 preparado para configurar las redes de administración y cliente opcionales durante la implementación, puede configurar estas redes cuando apruebe nodos de grid 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.

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 cuadrícula entre nodos de cuadrícula o entre sitios 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, la práctica recomendada es configurar la dirección de 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 a la subred de la red de red de red de red de red de cliente ni a ninguna subred de la GNSL.
- Las subredes de la AESL no pueden solaparse con las subredes de la GNSL.
- La subred de la red de cliente no puede superponerse a la subred de la red de red de red de red de red de red, a ninguna subred de la GNSL o a 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 administrativa incluyen conexiones de gestión, 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 contenedores. 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 CentOS 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 o CentOS (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, CentOS, Ubuntu o Debian (después de instalar el nodo)**: Linux: Añada tronco o interfaces

de acceso a un nodo

Recomendaciones mínimas de ancho de banda

La siguiente tabla muestra las recomendaciones sobre ancho de banda mínimo 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
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	1 Gbps	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 o CentOS)
- 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.. ¿Qué son los servicios de 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 cloud.

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 los 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 usar redes VLAN para servicios de plataforma o pools de almacenamiento en cloud. 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 en las instrucciones de instalación y mantenimiento del dispositivo:

- Servicios de aplicaciones SG100 y SG1000
- Dispositivos de almacenamiento SG6000
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG5600

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 es posible 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 volver a establecer 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 sólo permite conexiones entrantes a puertos específicos de la red de cuadrícula, a excepción de los puertos 22, 80, 123 y 443 (consulte la información sobre comunicaciones externas). 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. Si se permite el tráfico ICMP, puede mejorar el rendimiento de la conmutación por error cuando no se puede acceder a 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:

- Instale Red Hat Enterprise Linux o CentOS
- Instalar 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, consulteInstale 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. Para obtener más información acerca de la reasignación de puertos para los dispositivos, consulte:

- Servicios de aplicaciones SG100 y SG1000
- Dispositivos de almacenamiento SG6000
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG5600

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.
1139	TCP	Nodos de almacenamiento	Nodos de almacenamiento	Tráfico interno entre los nodos de almacenamiento.
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.
5353	UDP	Todos los nodos	Todos los nodos	Opcionalmente se utiliza para cambios en la IP de grid completo y para detección de nodos de administrador principal durante la instalación, la expansión y la recuperación.
7001	TCP	Nodos de almacenamiento	Nodos de almacenamiento	Comunicación del clúster entre nodos TLS de Cassandra.
7443	TCP	Todos los nodos	Nodos de administración	Tráfico interno para procedimientos de mantenimiento e informes de errores.
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 los usan para reenviar mensajes de AutoSupport desde E-Series SANtricity System Manager al nodo de administrador principal.
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.
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.
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. Entonces puede usar Redes de clientes no confiables para permitir el acceso sólo en los puertos de punto final del equilibrador de carga.

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 acerca de la reasignación de puertos, consulte las instrucciones de instalación de su plataforma:

Nodos basados en software

- Instale Red Hat Enterprise Linux o CentOS
- Instalar Ubuntu o Debian
- Instale VMware

Nodos del dispositivo

- Servicios de aplicaciones SG100 y SG1000
- Dispositivos de almacenamiento SG6000
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG5600

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 o se utiliza para "servidores de syslog".

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. De manera opcional, 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 el sistema de nombres de dominio.
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.
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 sólo es necesario si está activada la exportación de auditoría basada en SMB.

Puerto	TCP o UDP	Protocolo	De	Para	Detalles
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 sólo es necesario si está activada la exportación de auditoría basada en SMB.
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 sólo es necesario si está activada la exportación de auditoría basada en SMB.
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.

Puerto	TCP o UDP	Protocolo	De	Para	Detalles
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.
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.
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.

Puerto	TCP o UDP	Protocolo	De	Para	Detalles
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 anular el valor de puerto HTTP predeterminado de 443 al crear un extremo.
443	TCP	HTTPS	Nodos de almacenamiento	AWS	Solicitudes de Cloud Storage Pools enviadas a destinos de AWS que utilizan 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 sólo es necesario si está activada la exportación de auditoría basada en SMB.
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.
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.

Puerto	TCP o UDP	Protocolo	De	Para	Detalles
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.
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.
8082	TCP	HTTPS	Clientes S3	Nodos de puerta de enlace	Tráfico del cliente S3 al servicio CLB obsoleto en los nodos de puerta de enlace (HTTPS).
8083	TCP	HTTPS	Clientes Swift	Nodos de puerta de enlace	Tráfico del cliente de Swift al servicio CLB obsoleto en los nodos de puerta de enlace (HTTPS).
8084	TCP	HTTP	Clientes S3	Nodos de puerta de enlace	Tráfico del cliente S3 al servicio CLB obsoleto en los nodos de puerta de enlace (HTTP).

Puerto	TCP o UDP	Protocolo	De	Para	Detalles
8085	TCP	HTTP	Clientes Swift	Nodos de puerta de enlace	Tráfico del cliente de Swift al servicio CLB obsoleto en los nodos de puerta de enlace (HTTP).
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.
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.
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 del 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).

Instale y mantenga el hardware del dispositivo

Servicios de aplicaciones SG100 y SG1000

Dispositivos SG100 y SG1000: Descripción general

La aplicación de servicios SG100 de StorageGRID y la aplicación de servicios SG1000 pueden funcionar como nodo de puerta de enlace y como nodo de administración para ofrecer servicios de equilibrio de carga de alta disponibilidad en un sistema StorageGRID. Ambos dispositivos pueden funcionar como nodos de puerta de enlace y nodos de administración (primarios o no primarios) al mismo tiempo.

Funciones de los dispositivos

Ambos modelos del dispositivo de servicios ofrecen las siguientes características:

- Funciones del nodo de puerta de enlace o del nodo de administración para un sistema StorageGRID.
- El instalador de dispositivos StorageGRID para simplificar la puesta en marcha y la configuración de nodos.
- Cuando se implementa, puede acceder al software StorageGRID desde un nodo de administración existente o desde el software descargado en una unidad local. Para simplificar aún más el proceso de implementación, se incluye una versión reciente del software en el dispositivo durante la fabricación.
- Un controlador de administración en placa base (BMC) para supervisar y diagnosticar parte del hardware del dispositivo.
- La capacidad de conectarse a las tres redes StorageGRID, incluidas la red de grid, la red de administración y la red de cliente:
  - El SG100 admite hasta cuatro conexiones de 10 o 25 GbE a la red Grid y a la red de clientes.
  - El SG1000 admite hasta cuatro conexiones de 10, 25, 40 o 100 GbE a la red Grid y a la red de clientes.

Diagramas SG100 y SG1000

Esta figura muestra la parte frontal del SG100 y el SG1000 con el bisel retirado.

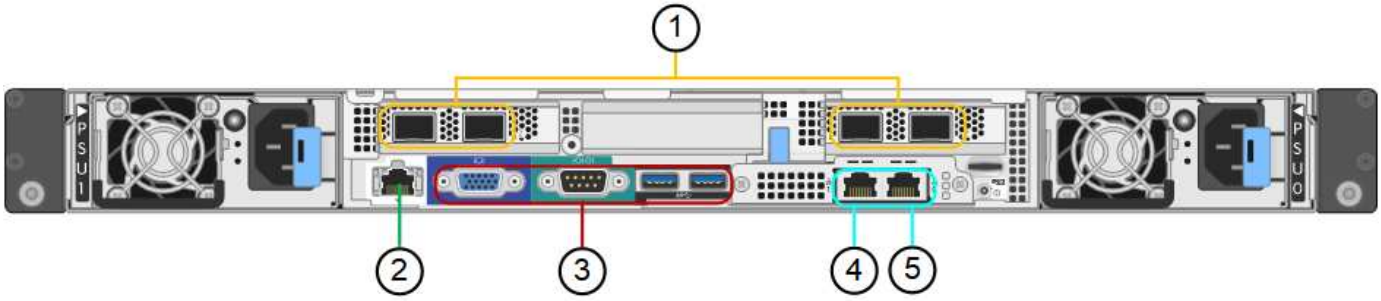
> Desde la parte frontal, los dos aparatos son idénticos a excepción del nombre del producto en el bisel.

Las dos unidades de estado sólido (SSD), indicadas en el contorno naranja, se utilizan para almacenar el sistema operativo StorageGRID y se reflejan con RAID1 para redundancia. Cuando el dispositivo de servicios SG100 o SG1000 se configura como un nodo de administración, estas unidades se utilizan para almacenar registros de auditoría, métricas y tablas de bases de datos.

Las ranuras de unidades restantes están vacías.

Conectores en la parte posterior del SG100

Esta figura muestra los conectores de la parte posterior del SG100.

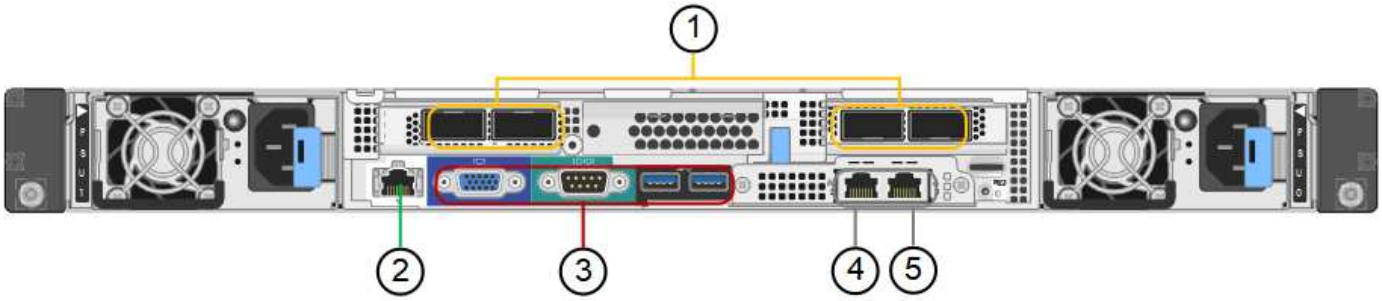


	Puerto	Tipo	Uso
1	Puertos de red 1-4	10/25-GbE, según el tipo de transceptor cable o SFP (se admiten los módulos SFP28 y SFP+), la velocidad del switch y la velocidad de enlace configurada	Conéctese a la red de red y a la red de cliente para StorageGRID.
2	Puerto de gestión de BMC	1 GbE (RJ-45).	Conéctese al controlador de administración de la placa base del dispositivo.
3	Puertos de diagnóstico y soporte	• VGA • Serie, 115200 8-N-1 • USB	Reservado para uso del soporte técnico.
4	Puerto de red de administrador 1	1 GbE (RJ-45).	Conecte el dispositivo a la red de administración para StorageGRID.

	Puerto	Tipo	Uso
5	Puerto de red de administrador 2	1 GbE (RJ-45).	Opciones: • Bond con el puerto de gestión 1 para una conexión redundante con la red de administrador para StorageGRID. • Deje desconectado y disponible para acceso local temporal (IP 169.254.0.1). • Durante la instalación, utilice el puerto 2 para la configuración de IP si las direcciones IP asignadas por DHCP no están disponibles.

Conectores en la parte posterior del SG1000

Esta figura muestra los conectores de la parte posterior del SG1000.



	Puerto	Tipo	Uso
1	Puertos de red 1-4	10/25/40/100-GbE, basado en el tipo de cable o transceptor, la velocidad del switch y la velocidad de enlace configurada. Se admiten QSFP28 y QSFP+ (40 GbE) de forma nativa y se pueden utilizar transceptores SFP28/SFP+ con una QSA (se vende por separado) para utilizar velocidades de 10 GbE.	Conéctese a la red de red y a la red de cliente para StorageGRID.

	Puerto	Tipo	Uso
2	Puerto de gestión de BMC	1 GbE (RJ-45).	Conéctese al controlador de administración de la placa base del dispositivo.
3	Puertos de diagnóstico y soporte	• VGA • Serie, 115200 8-N-1 • USB	Reservado para uso del soporte técnico.
4	Puerto de red de administrador 1	1 GbE (RJ-45).	Conecte el dispositivo a la red de administración para StorageGRID.
5	Puerto de red de administrador 2	1 GbE (RJ-45).	Opciones: • Bond con el puerto de gestión 1 para una conexión redundante con la red de administrador para StorageGRID. • Deje desconectado y disponible para acceso local temporal (IP 169.254.0.1). • Durante la instalación, utilice el puerto 2 para la configuración de IP si las direcciones IP asignadas por DHCP no están disponibles.

Aplicaciones SG100 y SG1000

Puede configurar los dispositivos de servicios StorageGRID de diversas formas para proporcionar servicios de puerta de enlace, así como redundancia de algunos servicios de administración de grid.

Los dispositivos se pueden implementar de las siguientes formas:

- Agregue a una cuadrícula nueva o existente como nodo de puerta de enlace
- Añada a un grid nuevo como nodo de administrador principal o no primario, o a un grid existente como nodo de administrador no primario
- Opere como un nodo de puerta de enlace y un nodo de administración (principal o no primario) al mismo tiempo

El dispositivo facilita el uso de grupos de alta disponibilidad (ha) y el equilibrio de carga inteligente para las conexiones de la ruta de datos S3 o Swift.

Los siguientes ejemplos describen cómo puede maximizar las funcionalidades del dispositivo:

- Utilice dos dispositivos SG100 o dos SG1000 para proporcionar servicios de puerta de enlace configurándolos como nodos de puerta de enlace.

> No instale los dispositivos de servicio SG100 y SG1000 en el mismo sitio. El rendimiento puede ser impredecible.

- Utilice dos dispositivos SG100 o dos SG1000 para ofrecer redundancia en algunos servicios de administración de grid. Para ello, configure cada dispositivo como nodos de administración.
- Utilice dos dispositivos SG100 o dos SG1000 para ofrecer servicios de equilibrio de carga y configuración de tráfico de alta disponibilidad a los que se accede a través de una o más direcciones IP virtuales. Para ello, configure los dispositivos como cualquier combinación de nodos de administrador o nodos de puerta de enlace y añada ambos nodos al mismo grupo de alta disponibilidad.

> Si se utilizan nodos de administrador y nodos de puerta de enlace en el mismo grupo de alta disponibilidad, los puertos de CLB (equilibrador de carga de conexión) y los puertos solo de nodo de administración no se conmutarán al nodo de respaldo. Para obtener instrucciones sobre cómo configurar grupos de alta disponibilidad, consulte las instrucciones para administrar StorageGRID.

> El servicio CLB está obsoleto.

Cuando se utiliza con dispositivos de almacenamiento StorageGRID, tanto el SG100 como los dispositivos de servicios SG1000 permiten la implementación de grids de dispositivo únicamente sin dependencias en hipervisores externos o hardware informático.

Información relacionada

Administre StorageGRID

Información general sobre la instalación y la implementación

Puede instalar uno o varios dispositivos de servicios StorageGRID cuando implemente StorageGRID por primera vez, o bien puede añadir nodos de dispositivos de servicios más adelante como parte de una ampliación.

Lo que necesitará

El sistema StorageGRID está utilizando la versión necesaria del software StorageGRID.

Dispositivo	Versión de StorageGRID requerida
SG100	11.4 o posterior (se recomienda la revisión más reciente)
SG1000	11.3 o posterior (se recomienda la revisión más reciente)

Tareas de instalación e implementación

Para preparar y añadir un dispositivo StorageGRID a la cuadrícula, se siguen cuatro pasos principales:

1. Preparación de la instalación:
    - Preparación del sitio de instalación
    - Desembalaje de las cajas y comprobación del contenido
    - Obtención de equipos y herramientas adicionales
    - Verificación de la configuración de red
    - Opcional: Configurar un servidor de gestión de claves (KMS) externo si planea cifrar todos los datos del dispositivo. Consulte detalles sobre la gestión de claves externas en las instrucciones para administrar StorageGRID.
2. Instalar el hardware:
    - Registrar el hardware
    - Instalación del dispositivo en un armario o rack
    - Cableado del aparato
    - Conexión del cable de alimentación y alimentación eléctrica
    - Ver los códigos de estado de inicio
3. Configurar el hardware:
    - Acceder al instalador de dispositivos de StorageGRID y configurar los ajustes de enlace e IP de red necesarios para conectarse a redes StorageGRID
    - Acceso a la interfaz del controlador de administración de la placa base (BMC) en el dispositivo.
    - Opcional: Habilitar el cifrado de nodos si tiene previsto utilizar un KMS externo para cifrar los datos del dispositivo.
4. Implementar una puerta de enlace de dispositivo o un nodo de administración

    Una vez instalado y configurado el hardware del dispositivo, puede implementar el dispositivo como nodo de puerta de enlace y nodo de administración en un sistema StorageGRID. Tanto los dispositivos SG100 como los SG1000 pueden funcionar al mismo tiempo como nodos de puerta de enlace y nodos de administración (primarios y no primarios).

Tarea	Instrucciones
Implementar una puerta de enlace del dispositivo o un nodo de administración en un nuevo sistema StorageGRID	Ponga en marcha un nodo de dispositivo de servicios
Añadir una puerta de enlace del dispositivo o un nodo de administración a un sistema StorageGRID existente	Amplíe un sistema StorageGRID
Implementar una puerta de enlace del dispositivo o un nodo de administrador como parte de una operación de recuperación de nodo	Recuperar y mantener un sistema StorageGRID

Información relacionada

Amplíe su grid

Recuperación y mantenimiento de su grid

Preparación de la instalación (SG100 y SG1000)

Para preparar la instalación de un dispositivo StorageGRID es necesario preparar el sitio y obtener todo el hardware, cables y herramientas necesarios. También debe recopilar información sobre las direcciones IP y la red.

Información relacionada

Requisitos del navegador web

Sitio de preparación (SG100 y SG1000)

Antes de instalar el dispositivo, debe asegurarse de que el sitio y el armario o rack que desee usar cumplan con las especificaciones de un dispositivo StorageGRID.

Pasos

1. Confirmar que el emplazamiento cumple los requisitos de temperatura, humedad, rango de altitud, flujo de aire, disipación de calor, cableado, alimentación y conexión a tierra. Si desea obtener más información, consulte Hardware Universe de NetApp.
2. Confirme que su ubicación proporciona la tensión correcta de la alimentación de CA (en el rango de 120 a 240 voltios de CA).
3. Obtenga un armario o rack de 19 pulgadas (48.3 cm) para colocar bandejas de este tamaño (sin cables):

Altura	Anchura	Profundidad	Peso máximo
1.70 pda (4.32 cm)	17.32 pda (44.0 cm)	32.0 pda (81.3 cm)	39 lb. (17.7 kg)

4. Decida dónde va a instalar el aparato.

Información relacionada

"Hardware Universe de NetApp"

"Herramienta de matriz de interoperabilidad de NetApp"

Desempaquetado (SG100 y SG1000)

Antes de instalar el aparato StorageGRID, desembale todas las cajas y compare el contenido con los artículos del recibo de embalaje.

Hardware de los dispositivos

- **SG100 o SG1000**

- **Kit de guías con instrucciones**

Cables de alimentación

El envío del dispositivo StorageGRID incluye los siguientes cables de alimentación:

- **Dos cables de alimentación para su país**

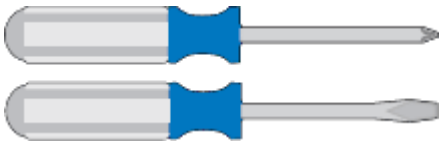
  Es posible que el armario tenga cables de alimentación especiales que utilice en lugar de los cables de alimentación que se suministran con el aparato.

Obtener equipamiento y herramientas adicionales (SG100 y SG1000)

Antes de instalar el aparato StorageGRID, confirme que dispone de todos los equipos y herramientas adicionales que necesita.

Necesitará el siguiente equipo adicional para instalar y configurar el hardware:

- **Destornilladores**

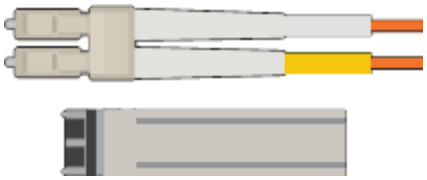
  

  Phillips no 2 destornillador

  Destornillador plano medio

- **Muñequera ESD**

- **Cables ópticos y transmisores**



- Cable
  - Twinax/Copper (de 1 a 4)

    o.

  - Fibra óptica (de 1 a 4)
- de 1 a 4 de cada uno de estos transceptores y adaptadores basados en velocidad de enlace (no se admiten velocidades mixtas)
  - SG100:

Velocidad de enlace (GbE)	Equipo necesario
10	Transceptor SFP+
25	Transceptor SFP28

  - SG1000:

Velocidad de enlace (GbE)	Equipo necesario
10	Adaptador QSFP a SFP (QSA) y transceptor SFP+
25	Adaptador QSFP a SFP (QSA) y transceptor SFP28
40	Transceptor QSFP+
100	Transceptor QFSP28

- **Cables Ethernet RJ-45 (Cat5/Cat5e/Cat6/Cat6a)**

- **Portátil de servicio**

Navegador web compatible

Puerto 1-GbE (RJ-45)

Es posible que algunos puertos no admitan 10/100 velocidades Ethernet.

- **Herramientas opcionales**

Taladro eléctrico con punta Phillips

Linterna

Revisar las conexiones de red de los dispositivos (SG100 y SG1000)

Antes de instalar el dispositivo StorageGRID, debe saber qué redes se pueden conectar al dispositivo.

Cuando implementa un dispositivo StorageGRID como nodo en un sistema StorageGRID, puede conectarlo a las siguientes redes:

- **Red de Grid para StorageGRID**: 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. Se requiere la red de red.
- **Red de administración para StorageGRID**: La Red de administración es una red cerrada que se utiliza para la administración y el mantenimiento del sistema. La red de administración suele ser una red privada y no es necesario que se pueda enrutar entre sitios. La red administrativa es opcional.
- **Red de clientes para StorageGRID:** la red de clientes es una red abierta que se utiliza para proporcionar acceso a las aplicaciones cliente, incluidos S3 y Swift. La red de cliente proporciona acceso de protocolo de cliente a la cuadrícula, de modo que la red de red de red pueda aislarse y protegerse. Puede configurar la red de cliente de modo que se pueda acceder al dispositivo a través de esta red utilizando sólo los puertos que elija abrir. La red cliente es opcional.
- **Red de administración de BMC para el dispositivo de servicios** (opcional): Esta red proporciona

acceso al controlador de administración de la placa base en los sistemas SG100 y SG1000, lo que le permite supervisar y administrar los componentes de hardware del dispositivo. Esta red de gestión puede ser la misma que la Red de administración para StorageGRID, o bien puede ser una red de gestión independiente.

Si la red de administración opcional de BMC no está conectada, será más difícil realizar algunos procedimientos de soporte y mantenimiento. Puede dejar la red de gestión de BMC sin conexión excepto cuando sea necesario para fines de soporte.

Información relacionada

Recopilar información de instalación (SG100 y SG1000)

Aparatos de cable SG100 y SG1000

Directrices sobre redes

Imprimador de rejilla

Modos de enlace de puerto para los dispositivos SG100 y SG1000

Al configurar enlaces de red para los dispositivos SG100 y SG1000, puede utilizar conexiones de puertos para los puertos que se conectan a la red Grid y a la red de clientes opcional, así como puertos de gestión de 1 GbE que se conectan a la red de administración opcional. El enlace de puertos ayuda a proteger los datos proporcionando rutas redundantes entre las redes StorageGRID y el dispositivo.

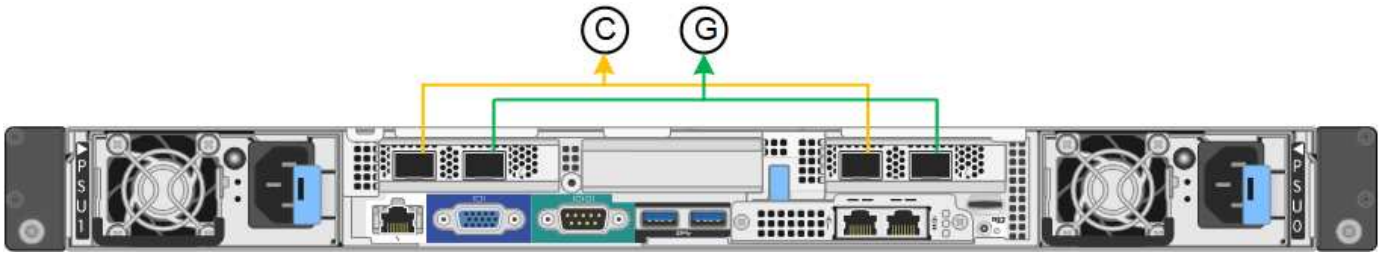
Modos de enlace de red

Los puertos de red del dispositivo de servicios admiten el modo de enlace de puerto fijo o el modo de enlace de puerto agregado para las conexiones de red de cliente y red de grid.

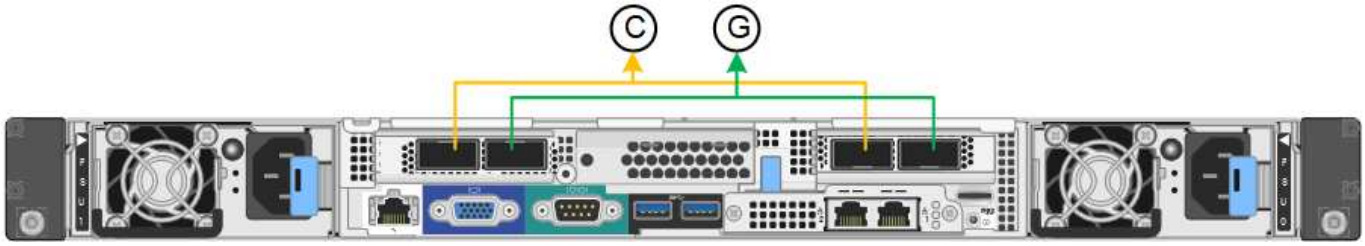
Modo de enlace de puerto fijo

El modo de enlace de puerto fijo es la configuración predeterminada de los puertos de red.

Modo de enlace de puerto fijo SG100



Modo de enlace de puerto fijo SG1000



Llamada	Qué puertos están Unidos
C	Los puertos 1 y 3 se unen para la red cliente, si se utiliza esta red.
G	Los puertos 2 y 4 están Unidos para la red de cuadrícula.

Cuando se utiliza el modo de enlace de puerto fijo, los puertos se pueden enlazar mediante el modo de copia de seguridad activa o el modo de protocolo de control de agregación de enlaces (LACP 802.3ad).

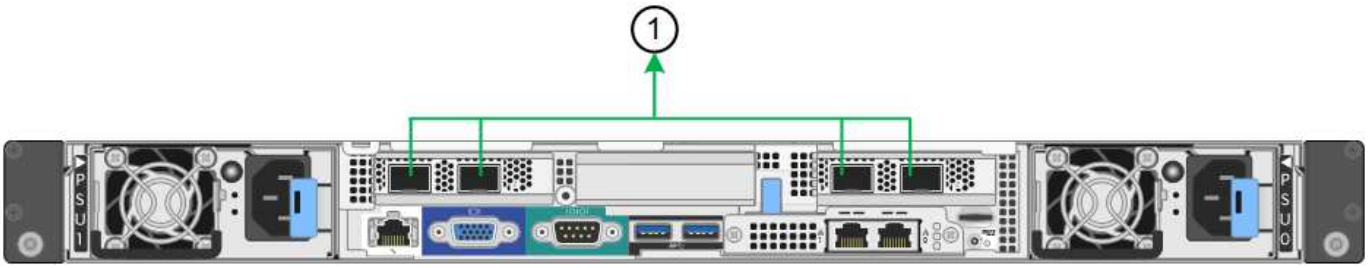
- En el modo activo-backup (predeterminado), solo hay un puerto activo a la vez. Si se produce un error en el puerto activo, su puerto de backup proporciona automáticamente una conexión de conmutación por error. El puerto 4 proporciona una ruta de copia de seguridad para el puerto 2 (red de red de cuadrícula) y el puerto 3 proporciona una ruta de copia de seguridad para el puerto 1 (red de cliente).
- En el modo LACP, cada par de puertos forma un canal lógico entre el dispositivo de servicios y la red, lo que permite un mayor rendimiento. Si un puerto falla, el otro continúa proporcionando el canal. El rendimiento se reduce, pero la conectividad no se ve afectada.

> Si no necesita conexiones redundantes, sólo puede utilizar un puerto para cada red. Sin embargo, tenga en cuenta que la alerta * vínculo inactivo* del dispositivo de servicios puede activarse en el administrador de grid después de instalar StorageGRID, lo que indica que un cable está desenchufado. Puede desactivar esta regla de alerta con seguridad.

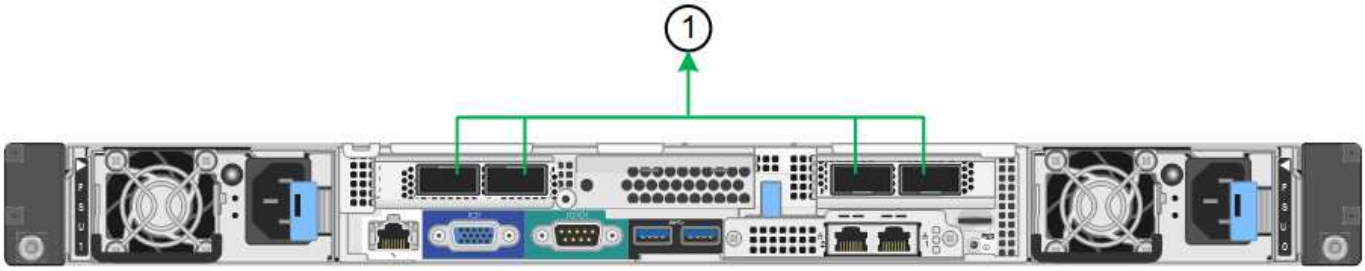
Modo de enlace de puerto agregado

El modo de enlace de puerto de agregado aumenta de manera significativa el rendimiento de cada red StorageGRID y proporciona rutas de conmutación al respaldo adicionales.

Modo de enlace de puerto agregado SG100



Modo de enlace de puerto agregado SG1000



Llamada	Qué puertos están Unidos
1	Todos los puertos conectados se agrupan en un único enlace LACP, lo que permite que todos los puertos se usen para el tráfico de red de grid y de red de cliente.

Si tiene pensado utilizar el modo de enlace de puerto agregado:

- Debe usar el modo de enlace de red LACP.
- Debe especificar una etiqueta de VLAN exclusiva para cada red. Esta etiqueta VLAN se añadirá a cada paquete de red para garantizar que el tráfico de red se dirija a la red correcta.
- Los puertos deben estar conectados a switches que sean compatibles con VLAN y LACP. Si varios switches participan en el enlace LACP, los switches deben ser compatibles con los grupos de agregación de enlaces de varios chasis (MLAG), o equivalentes.
- Debe comprender cómo configurar los switches para que utilicen VLAN, LACP y MLAG, o equivalente.

Si no desea usar los cuatro puertos, puede usar uno, dos o tres puertos. El uso de más de un puerto maximiza la posibilidad de que cierta conectividad de red permanezca disponible si se produce un error en uno de ellos.

> Si decide utilizar menos de cuatro puertos, tenga en cuenta que puede activarse una alerta * de enlace de dispositivo de servicios* en Grid Manager después de instalar el nodo del dispositivo, lo que indica que se ha desenchufado un cable. Puede deshabilitar con seguridad esta regla de alerta para la alerta activada. En Grid Manager, seleccione **ALERTS** > **Reglas**, seleccione la regla y haga clic en **Editar regla**. A continuación, desactive la casilla de verificación **Activado**.

Modos de enlace de red para los puertos de gestión

Para los dos puertos de gestión de 1-GbE en el dispositivo de servicios, puede elegir el modo de enlace de red independiente o el modo de enlace de red Active-Backup para conectarse a la red de administración opcional.

Puertos de administración de red SG100

Puertos de administración de redes SG1000

En modo independiente, solo el puerto de gestión de la izquierda está conectado a la red del administrador. Este modo no proporciona una ruta de acceso redundante. El puerto de gestión de la derecha no está conectado y está disponible para conexiones locales temporales (utiliza la dirección IP 169.254.0.1)

En el modo Active-Backup, ambos puertos de gestión están conectados a la red Admin. Solo hay un puerto activo a la vez. Si se produce un error en el puerto activo, su puerto de backup proporciona automáticamente una conexión de conmutación por error. La vinculación de estos dos puertos físicos en un puerto de gestión lógica proporciona una ruta redundante a la red de administración.

> Si necesita realizar una conexión local temporal al dispositivo de servicios cuando los puertos de gestión de 1-GbE están configurados para el modo Active-Backup, quite los cables de ambos puertos de gestión, enchufe el cable temporal al puerto de gestión a la derecha y acceda al dispositivo con la dirección IP 169.254.0.1.

Llamada	Modo de enlace de red
A.	Modo de copia de seguridad activa. Ambos puertos de gestión están Unidos en un puerto de gestión lógico conectado a la red administrativa.
YO	Modo independiente. El puerto de la izquierda está conectado a la red de administración. El puerto de la derecha está disponible para conexiones locales temporales (dirección IP 169.254.0.1).

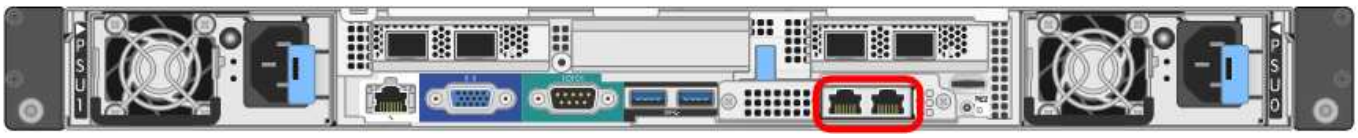
Recopilar información de instalación (SG100 y SG1000)

Al instalar y configurar el dispositivo StorageGRID, debe tomar decisiones y recopilar información acerca de los puertos del switch Ethernet, las direcciones IP y los modos de enlace de puerto y red. Registre la información necesaria de cada red que conecte al dispositivo. Estos valores son necesarios para instalar y configurar el hardware.

Puertos de administración y mantenimiento

La red de administración de StorageGRID es una red opcional que se utiliza para la administración y el mantenimiento del sistema. El dispositivo se conecta a la red de administración mediante los siguientes puertos de gestión de 1 GbE del dispositivo.

SG100 puertos RJ-45



SG1000 puertos RJ-45

Conexiones de administración y mantenimiento

Información necesaria	Su valor
Red de administrador habilitada	Elija una opción: • No • Sí (predeterminado)
Modo de enlace de red	Elija una opción: • Independiente (predeterminado) • Copia de seguridad activa
Puerto de conmutador para el puerto izquierdo con un círculo en el diagrama (puerto activo predeterminado para el modo de enlace de red independiente)	
Puerto de conmutador para el puerto derecho con un círculo en el diagrama (sólo modo de enlace de red Active-Backup)	
Dirección MAC del puerto de red de administración **Nota:** la etiqueta de dirección MAC de la parte frontal del dispositivo enumera la dirección MAC del puerto de administración del BMC. Para determinar la dirección MAC del puerto de red de administración, debe agregar **2** al número hexadecimal de la etiqueta. Por ejemplo, si la dirección MAC de la etiqueta termina en **09**, la dirección MAC del puerto de administración finalizará en **0B**. Si la dirección MAC de la etiqueta termina en **(*y*)FF**, la dirección MAC del puerto de administración finalizará en **(*y*+1)01**. Puede realizar este cálculo fácilmente abriendo Calculadora en Windows, establecerlo en modo Programador, seleccionando hex, escribiendo la dirección MAC y, a continuación, escribiendo **+ 2 =**.	

Información necesaria	Su valor
Dirección IP asignada por DHCP para el puerto de red de administración, si está disponible después del encendido **Nota:** puede determinar la dirección IP asignada por DHCP utilizando la dirección MAC para buscar la dirección IP asignada.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Dirección IP estática que piensa usar para el nodo del dispositivo en la red de administración **Nota:** Si su red no tiene una puerta de enlace, especifique la misma dirección IPv4 estática para la puerta de enlace.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Subredes de red de administración (CIDR)	

Puertos de red

Los cuatro puertos de red del dispositivo se conectan a la red Grid de StorageGRID y a la red de cliente opcional.

Conexiones de red

Información necesaria	Su valor
Velocidad de enlace	Para SG100, seleccione una de las opciones siguientes: • Automático (predeterminado) • 10 GbE • 25 GbE Para SG1000, seleccione una de las siguientes opciones: • Automático (predeterminado) • 10 GbE • 25 GbE • 40 GbE • 100 GbE **Nota:** para las velocidades SG1000, 10 y 25 GbE se necesitan adaptadores QSA.

Información necesaria	Su valor
Modo de enlace de puerto	Elija una opción: • Fijo (predeterminado) • Agregado
Puerto de conmutador para el puerto 1 (red cliente para modo fijo)	
Puerto de conmutador para el puerto 2 (red de cuadrícula para modo fijo)	
Puerto de conmutador para el puerto 3 (red cliente para modo fijo)	
Puerto de conmutador para el puerto 4 (red de cuadrícula para modo fijo)	

Puertos de red de grid

Grid Network para StorageGRID es una red necesaria que se utiliza para todo el tráfico interno de StorageGRID. El dispositivo se conecta a la red de cuadrícula mediante los cuatro puertos de red.

Conexiones de red de red

Información necesaria	Su valor
Modo de enlace de red	Elija una opción: • Active-Backup (predeterminado) • LACP (802.3ad)
Etiquetado VLAN habilitado	Elija una opción: • No (predeterminado) • Sí
Etiqueta de VLAN (si el etiquetado de VLAN está habilitado)	Introduzca un valor entre 0 y 4095:
Dirección IP asignada por DHCP para la red de cuadrícula, si está disponible después del encendido	• Dirección IPv4 (CIDR): • Puerta de enlace:

Información necesaria	Su valor
Dirección IP estática que se va a utilizar para el nodo del dispositivo en la red de cuadrícula **Nota:** Si su red no tiene una puerta de enlace, especifique la misma dirección IPv4 estática para la puerta de enlace.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Subredes de red de cuadrícula (CIDR)	
Configuración de unidad de transmisión máxima (MTU) (opcional)puede utilizar el valor predeterminado de 1500 o establecer el MTU en un valor adecuado para tramas gigantes, como 9000.	

Puertos de red del cliente

La red de cliente para StorageGRID es una red opcional que se suele utilizar para proporcionar acceso al protocolo de cliente al grid. El dispositivo se conecta a la red cliente mediante los cuatro puertos de red.

Conexiones de red cliente

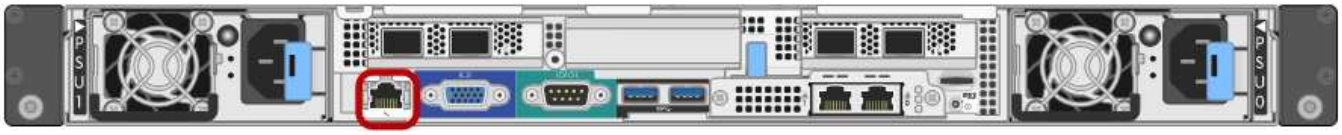
Información necesaria	Su valor
Red de cliente habilitada	Elija una opción: • No (predeterminado) • Sí
Modo de enlace de red	Elija una opción: • Active-Backup (predeterminado) • LACP (802.3ad)
Etiquetado VLAN habilitado	Elija una opción: • No (predeterminado) • Sí
Etiqueta de VLAN (si el etiquetado de VLAN está habilitado)	Introduzca un valor entre 0 y 4095:
Dirección IP asignada por DHCP para la red cliente, si está disponible después del encendido	• Dirección IPv4 (CIDR): • Puerta de enlace:

Información necesaria	Su valor
Dirección IP estática que se va a usar para el nodo del dispositivo en la red cliente **Nota:** Si la red de cliente está activada, la ruta predeterminada del dispositivo utilizará la puerta de enlace especificada aquí.	• Dirección IPv4 (CIDR): • Puerta de enlace:

Puertos de red de gestión de BMC

Puede acceder a la interfaz del BMC en el dispositivo de servicios mediante el puerto de gestión de 1-GbE rodeado por un círculo en el diagrama. Este puerto admite la gestión remota del hardware de la controladora a través de Ethernet mediante el estándar de interfaz de gestión de plataforma inteligente (IPMI).

SG100 Puerto de gestión BMC



Puerto de administración de SG1000 BMC

Conexiones de red de administración de BMC

Información necesaria	Su valor
Puerto del switch Ethernet se conectará al puerto de administración del BMC (con un círculo en el diagrama)	
Dirección IP asignada por DHCP para la red de gestión de BMC, si está disponible después del encendido	• Dirección IPv4 (CIDR): • Puerta de enlace:
La dirección IP estática que planea usar para el puerto de gestión de BMC	• Dirección IPv4 (CIDR): • Puerta de enlace:

Información relacionada

Descripción general de los dispositivos SG100 y SG1000

Aparatos de cable SG100 y SG1000

Configure las direcciones IP de StorageGRID

Instalación del hardware (SG100 y SG1000)

Registre el hardware

El registro del hardware del dispositivo proporciona ventajas de asistencia.

Pasos

1. Localice el número de serie del chasis para el dispositivo.

   Puede encontrar el número en el recibo de embalaje, en el correo electrónico de confirmación o en el aparato después de desembalarlo.

2. Vaya al sitio de soporte de NetApp en "mysupport.netapp.com".
3. Determine si necesita registrar el hardware:

Si usted es un…	Siga estos pasos…
Cliente existente de NetApp	a. Inicie sesión con su nombre de usuario y contraseña. b. Seleccione **Productos** > **Mis productos**. c. Confirme que el nuevo número de serie aparece en la lista. d. De lo contrario, siga las instrucciones para nuevos clientes de NetApp.
Nuevo cliente de NetApp	a. Haga clic en **Registrar ahora** y cree una cuenta. b. Seleccione **Productos** > **Registrar productos**. c. Introduzca el número de serie del producto y los detalles solicitados. Una vez aprobado el registro, puede descargar el software necesario. El proceso de aprobación puede llevar hasta 24 horas.

Instalar el dispositivo en un armario o rack (SG100 y SG1000)

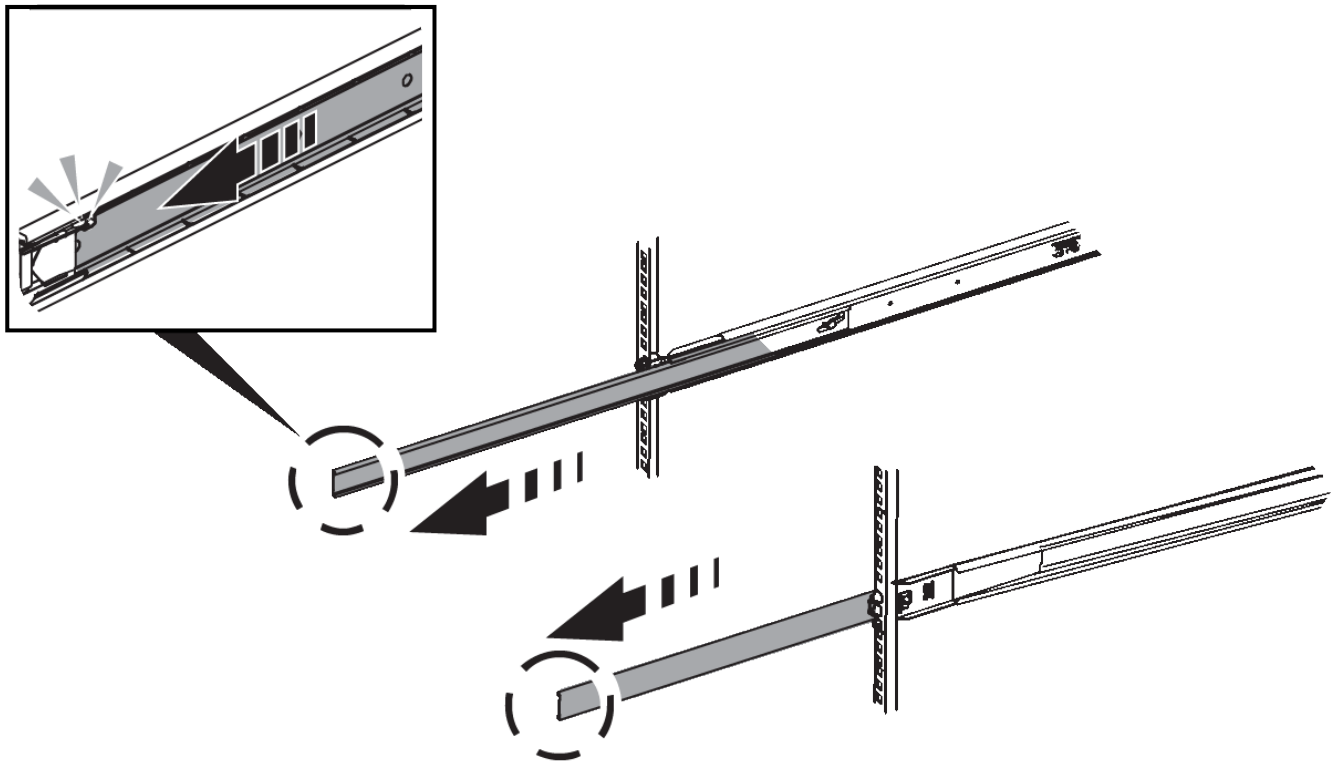
Debe instalar un conjunto de rieles para el dispositivo en su armario o rack y, a continuación, deslizar el dispositivo sobre los rieles.

Lo que necesitará

- Ha revisado el documento de avisos de seguridad que se incluye en la caja y comprende las precauciones para mover e instalar el hardware.
- Tiene las instrucciones incluidas en el kit de raíl.

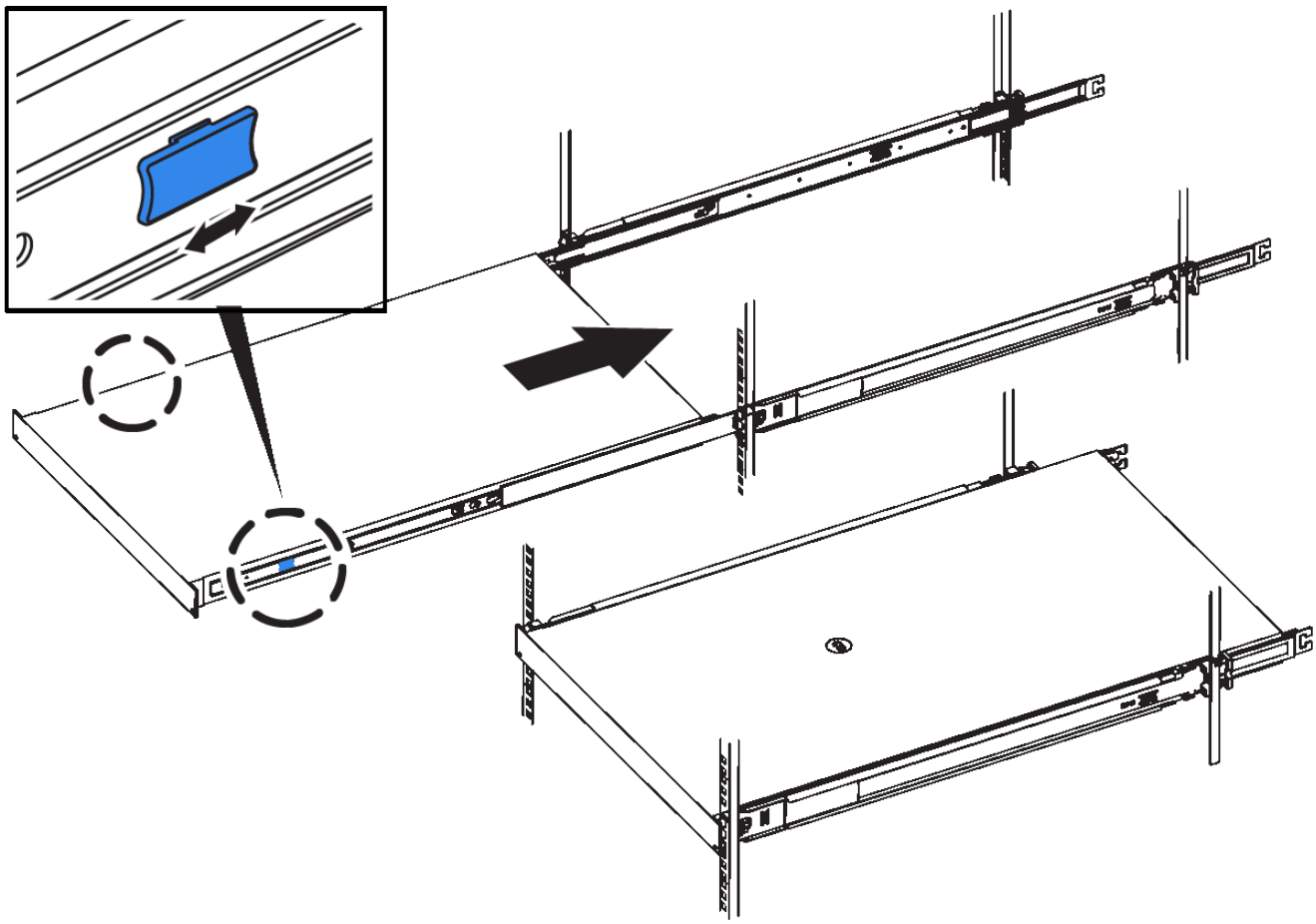
Pasos

1. Siga con cuidado las instrucciones del kit de raíl para instalar los rieles en su armario o rack.
2. En los dos rieles instalados en el armario o rack, extienda las partes móviles de los rieles hasta que oiga un clic.



3. Inserte el aparato en los rieles.
4. Deslice el aparato en el armario o rack.

   Cuando no pueda mover el aparato más allá, tire de los pestillos azules situados a ambos lados del chasis para deslizar el aparato completamente.



No conecte el bisel frontal hasta que haya encendido el aparato.

Aparatos de cable SG100 y SG1000

Debe conectar el puerto de administración del dispositivo al ordenador portátil de servicio y conectar los puertos de red del dispositivo a la red de grid y a la red de cliente opcional para StorageGRID.

Lo que necesitará

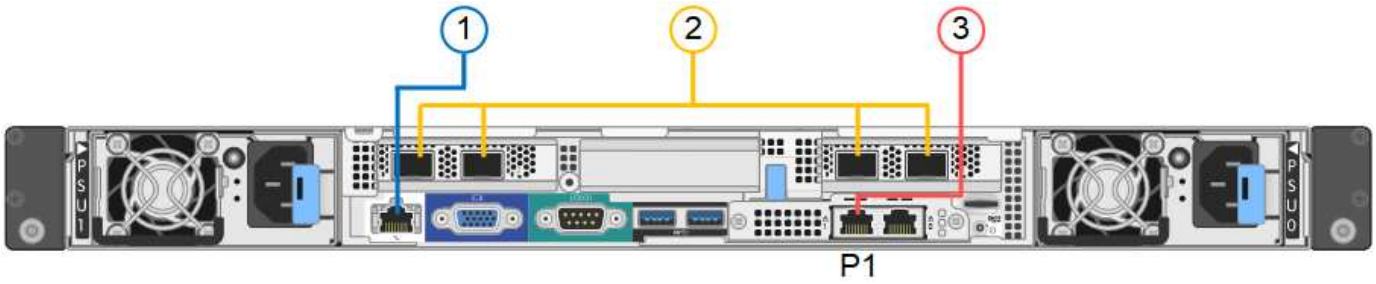
- Tiene un cable Ethernet RJ-45 para conectar el puerto de administración.
- Tiene una de las siguientes opciones para los puertos de red. Estos artículos no se proporcionan con el aparato.
  - De uno a cuatro cables Twinax para conectar los cuatro puertos de red.
  - Para SG100, de uno a cuatro transceptores SFP+ o SFP28 si planea utilizar cables ópticos para los puertos.
  - Para SG1000, de uno a cuatro transceptores QSFP+ o QSFP28 si va a utilizar cables ópticos para los puertos.

Riesgo de exposición a la radiación láser — no desmonte ni retire ninguna parte de un transceptor SFP o QSFP. Puede que esté expuesto a la radiación láser.

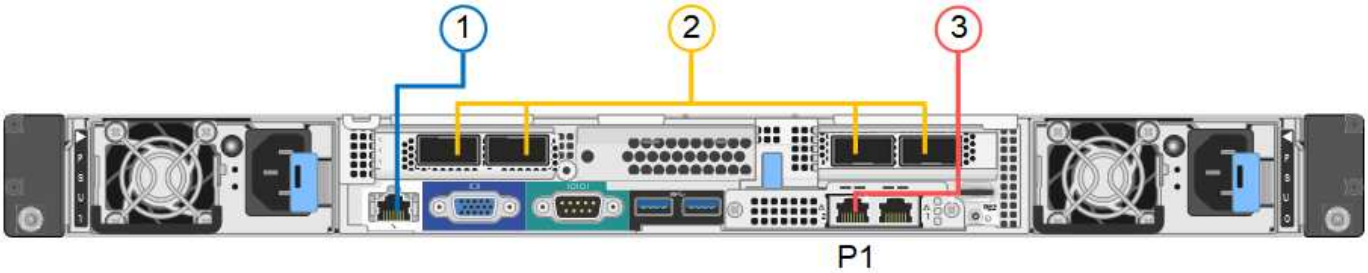
Acerca de esta tarea

Las siguientes figuras muestran los puertos de la parte posterior del aparato.

Conexiones de puerto SG100



Conexiones de puerto SG1000



	Puerto	Tipo de puerto	Función
1	Puerto de gestión BMC en el dispositivo	1 GbE (RJ-45).	Se conecta a la red en la que se accede a la interfaz del BMC.
2	Cuatro puertos de red en el dispositivo	• Para el SG100: 10/25-GbE • Para el SG1000: 10/25/40/100-GbE	Conéctese a la red de red y a la red de cliente para StorageGRID.
3	Puerto de red de administración en el dispositivo (etiquetado P1 en las figuras)	1 GbE (RJ-45). **Importante:** este puerto funciona sólo a 1000 BaseT/full y no admite velocidades de 10 o 100 megabits.	Conecta el dispositivo a la red de administración para StorageGRID.

	Puerto	Tipo de puerto	Función
	El puerto RJ-45 más a la derecha del aparato	1 GbE (RJ-45). **Importante:** este puerto funciona sólo a 1000 BaseT/full y no admite velocidades de 10 o 100 megabits.	• Se puede unir al puerto de administración 1 si desea una conexión redundante a la red de administración. • Se puede dejar desconectado y disponible para acceso local temporal (IP 169.254.0.1). • Durante la instalación, se puede utilizar para conectar el dispositivo a un ordenador portátil de servicio si las direcciones IP asignadas por DHCP no están disponibles.

Pasos

1. Conecte el puerto de gestión BMC del dispositivo a la red de gestión mediante un cable Ethernet.

   Aunque esta conexión es opcional, se recomienda facilitar el soporte.

2. Conecte los puertos de red del dispositivo a los switches de red adecuados utilizando cables Twinax o cables ópticos y transceptores.

   Los cuatro puertos de red deben usar la misma velocidad de enlace. Consulte las siguientes tablas para conocer el equipo necesario en función de su hardware y la velocidad de enlace.

Velocidad de enlace SG100 (GbE)	Equipo necesario
10	Transceptor SFP+
25	Transceptor SFP28
Velocidad de enlace SG1000 (GbE)	Equipo necesario
10	Transceptor QSA y SFP+
25	Transceptor QSA y SFP28
40	Transceptor QSFP+
100	Transceptor QFSP28

   - Si piensa utilizar el modo de enlace de puerto fijo (predeterminado), conecte los puertos a la red de StorageGRID y a las redes de cliente, como se muestra en la tabla.

Puerto	Conecta a…
Puerto 1	Red de cliente (opcional)
Puerto 2	Red Grid
Puerto 3	Red de cliente (opcional)
Puerto 4	Red Grid

- Si planea utilizar el modo de enlace de puerto agregado, conecte uno o varios puertos de red a uno o varios switches. Debe conectar al menos dos de los cuatro puertos para evitar tener un único punto de error. Si utiliza más de un switch para un único vínculo LACP, los switches deben ser compatibles con MLAG o equivalente.

3. Si tiene previsto utilizar la Red de administración para StorageGRID, conecte el puerto Red de administración del dispositivo a la Red de administración mediante un cable Ethernet.

Conexión de los cables de alimentación y alimentación (SG100 y SG1000)

Después de conectar los cables de red, estará preparado para alimentar el aparato.

Pasos

1. Conecte un cable de alimentación a cada una de las dos unidades de alimentación del aparato.
2. Conecte estos dos cables de alimentación a dos unidades de distribución de alimentación (PDU) diferentes en el armario o rack.
3. Si el botón de encendido de la parte frontal del aparato no está iluminado en azul actualmente, pulse el botón para encender el aparato.

   No vuelva a pulsar el botón de encendido durante el proceso de encendido.

4. Si se producen errores, corrija los problemas.
5. Coloque el bisel frontal en el aparato si lo ha extraído.

Información relacionada

Ver los indicadores de estado de los aparatos SG100 y SG1000

Ver los indicadores de estado de los aparatos SG100 y SG1000

El dispositivo incluye indicadores que ayudan a determinar el estado de la controladora del dispositivo y los dos SSD.

Botones e indicadores del aparato

	Mostrar	Estado
1	Botón de encendido	• Azul: El aparato está encendido. • Apagado: El aparato está apagado.
2	Botón de reinicio	Utilice este botón para realizar un restablecimiento completo del controlador.
3	Botón identificar	Este botón se puede establecer en enlace, encendido (sólido) o Apagado. • Azul, parpadeando: Identifica el dispositivo en el armario o rack. • Azul, sólido: Identifica el dispositivo en el armario o rack. • Desactivado: El aparato no se puede identificar visualmente en el armario o bastidor.
4	LED de alarma	• Ámbar, sólido: Se ha producido un error. **Nota:** para ver los códigos de arranque y error, debe acceder a la interfaz del BMC. • Desactivado: No hay errores.

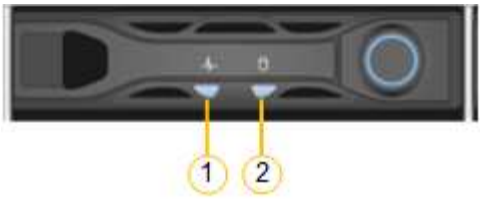
códigos generales de arranque

Durante el arranque o después de un reinicio duro del aparato, ocurre lo siguiente:

1. El controlador de administración de la placa base (BMC) registra los códigos de la secuencia de arranque, incluidos los errores que se produzcan.
2. El botón de encendido se ilumina.
3. Si se produce algún error durante el arranque, el LED de alarma se enciende.

   Para ver los códigos de arranque y error, debe acceder a la interfaz del BMC.

Indicadores de SSD



LED	Mostrar	Estado
1	Estado/fallo de la unidad	• Azul (sólido): La unidad está en línea • Ámbar (parpadea): Fallo de la unidad • Desactivado: La ranura está vacía
2	Unidad activa	Azul (parpadeante): Se está accediendo a la unidad

Información relacionada

Solucionar problemas de instalación de hardware (SG100 y SG1000)

Configurar la interfaz BMC (SG100 y SG1000)

Configurar conexiones StorageGRID (SG100 y SG1000)

Para poder implementar el dispositivo de servicios como nodo en un sistema StorageGRID, debe configurar las conexiones entre el dispositivo y las redes que planea usar. Puede configurar la conexión de red en el instalador de dispositivos de StorageGRID, que está preinstalado en el dispositivo de servicios.

Acceda al instalador de dispositivos de StorageGRID

Debe acceder al instalador de dispositivos de StorageGRID para configurar las conexiones entre el dispositivo y las tres redes StorageGRID: La red de grid, la red de administrador (opcional) y la red de cliente (opcional).

Lo que necesitará

- Está usando cualquier cliente de gestión que pueda conectarse a la red administrativa de StorageGRID.
- El cliente tiene un navegador web compatible.
- El dispositivo de servicios está conectado a todas las redes StorageGRID que tiene previsto utilizar.
- Conoce la dirección IP, la puerta de enlace y la subred del dispositivo de servicios de estas redes.
- Configuró los switches de red que planea utilizar.

Acerca de esta tarea

Para acceder inicialmente al instalador de dispositivos StorageGRID, puede utilizar la dirección IP asignada por DHCP para el puerto de la red de administración en el dispositivo de servicios (suponiendo que esté conectado a la red de administración) o puede conectar un portátil de servicio directamente al dispositivo de

servicios.

Pasos

1. Si es posible, utilice la dirección DHCP del puerto de red de administración en el dispositivo de servicios para acceder al instalador de StorageGRID Appliance.

   SG100 Puerto de red de administración

   SG1000 Admin Network Port

   a. Localice la etiqueta de dirección MAC en la parte frontal del dispositivo servicios y determine la dirección MAC del puerto de red de administración.

      La etiqueta de dirección MAC incluye la dirección MAC para el puerto de gestión del BMC.

      Para determinar la dirección MAC del puerto de red de administración, debe agregar **2** al número hexadecimal de la etiqueta. Por ejemplo, si la dirección MAC de la etiqueta termina en **09**, la dirección MAC del puerto de administración finalizará en **0B**. Si la dirección MAC de la etiqueta termina en **(*y*)FF**, la dirección MAC del puerto de administración finalizará en **(*y*+1)01**. Puede realizar este cálculo fácilmente abriendo Calculadora en Windows, establecerlo en modo Programador, seleccionando hex, escribiendo la dirección MAC y, a continuación, escribiendo **+ 2 =**.

   b. Proporcione la dirección MAC al administrador de red, de modo que puedan buscar la dirección DHCP del dispositivo en la red de administración.

   c. Desde el cliente, introduzca esta URL para el instalador de dispositivos StorageGRID: **`https://services-appliance_IP:8443`**

      Para *`services-appliance_IP`*, Utilice la dirección DHCP.

   d. Si se le solicita una alerta de seguridad, vea e instale el certificado con el asistente de instalación del explorador.

      La alerta no aparecerá la próxima vez que acceda a esta URL.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID. La información y los mensajes que se muestran cuando accede por primera vez a esta página dependen de cómo el dispositivo está conectado actualmente a redes StorageGRID. Pueden aparecer mensajes de error que se resolverán en pasos posteriores.

2. Como alternativa, si no puede obtener una dirección IP mediante DHCP, utilice una conexión local de enlace para acceder al instalador de dispositivos de StorageGRID.

   a. Conecte un ordenador portátil de servicio directamente al puerto RJ-45 más derecho del dispositivo de servicios mediante un cable Ethernet.

Conexión local de enlace SG100

Conexión local de enlace SG1000

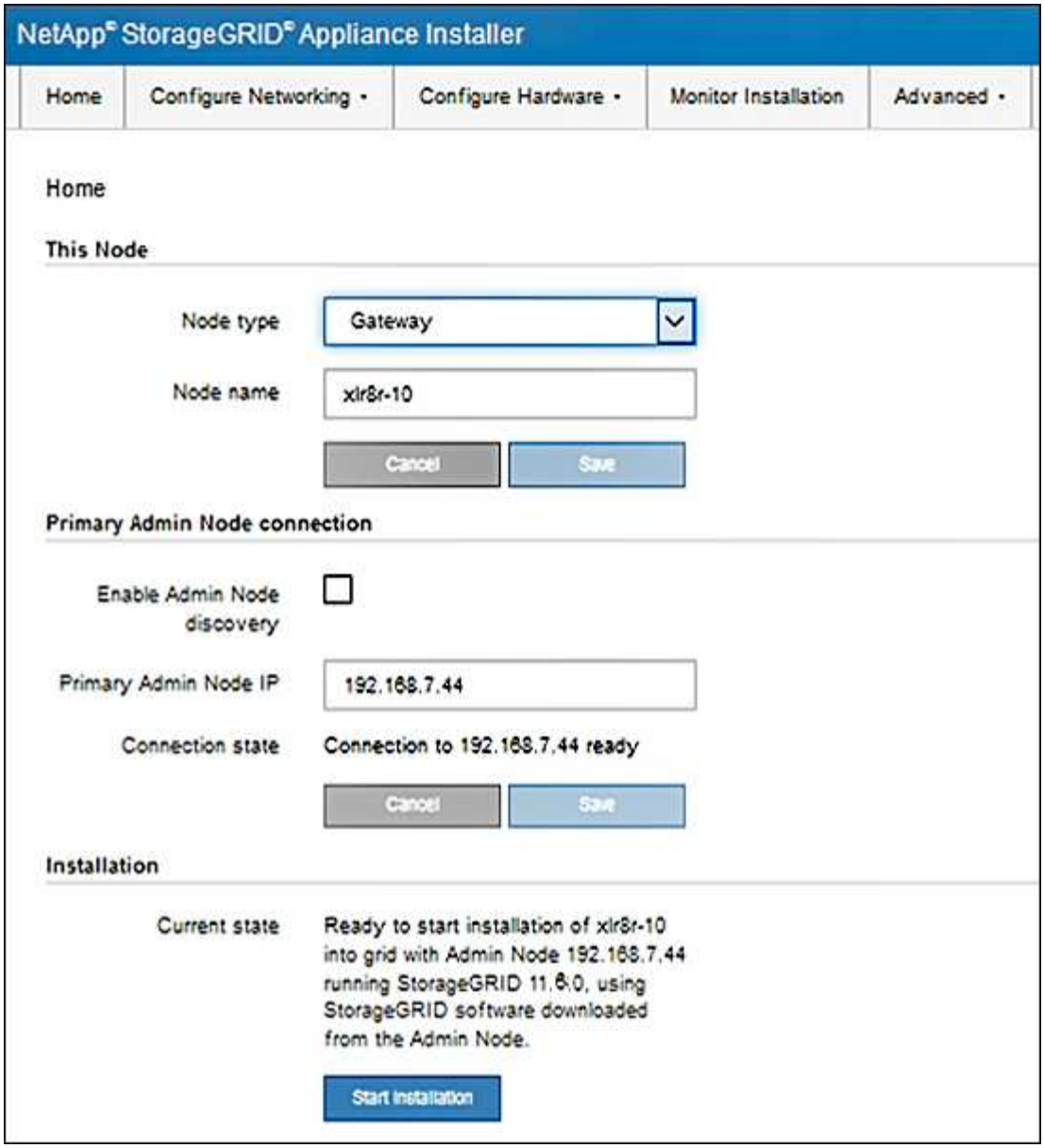
b. Abra un explorador web.

c. Introduzca esta URL para el instalador del dispositivo StorageGRID:
`https://169.254.0.1:8443`

Aparece la página de inicio del instalador de dispositivos de StorageGRID. La información y los mensajes que se muestran cuando accede por primera vez a esta página dependen de cómo el dispositivo está conectado actualmente a redes StorageGRID. Pueden aparecer mensajes de error que se resolverán en pasos posteriores.

> Si no puede acceder a la página de inicio a través de una conexión local de enlace, configure la dirección IP del portátil de servicio como `169.254.0.2`y vuelva a intentarlo.

3. Revise los mensajes que se muestran en la página Inicio y configure la configuración del vínculo y la configuración IP, según sea necesario.



Comprobar y actualizar la versión de StorageGRID Appliance Installer

La versión de instalador del dispositivo StorageGRID en el dispositivo debe coincidir con la versión de software instalada en el sistema StorageGRID para garantizar que todas las funciones de StorageGRID sean compatibles.

Lo que necesitará

Ha accedido al instalador de dispositivos de StorageGRID.

Acerca de esta tarea

Los dispositivos StorageGRID vienen de fábrica preinstalados con el instalador de dispositivos StorageGRID. Si va a añadir un dispositivo a un sistema StorageGRID actualizado recientemente, es posible que deba actualizar manualmente el instalador de dispositivos StorageGRID antes de instalar el dispositivo como un nodo nuevo.

El instalador de dispositivos de StorageGRID se actualiza automáticamente cuando se actualiza a una nueva versión de StorageGRID. No es necesario actualizar el instalador de dispositivos StorageGRID en los nodos

del dispositivo instalados. Este procedimiento sólo es necesario cuando se instala un dispositivo que contiene una versión anterior del instalador de dispositivos de StorageGRID.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Actualizar firmware**.
2. Compare la versión actual del firmware con la versión de software instalada en el sistema StorageGRID. (En la parte superior de Grid Manager, seleccione el icono de ayuda y seleccione **Acerca de**).

   El segundo dígito de las dos versiones debe coincidir. Por ejemplo, si el sistema StorageGRID está ejecutando la versión 11.**6**.*x*.*y*, la versión del instalador de dispositivos StorageGRID debe ser 3.**6**.*z*.

3. Si el dispositivo tiene una versión de nivel inferior del instalador de dispositivos de StorageGRID, vaya a. "Descargas de NetApp: Dispositivo de StorageGRID".

   Inicie sesión con el nombre de usuario y la contraseña de su cuenta de NetApp.

4. Descargue la versión adecuada del archivo **Soporte para dispositivos StorageGRID** y el archivo de suma de comprobación correspondiente.

   El archivo de soporte para dispositivos StorageGRID es un `.zip` archivo que contiene las versiones de firmware actuales y anteriores para todos los modelos de dispositivos StorageGRID, en subdirectorios para cada tipo de controlador.

   Después de descargar el archivo de soporte para dispositivos StorageGRID, extraiga el `.zip` archive y consulte el archivo README para obtener información importante sobre la instalación del instalador de dispositivos StorageGRID.

5. Siga las instrucciones de la página actualización del firmware del instalador del dispositivo StorageGRID para realizar estos pasos:
   a. Cargue el archivo de soporte (imagen de firmware) apropiado para el tipo de controladora y el archivo de suma de comprobación.
   b. Actualice la partición inactiva.
   c. Reiniciar e intercambiar particiones.
   d. Actualice la segunda partición (inactiva).

Información relacionada

Acceda al instalador de dispositivos de StorageGRID

Configurar enlaces de red (SG100 y SG1000)

Puede configurar los enlaces de red para los puertos utilizados para conectar el dispositivo a la red de grid, la red de cliente y la red de administración. Puede establecer la velocidad de enlace, así como los modos de enlace de red y puerto.

Lo que necesitará

- Ha obtenido el equipo adicional necesario para su tipo de cable y velocidad de enlace.
- Ha conectado los puertos de red a los switches que admiten la velocidad elegida.

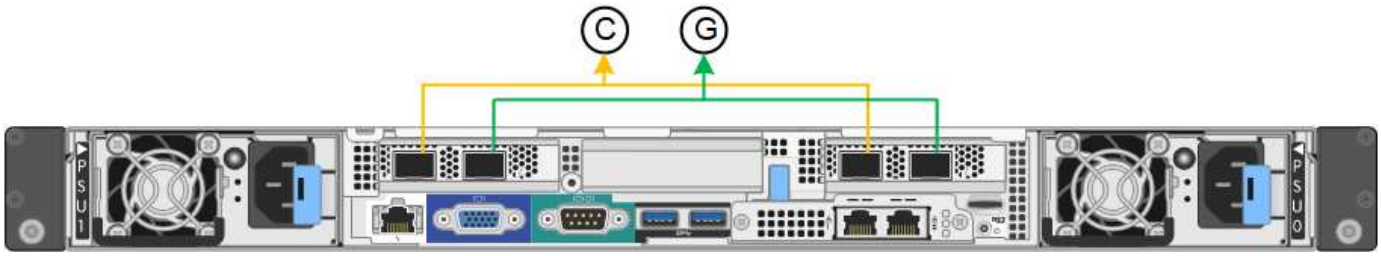
Si planea utilizar el modo de enlace de puerto de agregado, el modo de enlace de red LACP o el etiquetado de VLAN:

- Conectó los puertos de red del dispositivo a los switches que admiten VLAN y LACP.
- Si varios switches participan en el enlace LACP, los switches admiten grupos de agregación de enlaces de varios chasis (MLAG) o equivalente.
- Comprende cómo configurar los switches para que utilicen VLAN, LACP y MLAG o equivalente.
- Conoce la etiqueta de VLAN única que se utilizará para cada red. Esta etiqueta VLAN se añadirá a cada paquete de red para garantizar que el tráfico de red se dirija a la red correcta.

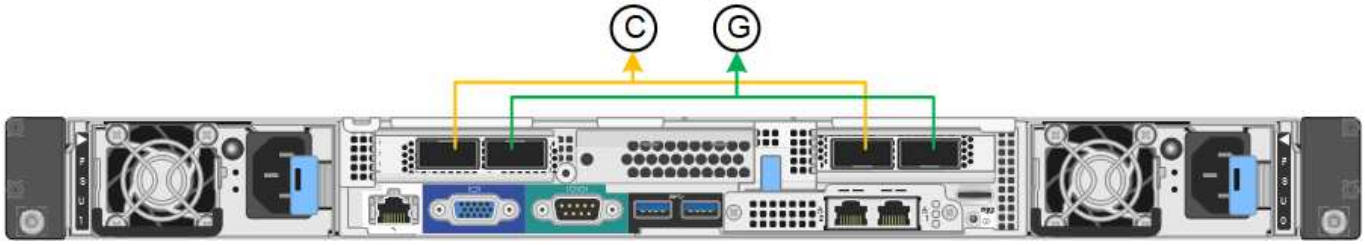
Acerca de esta tarea

Las figuras muestran cómo los cuatro puertos de red están Unidos en el modo de enlace de puerto fijo (configuración predeterminada).

Modo de enlace de puerto fijo SG100



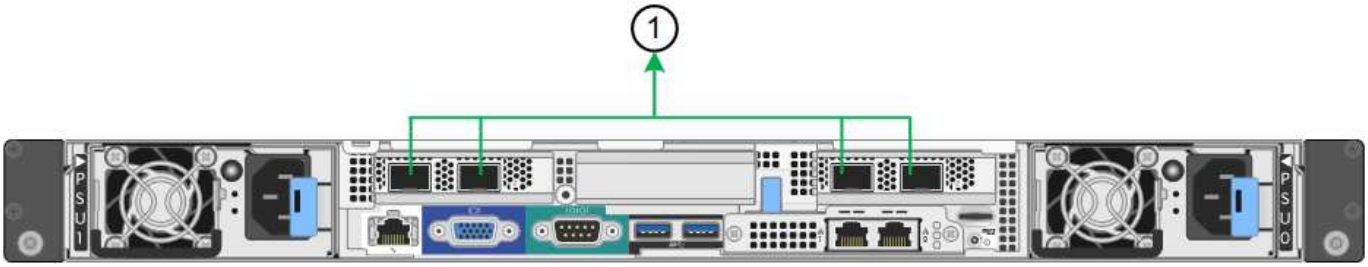
Modo de enlace de puerto fijo SG1000



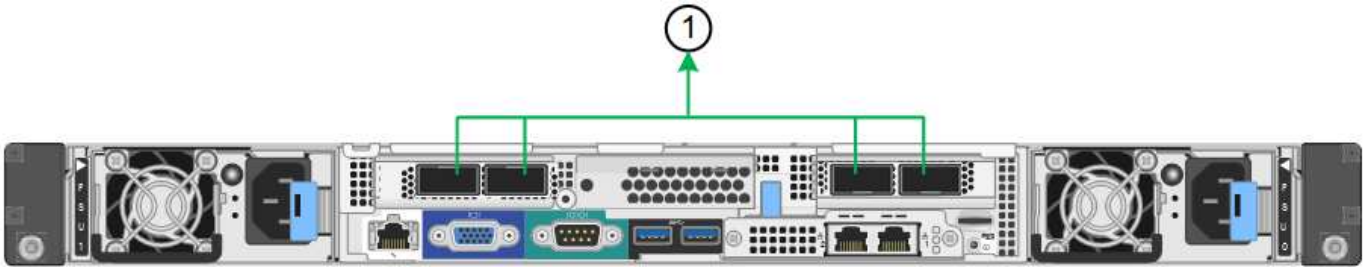
Llamada	Qué puertos están Unidos
C	Los puertos 1 y 3 se unen para la red cliente, si se utiliza esta red.
G	Los puertos 2 y 4 están Unidos para la red de cuadrícula.

En esta figura, se muestra cómo los cuatro puertos de red están Unidos en el modo de enlace de puerto agregado.

Modo de enlace de puerto agregado SG100



Modo de enlace de puerto agregado SG1000



Llamada	Qué puertos están Unidos
1	Los cuatro puertos se agrupan en un enlace LACP único, lo que permite que se usen todos los puertos para el tráfico de red de grid y de red de cliente.

La tabla resume las opciones para configurar los cuatro puertos de red. La configuración predeterminada se muestra en negrita. Sólo tiene que configurar los ajustes en la página Configuración de vínculos si desea utilizar un valor no predeterminado.

> De forma predeterminada, la política hash de transmisión LACP se establece en layer2+3 mode. Si es necesario, puede utilizar la API de gestión de grid para cambiarla al modo layer3+4.

- **Modo de enlace de puerto fijo (predeterminado)**

Modo de enlace de red	Red de cliente desactivada (predeterminada)	Red de cliente habilitada
Active-Backup (predeterminado)	• Los puertos 2 y 4 utilizan un vínculo de copia de seguridad activa para la red Grid. • Los puertos 1 y 3 no se usan. • Una etiqueta de VLAN es opcional.	• Los puertos 2 y 4 utilizan un vínculo de copia de seguridad activa para la red Grid. • Los puertos 1 y 3 utilizan un vínculo de backup activo para la red cliente. • Es posible especificar etiquetas de VLAN para ambas redes.
LACP (802.3ad)	• Los puertos 2 y 4 utilizan un enlace LACP para la red de grid. • Los puertos 1 y 3 no se usan. • Una etiqueta de VLAN es opcional.	• Los puertos 2 y 4 utilizan un enlace LACP para la red de grid. • Los puertos 1 y 3 utilizan un enlace LACP para la red de cliente. • Es posible especificar etiquetas de VLAN para ambas redes.

- **Modo de enlace de puerto agregado**

Modo de enlace de red	Red de cliente desactivada (predeterminada)	Red de cliente habilitada
Solo LACP (802.3ad)	• Los puertos 1-4 utilizan un enlace LACP único para la red de grid. • Una única etiqueta VLAN identifica los paquetes de red Grid.	• Los puertos 1-4 utilizan un enlace LACP único para la red de grid y la red de cliente. • Dos etiquetas VLAN permiten que los paquetes de red de cuadrícula se separen de los paquetes de red de cliente.

Para obtener información adicional, consulte el artículo sobre las conexiones de puerto GbE para el dispositivo de servicios.

Esta figura muestra cómo los dos puertos de gestión de 1 GbE de SG100 están Unidos en el modo de enlace de red Active-Backup para la red Admin.

Estas figuras muestran cómo los dos puertos de gestión de 1-GbE del dispositivo están Unidos en el modo de enlace de red de Active-Backup para la red de administración.

SG100 puertos de red de administración asociados

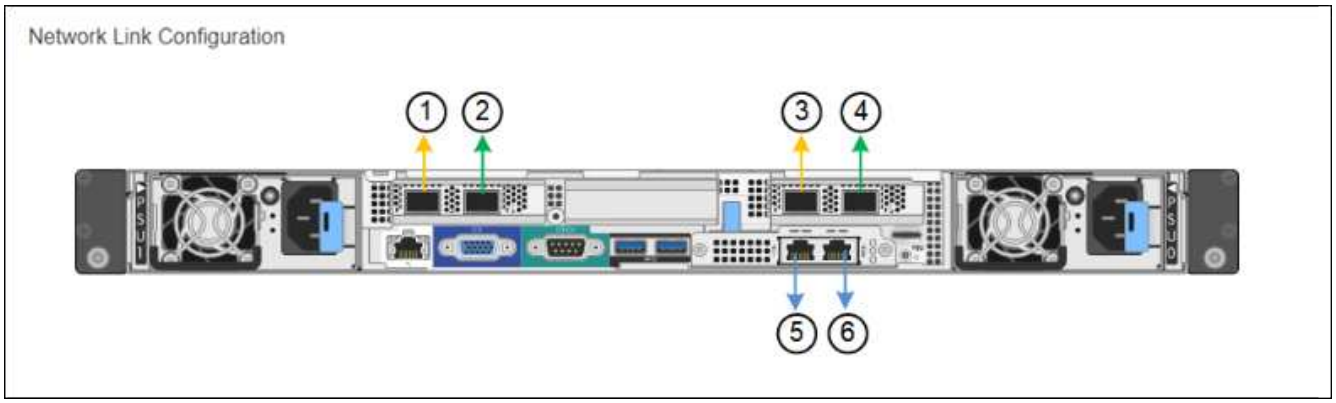
SG1000 puertos de red de administración asociados

Pasos

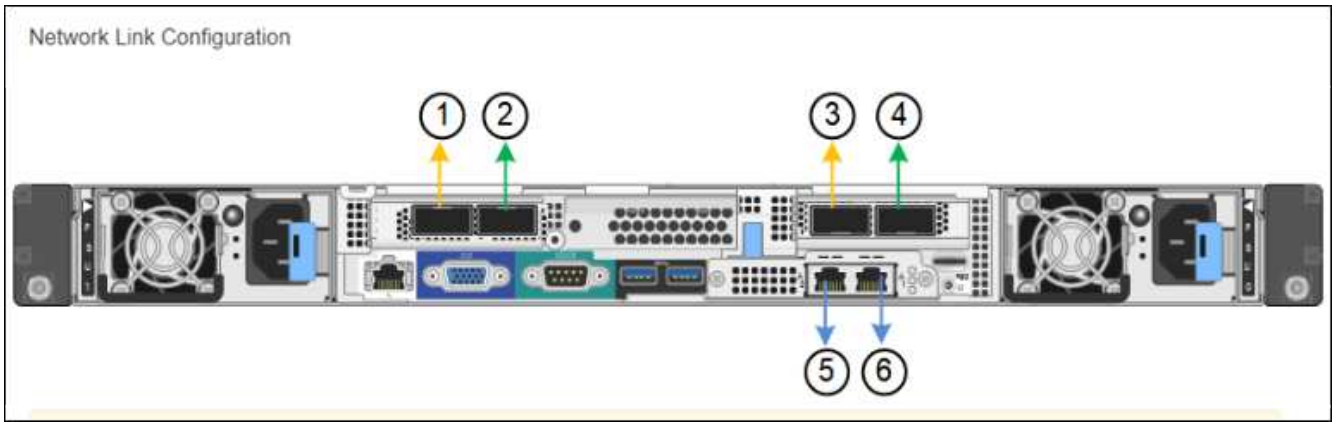
1. En la barra de menús del instalador del dispositivo StorageGRID, haga clic en **Configurar redes** > **Configuración de vínculo**.

   La página Network Link Configuration muestra un diagrama del dispositivo con los puertos de red y administración numerados.

   Puertos SG100



Puertos SG1000



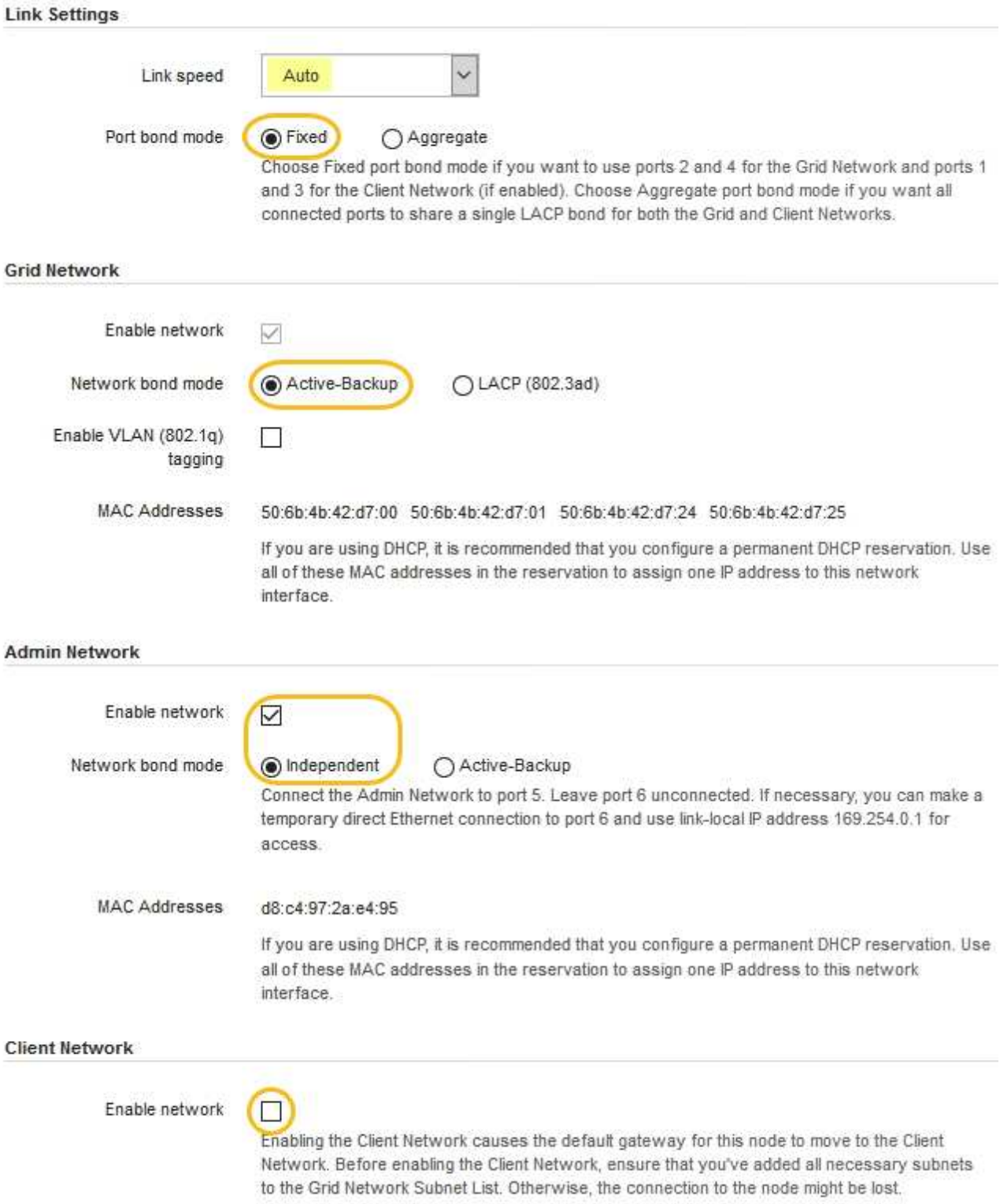
La tabla Estado del vínculo muestra el estado y la velocidad de los puertos numerados (se muestra SG1000).

Link Status

Link	State	Speed (Gbps)
1	Up	100
2	Down	N/A
3	Down	N/A
4	Down	N/A
5	Up	1
6	Up	1

La primera vez que acceda a esta página:

- **Velocidad de enlace** se ajusta en **Auto**.
- **El modo de enlace de puerto** está establecido en **fijo**.
- **El modo de enlace de red** se establece en **Active-Backup** para la red de cuadrícula.
- La **Red de administración** está activada y el modo de enlace de red se establece en **independiente**.
- La **Red cliente** está desactivada.



2. Seleccione la velocidad de enlace para los puertos de red en la lista desplegable **velocidad de enlace**.

   Los switches de red que utiliza para la red de cuadrícula y la red de cliente también deben ser compatibles y configurados para esta velocidad. Debe utilizar los adaptadores o transceptores adecuados para la velocidad de enlace configurada. Utilice la velocidad de enlace automático cuando sea posible porque esta opción negocia tanto la velocidad de enlace como el modo de corrección de error de avance (FEC) con el interlocutor de enlace.

3. Habilite o deshabilite las redes StorageGRID que tiene previsto utilizar.

   Se requiere la red de red. No se puede deshabilitar esta red.

   a. Si el dispositivo no está conectado a la red de administración, anule la selección de la casilla de verificación **Activar red** para la red de administración.

      Admin Network

      Enable network ☐

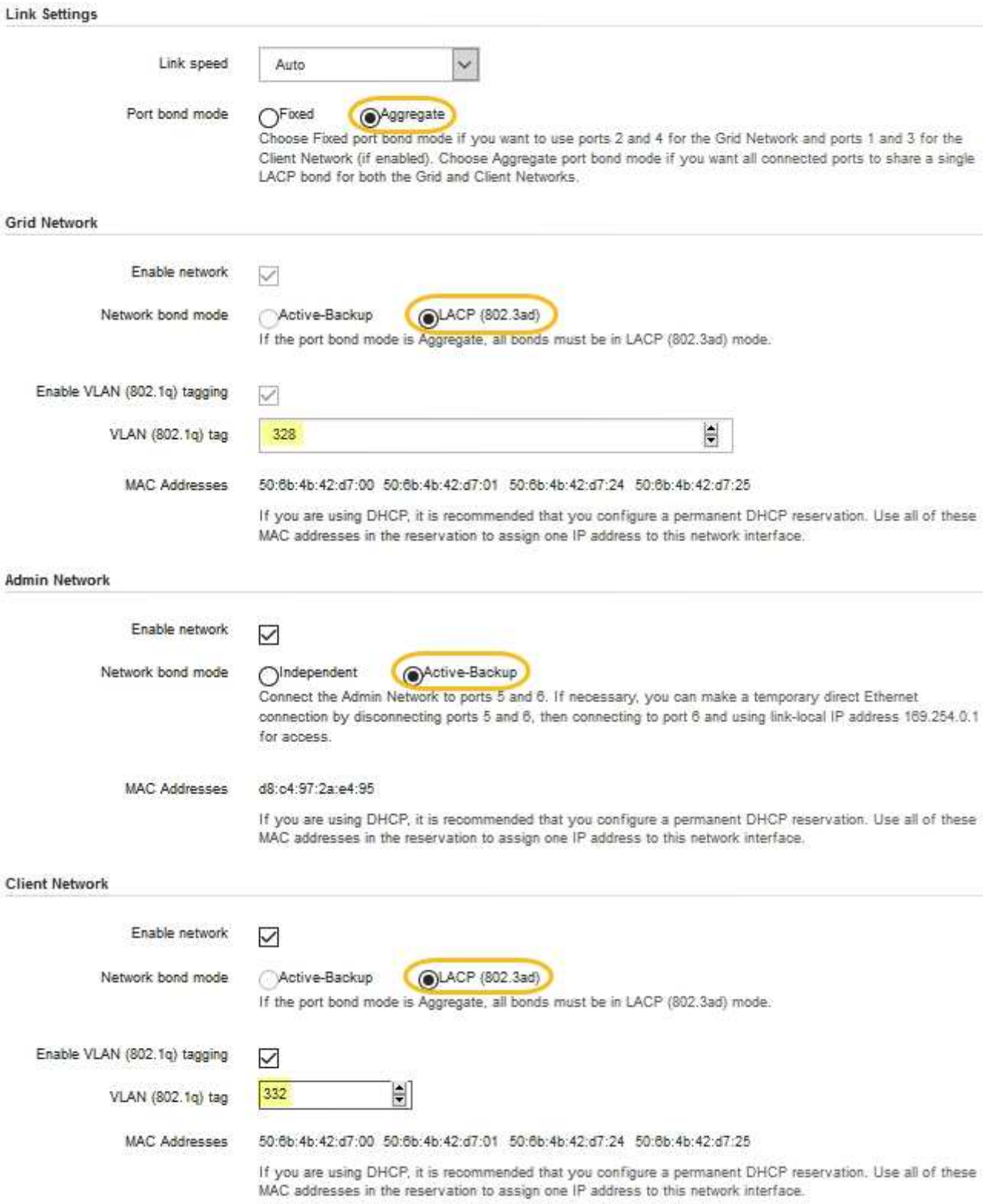
   b. Si el dispositivo está conectado a la red cliente, seleccione la casilla de verificación **Activar red** de la red cliente.

      Ahora se muestra la configuración de la red de cliente para los puertos NIC de datos.

4. Consulte la tabla y configure el modo de enlace de puerto y el modo de enlace de red.

   Este ejemplo muestra:

   - **Agregado** y **LACP** seleccionados para la red Grid y las redes cliente. Debe especificar una etiqueta de VLAN exclusiva para cada red. Puede seleccionar valores entre 0 y 4095.
   - **Active-Backup** seleccionado para la red de administración.



5. Cuando esté satisfecho con sus selecciones, haga clic en **Guardar**.

Puede perder la conexión si ha realizado cambios en la red o el enlace que está conectado a través de. Si no vuelve a conectarse en un minuto, vuelva a introducir la URL del instalador de dispositivos StorageGRID utilizando una de las otras direcciones IP asignadas al dispositivo:
https://*services_appliance_IP*:8443

Información relacionada

Obtener equipamiento y herramientas adicionales (SG100 y SG1000)

Configure las direcciones IP de StorageGRID

El instalador de dispositivos StorageGRID se utiliza para configurar las direcciones IP y la información de enrutamiento utilizadas para el dispositivo de servicios en las redes Grid, Admin y Cliente de StorageGRID.

Acerca de esta tarea

Debe asignar una IP estática al dispositivo en cada red conectada o asignar una concesión permanente a la dirección del servidor DHCP.

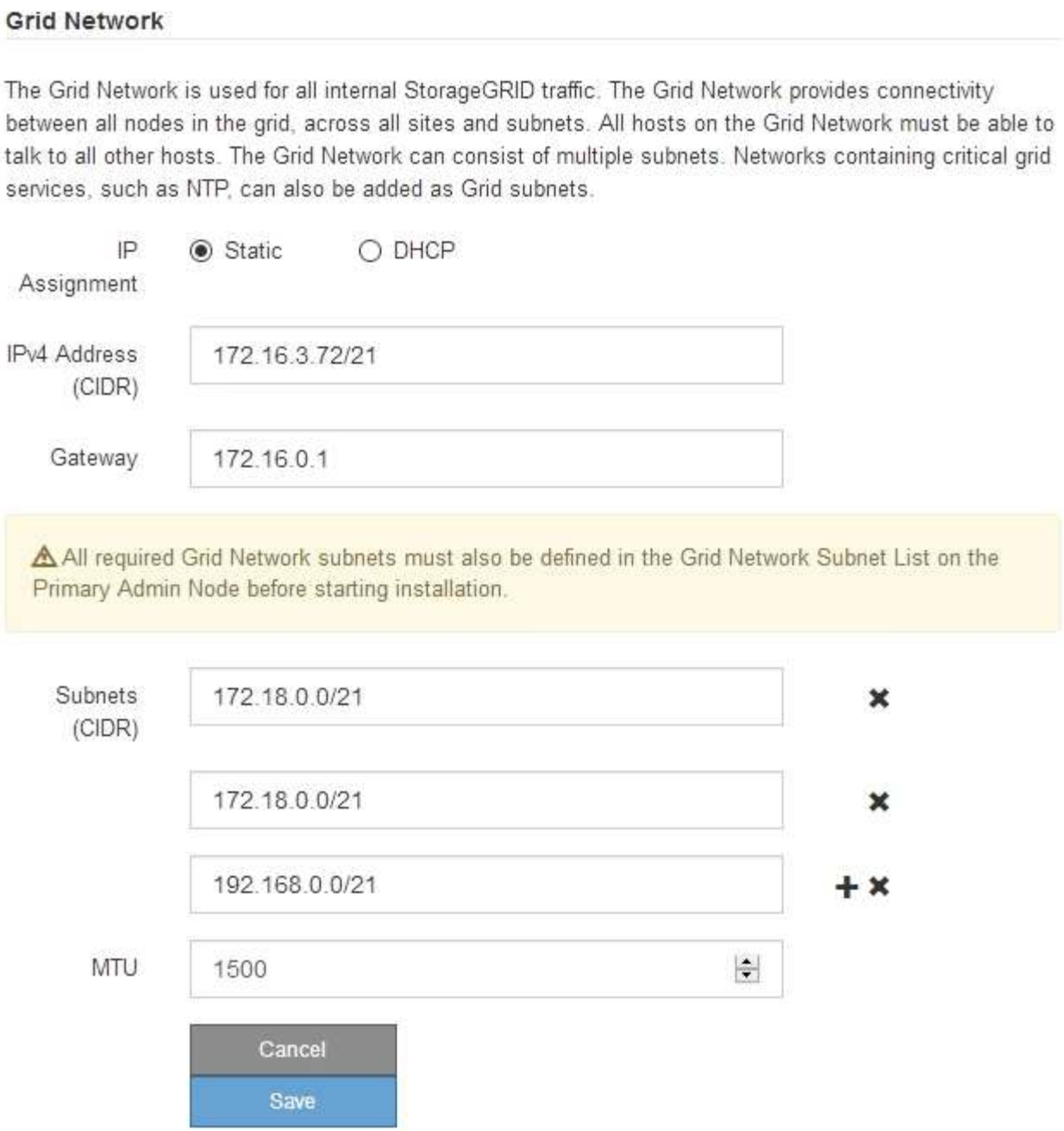
Si desea cambiar la configuración del enlace, consulte las instrucciones para cambiar la configuración del vínculo del dispositivo de servicios.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Configurar redes** > **Configuración IP**.

   Aparece la página Configuración de IP.

2. Para configurar Grid Network, seleccione **Static** o **DHCP** en la sección **Grid Network** de la página.



3. Si ha seleccionado **estático**, siga estos pasos para configurar la red de cuadrícula:
   a. Introduzca la dirección IPv4 estática utilizando la notación CIDR.
   b. Introduzca la puerta de enlace.

      Si la red no tiene una puerta de enlace, vuelva a introducir la misma dirección IPv4 estática.

   c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

      > 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. Los valores de MTU no tienen que ser iguales para todos los tipos de red.

d. Haga clic en **Guardar**.

   Al cambiar la dirección IP, la pasarela y la lista de subredes también pueden cambiar.

   Si pierde la conexión con el instalador de dispositivos StorageGRID, vuelva a introducir la URL con la nueva dirección IP estática que acaba de asignar. Por ejemplo, `https://services_appliance_IP:8443`

e. Confirme que la lista de subredes de red es correcta.

   Si tiene 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. Estas subredes de red de cuadrícula también deben definirse en la Lista de subredes de red de cuadrícula del nodo de administración principal al iniciar la instalación de StorageGRID.

   > La ruta predeterminada no aparece en la lista. Si la red de cliente no está activada, la ruta predeterminada utilizará la puerta de enlace de red de cuadrícula.

   - Para agregar una subred, haga clic en el icono de inserción ➕ a la derecha de la última entrada.
   - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

f. Haga clic en **Guardar**.

4. Si ha seleccionado **DHCP**, siga estos pasos para configurar Grid Network:

a. Después de seleccionar el botón de opción **DHCP**, haga clic en **Guardar**.

   Los campos **Dirección IPv4**, **Puerta de enlace** y **subredes** se rellenan automáticamente. Si el servidor DHCP está configurado para asignar un valor MTU, el campo **MTU** se rellena con ese valor y el campo pasa a ser de sólo lectura.

   El navegador web se redirige automáticamente a la nueva dirección IP para el instalador de dispositivos StorageGRID.

b. Confirme que la lista de subredes de red es correcta.

   Si tiene 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. Estas subredes de red de cuadrícula también deben definirse en la Lista de subredes de red de cuadrícula del nodo de administración principal al iniciar la instalación de StorageGRID.

   > La ruta predeterminada no aparece en la lista. Si la red de cliente no está activada, la ruta predeterminada utilizará la puerta de enlace de red de cuadrícula.

   - Para agregar una subred, haga clic en el icono de inserción ➕ a la derecha de la última entrada.
   - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes,

como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

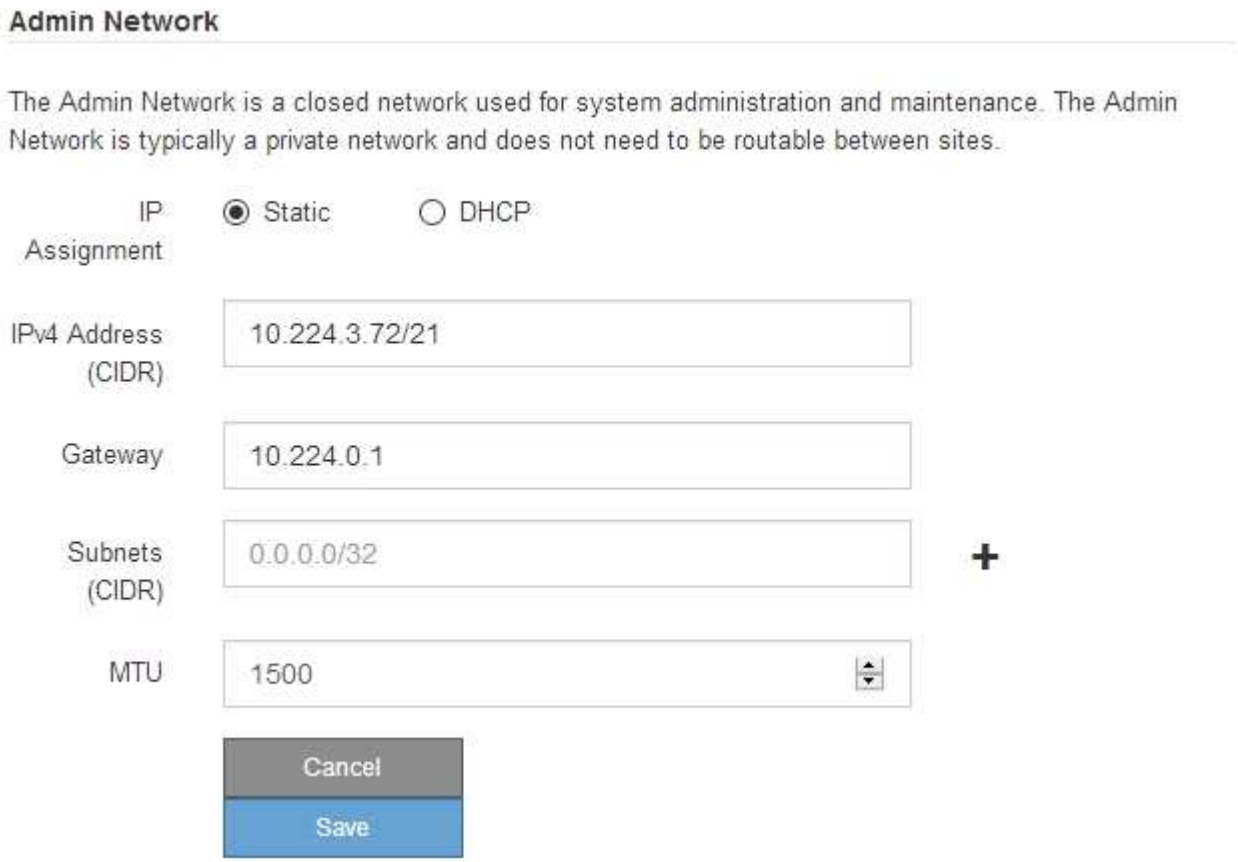
> El valor de MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, pueden ocurrir problemas de rendimiento de red o pérdida de paquetes.

> 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. Los valores de MTU no tienen que ser iguales para todos los tipos de red.

a. Haga clic en **Guardar**.

5. Para configurar la Red de administración, seleccione **estático** o **DHCP** en la sección Red de administración de la página.

> Para configurar la Red de administración, debe activar la Red de administración en la página Configuración de vínculos.



6. Si ha seleccionado **estático**, siga estos pasos para configurar la red de administración:

   a. Introduzca la dirección IPv4 estática, mediante la notación CIDR, para el puerto de gestión 1 del dispositivo.

      El puerto de gestión 1 está a la izquierda de los dos puertos RJ45 de 1-GbE del extremo derecho del dispositivo.

b. Introduzca la puerta de enlace.

   Si la red no tiene una puerta de enlace, vuelva a introducir la misma dirección IPv4 estática.

c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

   > 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.

d. Haga clic en **Guardar**.

   Al cambiar la dirección IP, la pasarela y la lista de subredes también pueden cambiar.

   Si pierde la conexión con el instalador de dispositivos StorageGRID, vuelva a introducir la URL con la nueva dirección IP estática que acaba de asignar. Por ejemplo, `https://services_appliance:8443`

e. Confirme que la lista de subredes de la red administrativa es correcta.

   Debe verificar que se pueda acceder a todas las subredes mediante la puerta de enlace que ha proporcionado.

   > No se puede realizar la ruta predeterminada para utilizar la puerta de enlace de red de administración.

   - Para agregar una subred, haga clic en el icono de inserción + a la derecha de la última entrada.
   - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

f. Haga clic en **Guardar**.

7. Si ha seleccionado **DHCP**, siga estos pasos para configurar la red de administración:

   a. Después de seleccionar el botón de opción **DHCP**, haga clic en **Guardar**.

      Los campos **Dirección IPv4**, **Puerta de enlace** y **subredes** se rellenan automáticamente. Si el servidor DHCP está configurado para asignar un valor MTU, el campo **MTU** se rellena con ese valor y el campo pasa a ser de sólo lectura.

      El navegador web se redirige automáticamente a la nueva dirección IP para el instalador de dispositivos StorageGRID.

   b. Confirme que la lista de subredes de la red administrativa es correcta.

      Debe verificar que se pueda acceder a todas las subredes mediante la puerta de enlace que ha proporcionado.

      > No se puede realizar la ruta predeterminada para utilizar la puerta de enlace de red de administración.

      - Para agregar una subred, haga clic en el icono de inserción + a la derecha de la última entrada.
      - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

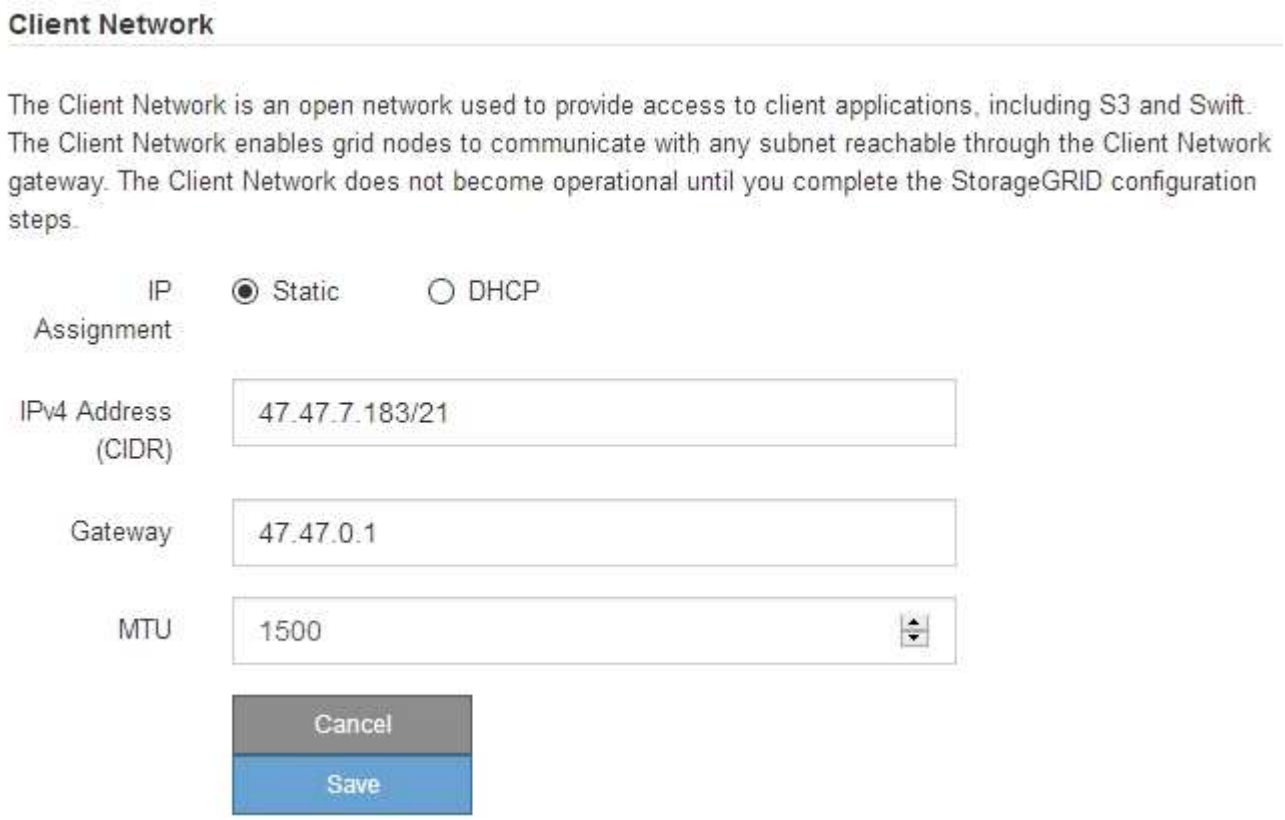
c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

> 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.

d. Haga clic en **Guardar**.

8. Para configurar la red de cliente, seleccione **Static** o **DHCP** en la sección **Client Network** de la página.

> Para configurar la red de cliente, debe activar la red de cliente en la página Configuración de vínculos.



9. Si ha seleccionado **estático**, siga estos pasos para configurar la red de cliente:

a. Introduzca la dirección IPv4 estática utilizando la notación CIDR.

b. Haga clic en **Guardar**.

c. Confirme que la dirección IP de la puerta de enlace de red de cliente es correcta.

> Si la red de cliente está activada, se muestra la ruta predeterminada. La ruta predeterminada utiliza la puerta de enlace de red de cliente y no se puede mover a otra interfaz mientras la red de cliente está activada.

d. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

> 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.

e. Haga clic en **Guardar**.

10. Si ha seleccionado **DHCP**, siga estos pasos para configurar la red de cliente:

    a. Después de seleccionar el botón de opción **DHCP**, haga clic en **Guardar**.

    Los campos **Dirección IPv4** y **Puerta de enlace** se rellenan automáticamente. Si el servidor DHCP está configurado para asignar un valor MTU, el campo **MTU** se rellena con ese valor y el campo pasa a ser de sólo lectura.

    El navegador web se redirige automáticamente a la nueva dirección IP para el instalador de dispositivos StorageGRID.

    a. Confirme que la puerta de enlace es correcta.

    > Si la red de cliente está activada, se muestra la ruta predeterminada. La ruta predeterminada utiliza la puerta de enlace de red de cliente y no se puede mover a otra interfaz mientras la red de cliente está activada.

    b. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

    > 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.

Información relacionada

Cambiar la configuración del vínculo del dispositivo de servicios

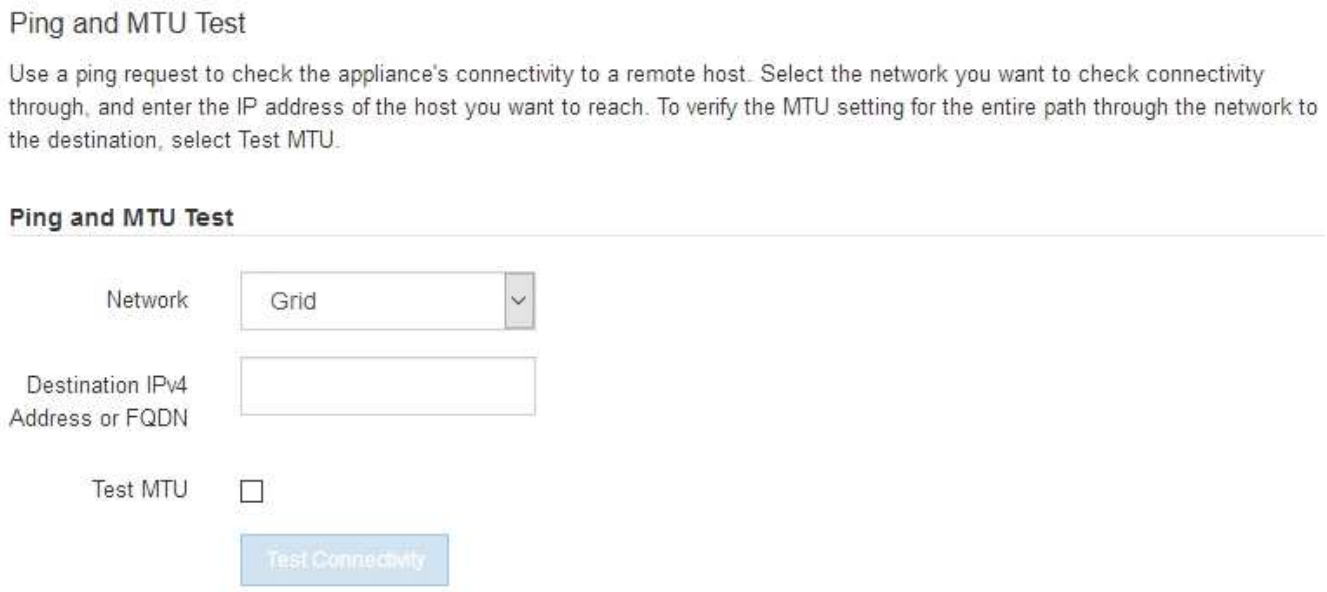
Compruebe las conexiones de red

Debe confirmar que puede acceder a las redes StorageGRID que está utilizando desde el dispositivo. Para validar el enrutamiento mediante puertas de enlace de red, debe probar la conectividad entre el instalador de dispositivos de StorageGRID y las direcciones IP en subredes diferentes. También puede verificar la configuración de MTU.

Pasos

1. En la barra de menús del instalador del dispositivo StorageGRID, haga clic en **Configurar redes** > **Ping y prueba de MTU**.

   Aparece la página pruebas de ping y MTU.



2. En el cuadro desplegable **Red**, seleccione la red que desea probar: Grid, Admin o Client.
3. Introduzca la dirección IPv4 o el nombre de dominio completo (FQDN) correspondiente a un host en esa red.

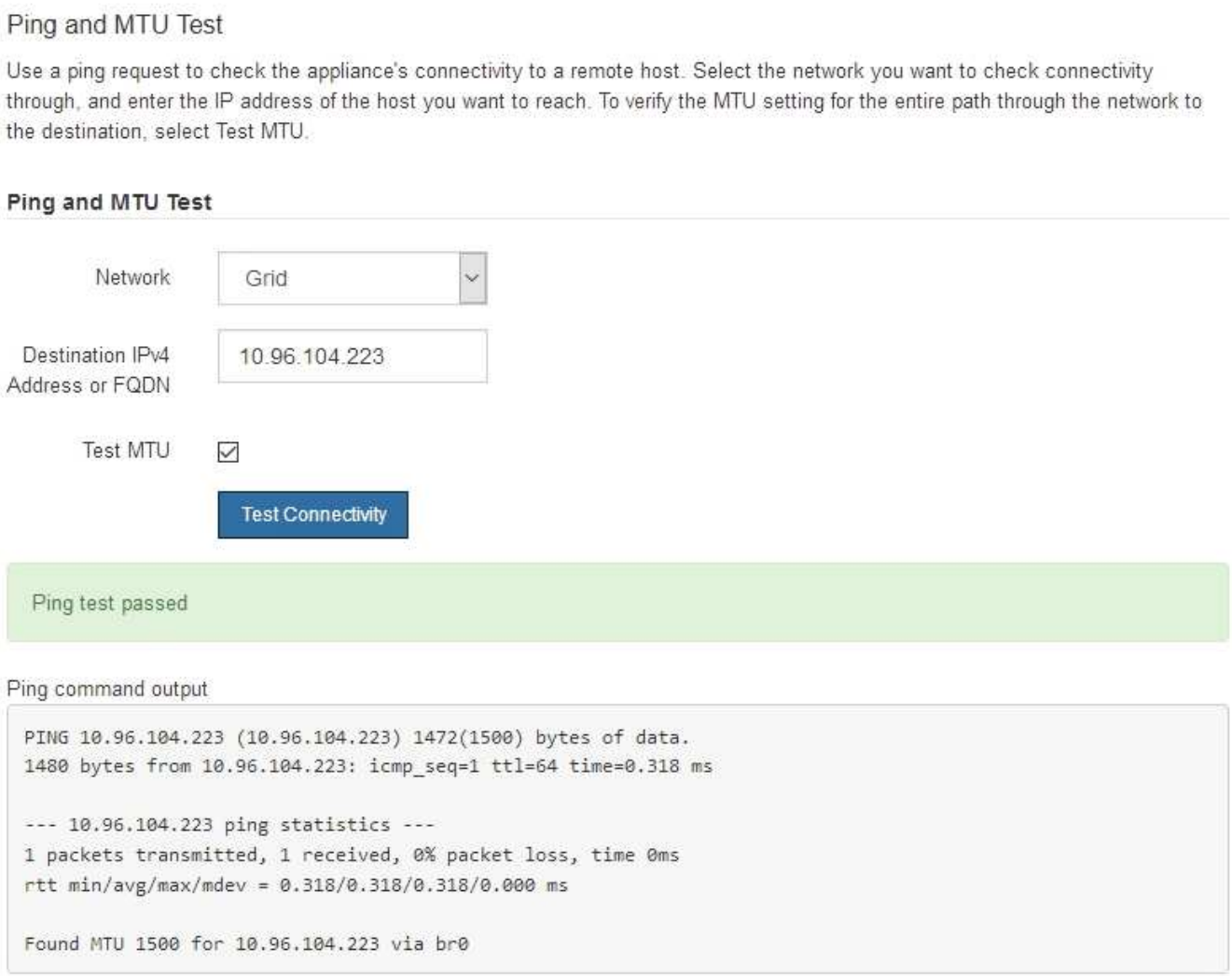
   Por ejemplo, puede hacer ping a la puerta de enlace de la red o al nodo de administración principal.

4. Opcionalmente, active la casilla de verificación **probar MTU** para comprobar la configuración de MTU para toda la ruta de acceso a través de la red hasta el destino.

   Por ejemplo, puede probar la ruta entre el nodo del dispositivo y un nodo en un sitio diferente.

5. Haga clic en **probar conectividad**.

   Si la conexión de red es válida, aparece el mensaje "Ping test pased", con la salida del comando ping en la lista.



Información relacionada

Configurar enlaces de red (SG100 y SG1000)

Cambie la configuración de MTU

Verifique las conexiones de red a nivel de puerto

Para garantizar que los firewalls no obstruyan el acceso entre el instalador del dispositivo StorageGRID y otros nodos, confirme que el instalador del dispositivo StorageGRID puede conectarse a un puerto TCP o a un conjunto de puertos en la dirección IP o el rango de direcciones especificados.

Acerca de esta tarea

Con la lista de puertos que se incluye en el instalador de dispositivos de StorageGRID, puede probar la conectividad entre el dispositivo y los demás nodos de la red de grid.

Además, puede probar la conectividad en las redes de administración y cliente y en los puertos UDP, como los que se utilizan para servidores NFS o DNS externos. Para obtener una lista de estos puertos, consulte la referencia de puertos en las directrices de red de StorageGRID.

Los puertos de red de red enumerados en la tabla de conectividad de puertos sólo son válidos para StorageGRID versión 11.6.0. Para verificar qué puertos son correctos para cada tipo de nodo, siempre debe consultar las directrices de red para su versión de StorageGRID.

Pasos

1. En el instalador del dispositivo StorageGRID, haga clic en **Configurar red** > **Prueba de conectividad de puerto (nmap)**.

   Aparece la página Prueba de conectividad de puerto.

   La tabla de conectividad de puertos enumera los tipos de nodos que requieren conectividad TCP en la red de cuadrícula. Para cada tipo de nodo, la tabla enumera los puertos de red de cuadrícula a los que el dispositivo debe acceder.

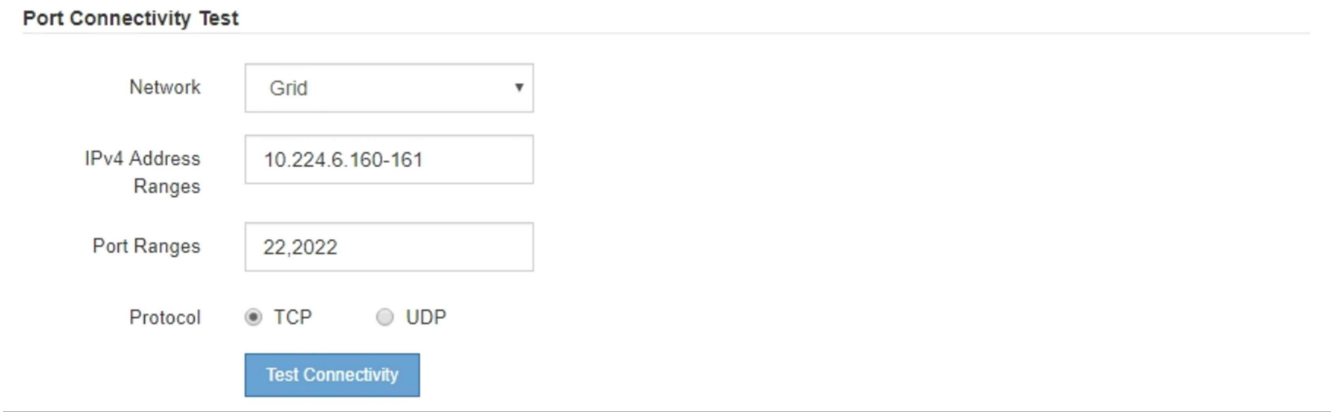
   Puede probar la conectividad entre los puertos del dispositivo que aparecen en la tabla y los demás nodos de la red de grid.

2. En el menú desplegable **Red**, seleccione la red que desea probar: **Grid**, **Admin** o **Cliente**.
3. Especifique un rango de direcciones IPv4 para los hosts en esa red.

   Por ejemplo, es posible que desee sondear la puerta de enlace en la red o en el nodo de administración principal.

   Especifique un rango utilizando un guión, como se muestra en el ejemplo.

4. Introduzca un número de puerto TCP, una lista de puertos separados por comas o un intervalo de puertos.



5. Haga clic en **probar conectividad**.

   - Si las conexiones de red a nivel de puerto seleccionadas son válidas, el mensaje "'Prueba de conectividad de puerto superada'" aparece en un banner verde. El resultado del comando nmap se muestra debajo del banner.

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- Si se realiza una conexión de red a nivel de puerto al host remoto, pero el host no escucha en uno o más de los puertos seleccionados, el mensaje "'error de prueba de conectividad de puerto'" aparece en un banner amarillo. El resultado del comando nmap se muestra debajo del banner.

  Cualquier puerto remoto al que no esté escuchando el host tiene un estado de "'cerrado'". Por ejemplo, puede ver este banner amarillo cuando el nodo al que intenta conectarse está en estado preinstalado y el servicio NMS de StorageGRID aún no se está ejecutando en ese nodo.

Port connectivity test failed
Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
1504/tcp closed evb-elm
1505/tcp open   funkproxy
1506/tcp open   utcd
1508/tcp open   diagmond
7443/tcp open   oracleas-https
9999/tcp open   abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- Si no se puede establecer una conexión de red a nivel de puerto para uno o más puertos seleccionados, el mensaje "'Port Connectivity test failed'" aparece en un banner rojo. El resultado del comando nmap se muestra debajo del banner.

  El banner rojo indica que se ha realizado un intento de conexión TCP a un puerto en el host remoto, pero no se ha devuelto nada al remitente. Cuando no se devuelve ninguna respuesta, el puerto tiene un estado de "filtrado" y es probable que sea bloqueado por un firewall.

  ⓘ También se enumeran los puertos con «'cerrado'».

Port connectivity test failed
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT     STATE    SERVICE
22/tcp   open     ssh
79/tcp   filtered finger
80/tcp   open     http
443/tcp  open     https
1504/tcp closed   evb-elm
1505/tcp open     funkproxy
1506/tcp open     utcd
1508/tcp open     diagmond
7443/tcp open     oracleas-https
9999/tcp open     abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

Información relacionada

Directrices sobre redes

Configurar la interfaz BMC (SG100 y SG1000)

La interfaz de usuario del controlador de administración de la placa base (BMC) en el dispositivo de servicios proporciona información de estado sobre el hardware y permite configurar los ajustes SNMP y otras opciones para el dispositivo de servicios.

Cambie la contraseña raíz de la interfaz de BMC

Por motivos de seguridad, debe cambiar la contraseña del usuario raíz del BMC.

Lo que necesitará

El cliente de gestión está usando un navegador web compatible.

Acerca de esta tarea

Al instalar el dispositivo por primera vez, el BMC utiliza una contraseña predeterminada para el usuario raíz (`root/calvin`). Debe cambiar la contraseña del usuario raíz para proteger el sistema.

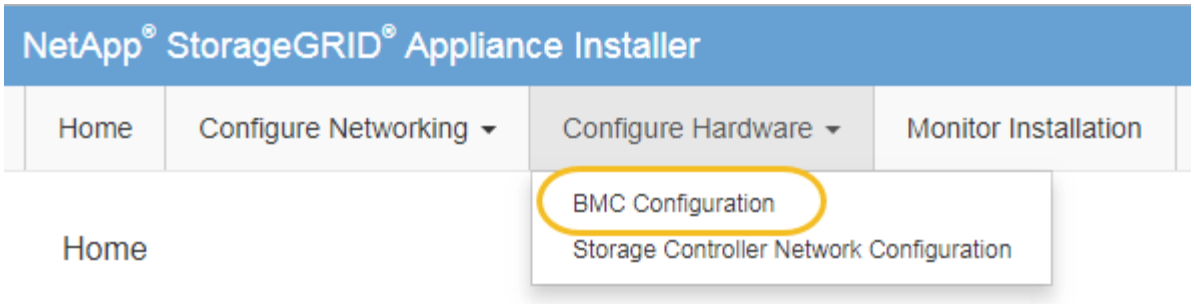
Pasos

1. Desde el cliente, introduzca la URL del instalador de dispositivos de StorageGRID: **`https://`*`services_appliance_IP`*`:8443`**

   Para `services_appliance_IP`, Utilice la dirección IP del dispositivo en cualquier red StorageGRID.

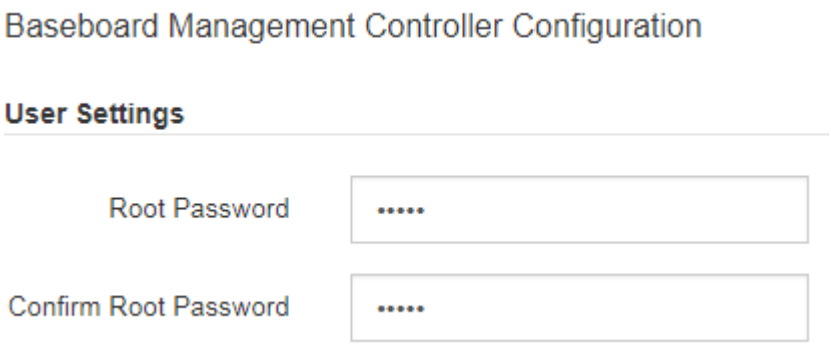
   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Configurar hardware Configuración de BMC**.



Aparece la página Configuración de la controladora de gestión de placa base.

3. Introduzca una nueva contraseña para la cuenta raíz en los dos campos proporcionados.



4. Haga clic en **Guardar**.

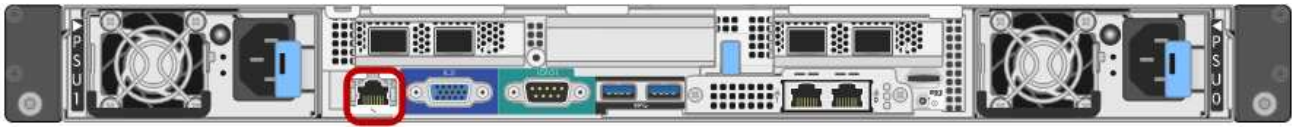
Establezca la dirección IP para el puerto de administración de BMC

Para poder acceder a la interfaz del BMC, debe configurar la dirección IP para el puerto de administración del BMC en el dispositivo de servicios.

Lo que necesitará

- El cliente de gestión está usando un navegador web compatible.
- Está usando cualquier cliente de gestión que pueda conectarse a una red StorageGRID.
- El puerto de gestión del BMC está conectado a la red de gestión que tiene previsto utilizar.

SG100 Puerto de gestión BMC



Puerto de administración de SG1000 BMC

Acerca de esta tarea

Para fines de soporte, el puerto de gestión del BMC permite un acceso bajo al hardware. Solo debe conectar este puerto a una red de gestión interna segura y de confianza. Si no hay ninguna red disponible, deje el puerto BMC desconectado o bloqueado, a menos que el soporte técnico solicite una conexión a BMC.

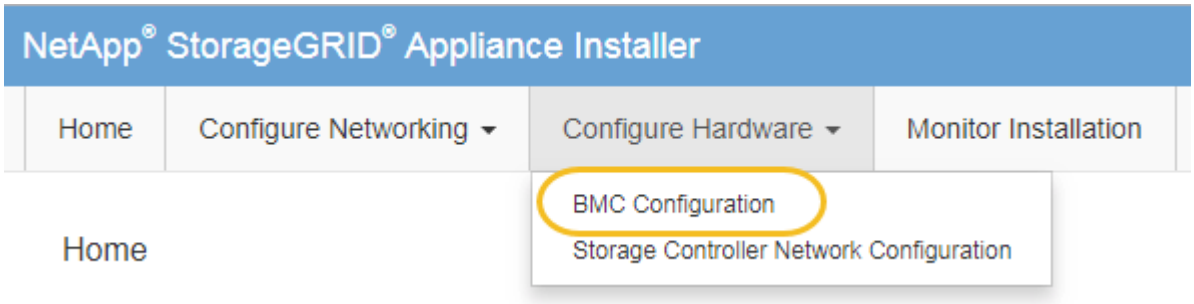
Pasos

1. Desde el cliente, introduzca la URL del instalador de dispositivos de StorageGRID: **`https://services_appliance_IP:8443`**

   Para *`services_appliance_IP`*, Utilice la dirección IP del dispositivo en cualquier red StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Configurar hardware Configuración de BMC**.

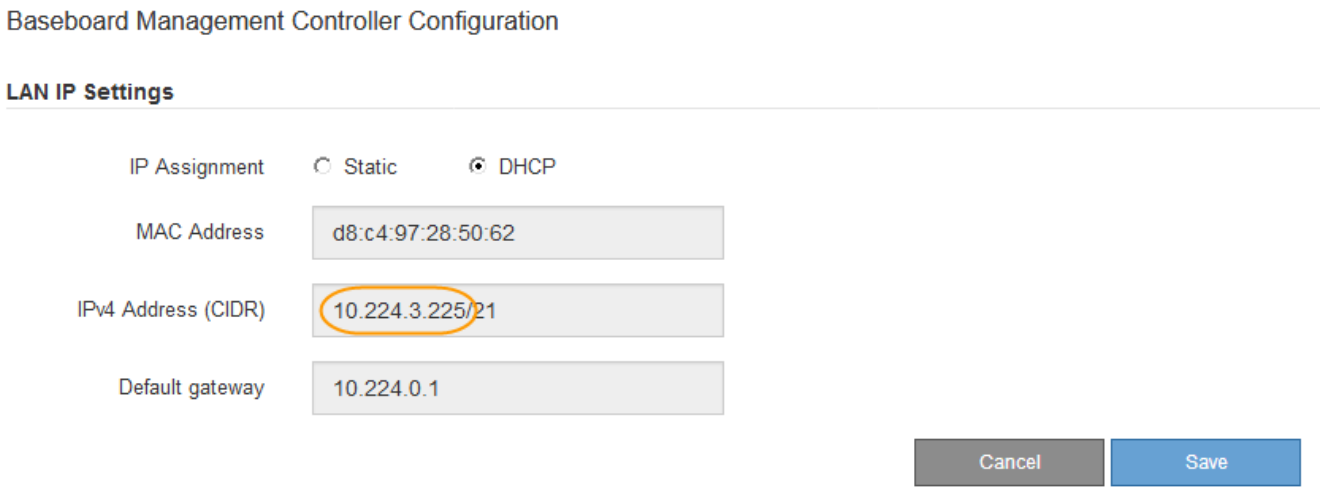


   Aparece la página Configuración de la controladora de gestión de placa base.

3. Anote la dirección IPv4 que se muestra automáticamente.

   DHCP es el método predeterminado para asignar una dirección IP a este puerto.

   Puede que los valores de DHCP deban tardar varios minutos en aparecer.



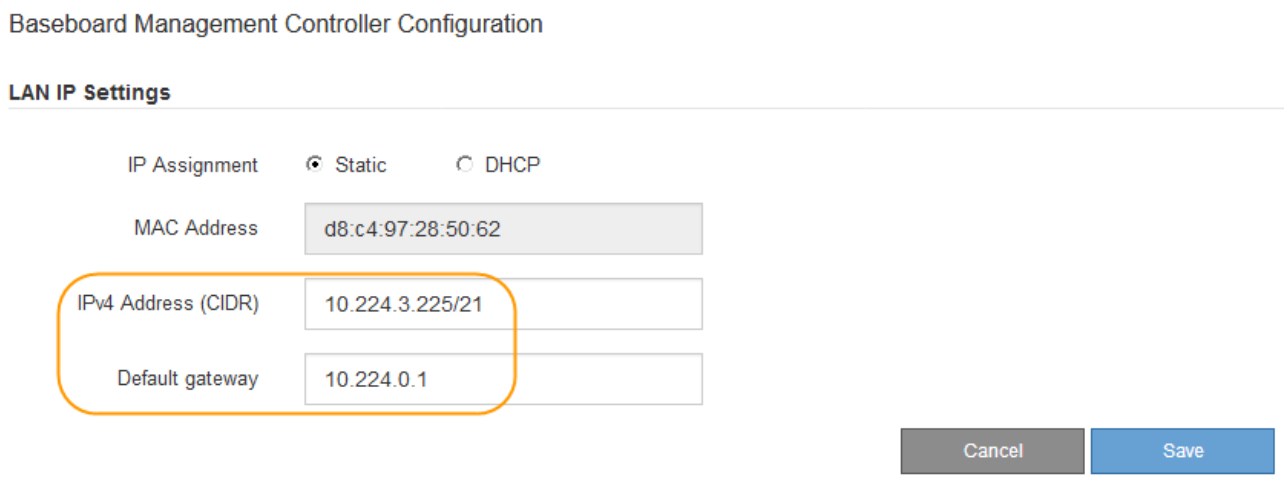
4. De manera opcional, establezca una dirección IP estática para el puerto de gestión del BMC.

> Debe asignar una IP estática al puerto de gestión de BMC o una concesión permanente para la dirección en el servidor DHCP.

a. Seleccione **estático**.

b. Introduzca la dirección IPv4 mediante la notación CIDR.

c. Introduzca la pasarela predeterminada.



d. Haga clic en **Guardar**.

Puede que los cambios se apliquen en unos minutos.

Acceda a la interfaz de BMC

Puede acceder a la interfaz del BMC en el dispositivo de servicios mediante la dirección IP estática o DHCP del puerto de gestión del BMC.

Lo que necesitará

- El cliente de gestión está usando un navegador web compatible.
- El puerto de administración de BMC del dispositivo de servicios está conectado a la red de administración que planea utilizar.

SG100 Puerto de gestión BMC

Puerto de administración de SG1000 BMC

Pasos

1. Introduzca la dirección URL de la interfaz del BMC:
   `https://BMC_Port_IP`

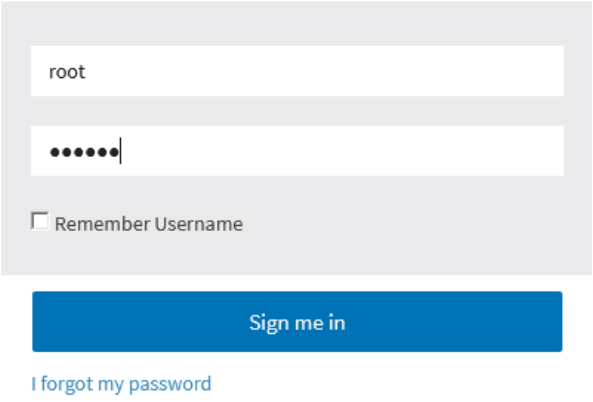
   Para *`BMC_Port_IP`*, Utilice la dirección IP estática o DHCP para el puerto de administración del BMC.

   Aparece la página de inicio de sesión de BMC.

   > Si aún no ha configurado `BMC_Port_IP` siga las instrucciones de Configurar la interfaz BMC (SG100/SG1000). Si no puede seguir este procedimiento debido a un problema de hardware y aún no ha configurado una dirección IP de BMC, es posible que aún pueda acceder al BMC. De forma predeterminada, el BMC obtiene una dirección IP mediante DHCP. Si DHCP está activado en la red BMC, el administrador de red puede proporcionar la dirección IP asignada al BMC MAC, que se imprime en la etiqueta situada en la parte frontal del controlador SG6000-CN. Si DHCP no está habilitado en la red BMC, el BMC no responderá después de unos minutos y se asignará la IP estática predeterminada `192.168.0.120`. Es posible que necesite conectar su portátil directamente al puerto BMC y cambiar la configuración de red para asignar una IP a su portátil `192.168.0.200/24`, para navegar a. `192.168.0.120`.

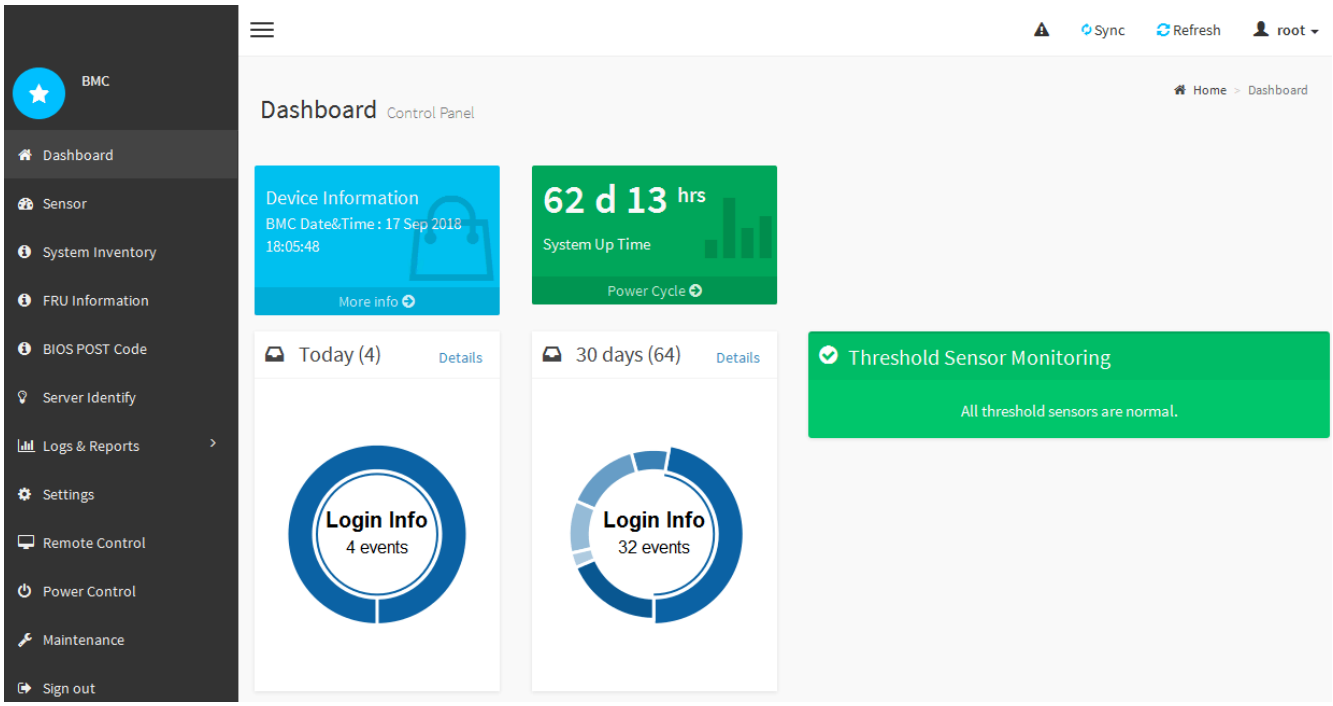
2. Introduzca el nombre de usuario raíz y la contraseña, utilizando la contraseña que estableció al cambiar la contraseña raíz predeterminada:
   `root`

   `password`



3. Haga clic en **Iniciar sesión**

   Aparece el panel BMC.



4. Opcionalmente, cree usuarios adicionales seleccionando **Ajustes Gestión de usuarios** y haciendo clic en cualquier usuario "desactivado".

> Cuando los usuarios inician sesión por primera vez, es posible que se les pida que cambien su contraseña para aumentar la seguridad.

Información relacionada

Cambie la contraseña raíz de la interfaz del BMC

Configurar los ajustes SNMP para el dispositivo de servicios

Si está familiarizado con la configuración de SNMP para el hardware, puede utilizar la interfaz BMC para configurar los ajustes SNMP para el dispositivo de servicios. Puede proporcionar cadenas de comunidad seguras, habilitar capturas SNMP y especificar hasta cinco destinos SNMP.

Lo que necesitará

- Sabe cómo acceder al panel de BMC.
- Tiene experiencia en la configuración de la configuración de SNMP para el equipo SNMPv1-v2c.

> Es posible que los ajustes del BMC realizados con este procedimiento no se conserven si el aparato falla y se tiene que sustituir. Asegúrese de que tiene un registro de todos los ajustes que ha aplicado, para que se puedan volver a aplicar fácilmente después de reemplazar el hardware si es necesario.

Pasos

1. En el panel del BMC, seleccione **Ajustes Ajustes SNMP**.
2. En la página SNMP Settings (Configuración SNMP), seleccione **Enable SNMP V1/V2** (Activar SNMP V1/V2*) y, a continuación, proporcione una cadena de comunidad de sólo lectura y una cadena de

comunidad de lectura y escritura.

La cadena de comunidad de sólo lectura es como un ID de usuario o una contraseña. Debe cambiar este valor para evitar que los intrusos obtengan información acerca de la configuración de la red. La cadena de comunidad de lectura y escritura protege el dispositivo contra cambios no autorizados.

3. Opcionalmente, seleccione **Activar solapamiento** e introduzca la información necesaria.

> Introduzca la IP de destino para cada captura SNMP mediante una dirección IP. No se admiten los nombres de dominio completos.

Habilite las capturas si desea que el dispositivo de servicios envíe notificaciones inmediatas a una consola SNMP cuando esté en un estado inusual. Los traps pueden indicar condiciones de enlace ascendente/descendente, temperaturas que superan determinados umbrales o tráfico elevado.

4. Opcionalmente, haga clic en **Enviar captura de prueba** para probar la configuración.
5. Si la configuración es correcta, haga clic en **Guardar**.

Configure notificaciones por correo electrónico para las alertas

Si desea que las notificaciones de correo electrónico se envíen cuando se produzcan alertas, debe utilizar la interfaz de BMC para configurar las opciones SMTP, los usuarios, los destinos LAN, las directivas de alerta y los filtros de eventos.

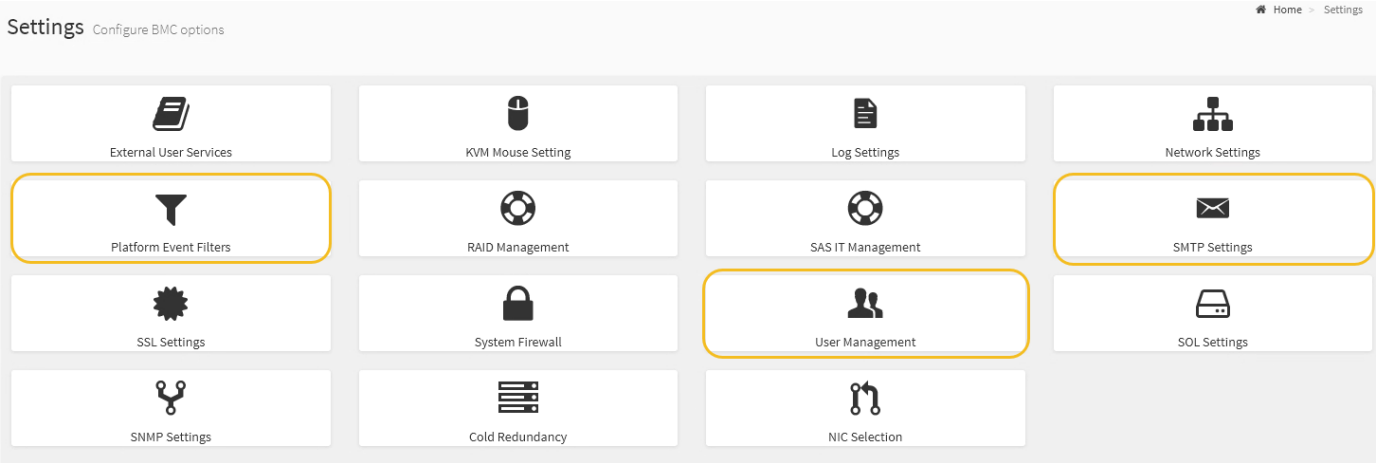
> Es posible que los ajustes del BMC realizados con este procedimiento no se conserven si el aparato falla y se tiene que sustituir. Asegúrese de que tiene un registro de todos los ajustes que ha aplicado, para que se puedan volver a aplicar fácilmente después de reemplazar el hardware si es necesario.

Lo que necesitará

Sabe cómo acceder al panel de BMC.

Acerca de esta tarea

En la interfaz del BMC, utilice las opciones **Configuración SMTP**, **Administración de usuarios** y **Filtros de sucesos de plataforma** de la página Configuración para configurar notificaciones por correo electrónico.



Pasos

1. Configure los ajustes de SMTP.
   a. Seleccione **Ajustes Ajustes SMTP**.
   b. Para el ID de correo electrónico del remitente, introduzca una dirección de correo electrónico válida.

      Esta dirección de correo electrónico se proporciona como dirección de origen cuando el BMC envía correo electrónico.

2. Configurar los usuarios para que reciban alertas.
   a. En el panel de control del BMC, seleccione **Configuración Administración de usuarios**.
   b. Añada al menos un usuario para recibir notificaciones de alerta.

      La dirección de correo electrónico que configure para un usuario es la dirección a la que el BMC envía notificaciones de alerta. Por ejemplo, puede agregar un usuario genérico, como «'usuario de notificación'» y utilizar la dirección de correo electrónico de una lista de distribución de correo electrónico del equipo de soporte técnico.

3. Configure el destino de LAN para las alertas.
   a. Seleccione **Ajustes Filtros de sucesos de plataforma Destinos LAN**.
   b. Configure al menos un destino de LAN.
      - Seleccione **correo electrónico** como tipo de destino.
      - En Nombre de usuario de BMC, seleccione un nombre de usuario que haya añadido anteriormente.
      - Si agregó varios usuarios y desea que todos reciban mensajes de correo electrónico de notificación, debe agregar un destino LAN para cada usuario.
   c. Envía una alerta de prueba.
4. Configurar directivas de alerta para poder definir cuándo y dónde envía alertas el BMC.
   a. Seleccione **Configuración Filtros de sucesos de plataforma Directivas de alerta**.
   b. Configure al menos una directiva de alerta para cada destino de LAN.
      - Para número de grupo de directivas, seleccione **1**.
      - Para Acción de directiva, seleccione **siempre enviar alerta a este destino**.
      - Para el canal LAN, seleccione **1**.
      - En el Selector de destinos, seleccione el destino LAN de la directiva.
5. Configurar filtros de eventos para dirigir las alertas de diferentes tipos de eventos a los usuarios correspondientes.
   a. Seleccione **Ajustes Filtros de sucesos de plataforma Filtros de sucesos**.
   b. Para el número de grupo de políticas de alerta, introduzca **1**.
   c. Cree filtros para cada evento del que desee que se notifique al grupo de directivas de alerta.
      - Puede crear filtros de eventos para acciones de alimentación, eventos de sensor específicos o todos los eventos.
      - Si no está seguro de qué eventos debe supervisar, seleccione **todos los sensores** para el tipo de sensor y **todos los eventos** para las opciones de evento. Si recibe notificaciones no deseadas, puede cambiar sus selecciones más adelante.

Opcional: Habilite el cifrado de nodos

Si habilita el cifrado de nodos, los discos del dispositivo pueden protegerse mediante el cifrado del servidor de gestión de claves seguro (KMS) contra la pérdida física o la eliminación del sitio. Debe seleccionar y habilitar el cifrado de nodos durante la instalación del dispositivo y no puede anular la selección del cifrado de nodos una vez que se inicia el proceso de cifrado KMS.

Lo que necesitará

Revise la información sobre KMS en las instrucciones para administrar StorageGRID.

Acerca de esta tarea

Un dispositivo con el cifrado de nodos habilitado se conecta al servidor de gestión de claves (KMS) externo que está configurado para el sitio StorageGRID. Cada KMS (o clúster KMS) administra las claves de cifrado de todos los nodos de dispositivos del sitio. Estas claves cifran y descifran los datos de cada disco de un dispositivo que tiene habilitado el cifrado de nodos.

Se puede configurar un KMS en Grid Manager antes o después de instalar el dispositivo en StorageGRID. Consulte la información sobre la configuración de KMS y del dispositivo en las instrucciones para administrar StorageGRID para obtener más detalles.

- Si se configura un KMS antes de instalar el dispositivo, el cifrado controlado por KMS comienza cuando se habilita el cifrado de nodos en el dispositivo y se lo agrega a un sitio StorageGRID donde se configura KMS.
- Si no se configura un KMS antes de instalar el dispositivo, el cifrado controlado por KMS se lleva a cabo en cada dispositivo que tenga activado el cifrado de nodos en cuanto se configure un KMS y esté disponible para el sitio que contiene el nodo del dispositivo.

> Los datos que existen antes de conectarse al KMS en un dispositivo con el cifrado de nodos habilitado se cifran con una clave temporal que no es segura. El dispositivo no está protegido de la retirada o robo hasta que la clave se configure en un valor proporcionado por el KMS.

Sin la clave KMS necesaria para descifrar el disco, los datos del dispositivo no se pueden recuperar y se pierden de forma efectiva. Este es el caso siempre que la clave de descifrado no se pueda recuperar del KMS. La clave se vuelve inaccesible si elimina la configuración de KMS, caduca una clave KMS, se pierde la conexión con el KMS o se elimina el dispositivo del sistema StorageGRID donde están instaladas sus claves KMS.

Pasos

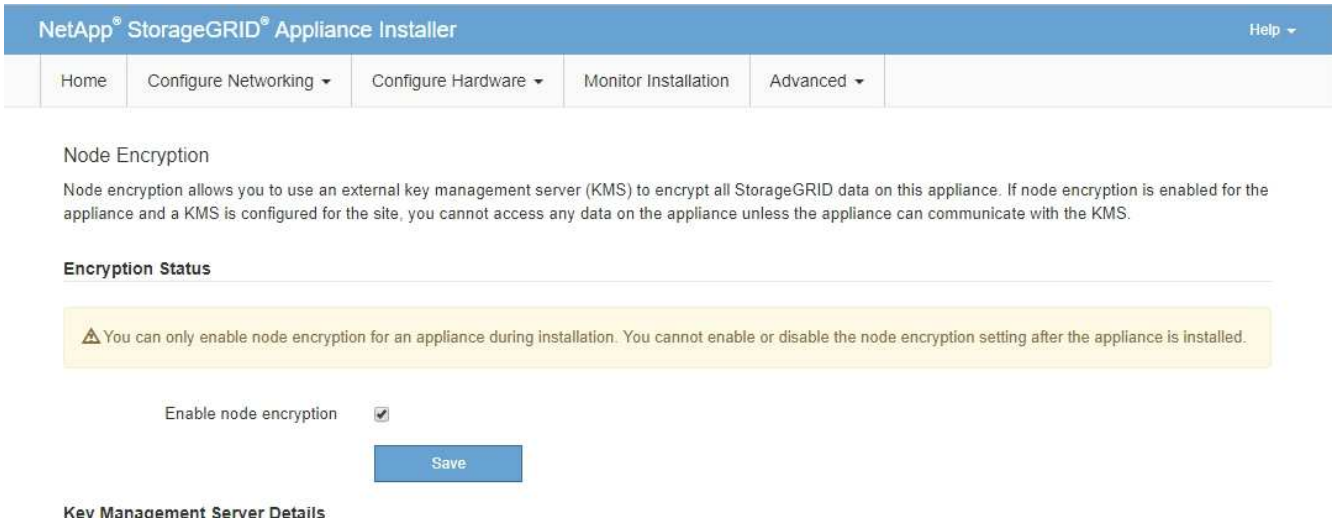
1. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.
   `https://`*`Controller_IP`*`:8443`

   `Controller_IP` Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

   > Una vez que el dispositivo se ha cifrado con una clave KMS, los discos del dispositivo no se pueden descifrar sin utilizar la misma clave KMS.

2. Seleccione **Configurar hardware** > **cifrado de nodos**.



3. Seleccione **Activar cifrado de nodo**.

   Antes de instalar el dispositivo, puede anular la selección **Activar cifrado de nodo** sin riesgo de pérdida de datos. Cuando se inicia la instalación el nodo del dispositivo, accede a las claves de cifrado de KMS en el sistema StorageGRID y comienza el cifrado de disco. No se puede deshabilitar el cifrado de nodos después de haber instalado el dispositivo.

   > Después de agregar un dispositivo que tiene habilitado el cifrado de nodos a un sitio StorageGRID que tiene un KMS, no puede detener el uso del cifrado KMS para el nodo.

4. Seleccione **Guardar**.
5. Ponga en marcha el dispositivo como nodo en su sistema StorageGRID.

   El cifrado controlado POR KMS se inicia cuando el dispositivo accede a las claves KMS configuradas para el sitio StorageGRID. El instalador muestra mensajes de progreso durante el proceso de cifrado KMS, que puede tardar unos minutos en función del número de volúmenes de disco del dispositivo.

   > Los dispositivos se configuran inicialmente con una clave de cifrado no KMS aleatoria asignada a cada volumen de disco. Los discos se cifran con esta clave de cifrado temporal, que no es segura, hasta que el dispositivo con cifrado de nodos habilitado acceda a las claves KMS configuradas para el sitio StorageGRID.

Después de terminar

Puede ver el estado de cifrado de nodo, los detalles de KMS y los certificados en uso cuando el nodo del dispositivo está en modo de mantenimiento.

Información relacionada

Administre StorageGRID

Supervisión del cifrado de nodos en modo de mantenimiento (SG100 y SG1000)

Implemente el nodo del dispositivo de servicios

Puede implementar un dispositivo de servicios como un nodo de administrador principal,

un nodo de administrador que no sea primario o un nodo de puerta de enlace. Tanto los dispositivos SG100 como los SG1000 pueden funcionar al mismo tiempo como nodos de puerta de enlace y nodos de administración (primarios o no primarios).

Ponga en marcha el dispositivo de servicios como nodo de administración principal

Al poner en marcha un dispositivo de servicios como nodo administrador principal, utiliza el instalador de dispositivos StorageGRID incluido en el dispositivo para instalar el software StorageGRID o carga la versión de software que desea instalar. Debe instalar y configurar el nodo de administración principal antes de instalar cualquier otro tipo de nodos de dispositivos. Un nodo de administración principal puede conectarse a la red de grid y a la red de administración y la red de cliente opcionales, si se han configurado uno o ambos.

Lo que necesitará

- El dispositivo se ha instalado en un rack o armario, conectado a las redes y encendido.
- Se han configurado los enlaces de red, las direcciones IP y la reasignación de puertos (si fuera necesario) para el dispositivo con el instalador de dispositivos de StorageGRID.

  > Si ha reasignado algún puerto, no puede utilizar los mismos puertos para configurar los extremos de equilibrador de carga. Puede crear puntos finales mediante puertos reasignados, pero esos puntos finales se volverán a asignar a los puertos y servicios de CLB originales, no al servicio Load Balancer. Siga los pasos de Eliminar reasignaciones de puertos.

  Consulte Cómo funciona el equilibrio de carga: Servicio CLB (obsoleto) Para obtener más información sobre el servicio CLB.

  > El servicio CLB está obsoleto.

- Tiene un ordenador portátil de servicio con un navegador web compatible.
- Conoce una de las direcciones IP asignadas al dispositivo. Puede usar la dirección IP para cualquier red StorageGRID conectada.

Acerca de esta tarea

Para instalar StorageGRID en un nodo de administrador principal de un dispositivo:

- Utilice el instalador de dispositivos de StorageGRID para instalar el software de StorageGRID. Si desea instalar una versión diferente del software, primero lo cargue con el instalador de dispositivos de StorageGRID.
- Espera a que el software esté instalado.
- Cuando se ha instalado el software, el dispositivo se reinicia automáticamente.

Pasos

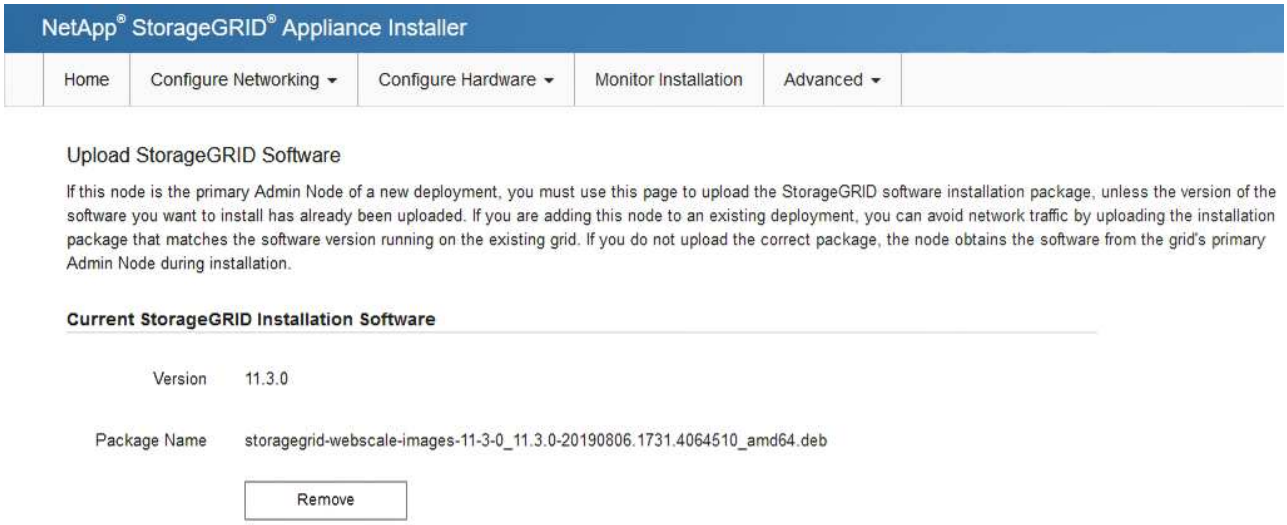
1. Abra un explorador e introduzca la dirección IP del dispositivo.
   `https://services_appliance_IP:8443`

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

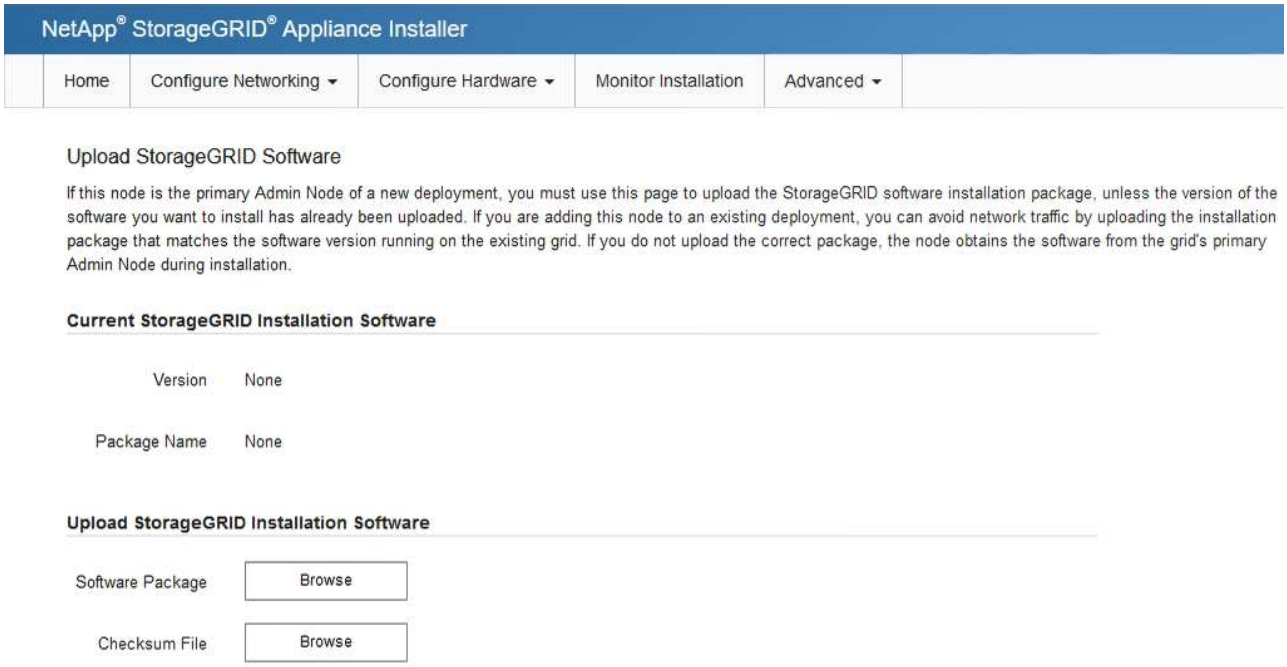
2. En la sección **este nodo**, seleccione **Administración primaria**.
3. En el campo **Nombre de nodo**, introduzca el nombre que desea utilizar para este nodo de dispositivo y haga clic en **Guardar**.

   El nombre del nodo está asignado a este nodo del dispositivo en el sistema StorageGRID. Se muestra en la página Grid Nodes del Grid Manager.

4. Opcionalmente, para instalar una versión diferente del software StorageGRID, siga estos pasos:
   a. Descargue el archivo de instalación:https://mysupport.netapp.com/site/products/all/details/storagegrid-appliance/downloads-tab["Descargas de NetApp: Dispositivo de StorageGRID"^].
   b. Extraiga el archivo.
   c. En el instalador del dispositivo StorageGRID, seleccione **Avanzado cargar software StorageGRID**.
   d. Haga clic en **Eliminar** para eliminar el paquete de software actual.



   e. Haga clic en **examinar** para ver el paquete de software que descargó y extrajo y, a continuación, haga clic en **examinar** para ver el archivo de suma de comprobación.

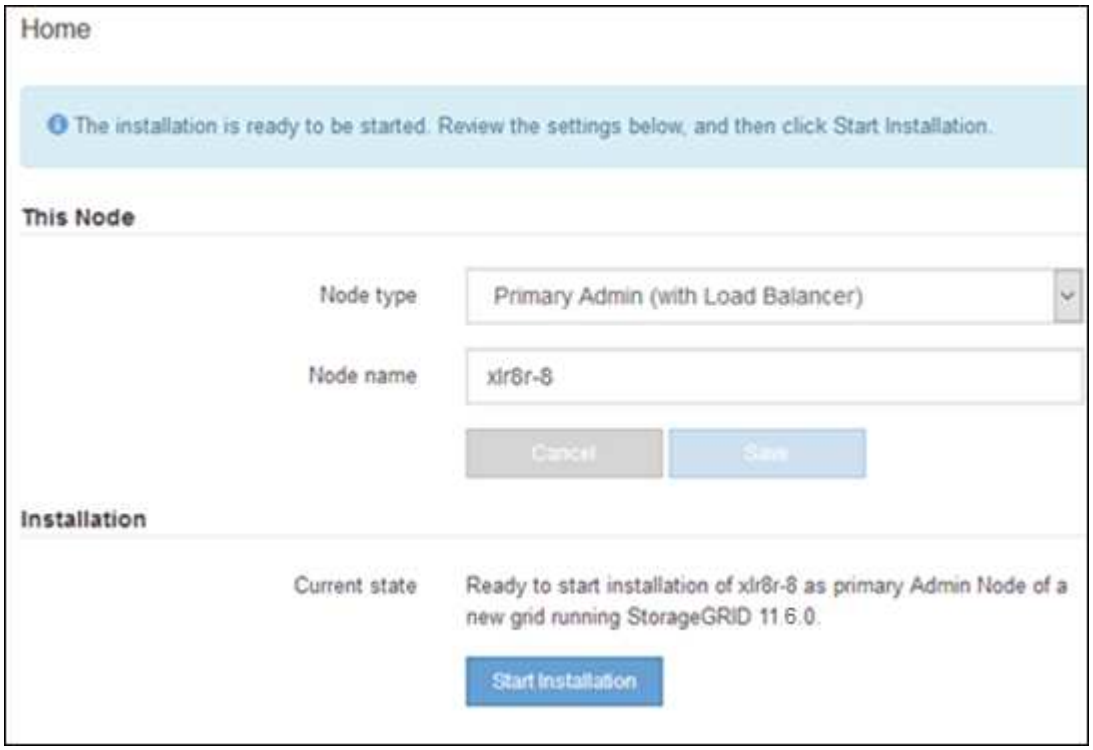


f. Seleccione **Inicio** para volver a la página de inicio.

5. Confirme que el estado actual es "'preparado para iniciar la instalación del nombre del nodo de administración principal con la versión de software x.y'" y que el botón **Iniciar instalación** está activado.

> Si va a implementar el dispositivo Admin Node como destino de clonado de nodos, detenga el proceso de implementación aquí y continúe con el procedimiento de clonado de nodos de acuerdo con el Recuperación y mantenimiento instrucciones.

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.

Implemente el dispositivo de servicios como puerta de enlace o un nodo administrador que no sea el principal

Cuando se implementa un dispositivo de servicios como nodo de puerta de enlace o nodo de administración no primario, se usa el instalador de dispositivos StorageGRID incluido en el dispositivo.

Lo que necesitará

- El dispositivo se ha instalado en un rack o armario, conectado a las redes y encendido.
- Se han configurado los enlaces de red, las direcciones IP y la reasignación de puertos (si fuera necesario) para el dispositivo con el instalador de dispositivos de StorageGRID.

  Si ha reasignado algún puerto, no puede utilizar los mismos puertos para configurar los extremos de equilibrador de carga. Puede crear puntos finales mediante puertos reasignados, pero esos puntos finales se volverán a asignar a los puertos y servicios de CLB originales, no al servicio Load Balancer. Siga los pasos de Eliminar reasignaciones de puertos.

  El servicio CLB está obsoleto.

- Se puso en marcha el nodo de administración principal del sistema 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.
- Tiene un ordenador portátil de servicio con un navegador web compatible.
- Conoce la dirección IP asignada al dispositivo. Puede usar la dirección IP para cualquier red StorageGRID conectada.

Acerca de esta tarea

Para instalar StorageGRID en un nodo del dispositivo de servicios:

- Especifique o confirme la dirección IP del nodo de administración principal y el nombre del nodo de dispositivo.
- Se inicia la instalación y se espera a medida que se instala el software.

  Paso a través de las tareas de instalación del nodo de puerta de enlace 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. La instalación de un nodo de administración no primario no requiere su aprobación.

No instale los dispositivos de servicio SG100 y SG1000 en el mismo sitio. El rendimiento puede ser impredecible.

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. También puede usar el instalador de dispositivos para cargar un archivo JSON que contenga información de configuración. Consulte Automatización de la instalación y configuración de dispositivos (SG100 y SG1000) para obtener más información sobre cómo automatizar la instalación.

Pasos

1. Abra un explorador e introduzca la dirección IP del 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.

   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:

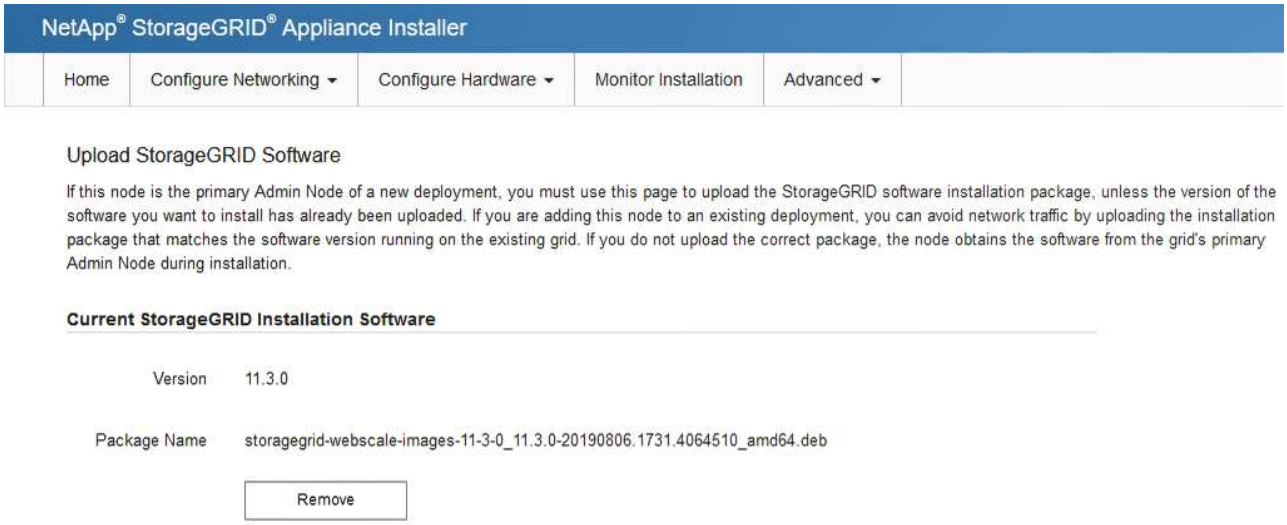
Opción	Descripción
Entrada IP manual	a. Anule la selección de la casilla de verificación **Activar descubrimiento de nodo de administración**. b. Introduzca la dirección IP de forma manual. c. Haga clic en **Guardar**. d. Espere a que el estado de la conexión para que la nueva dirección IP se prepare.
Detección automática de todos los nodos principales de administración conectados	a. Active la casilla de verificación **Activar descubrimiento de nodos de administración**. 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 haga clic en **Guardar**.

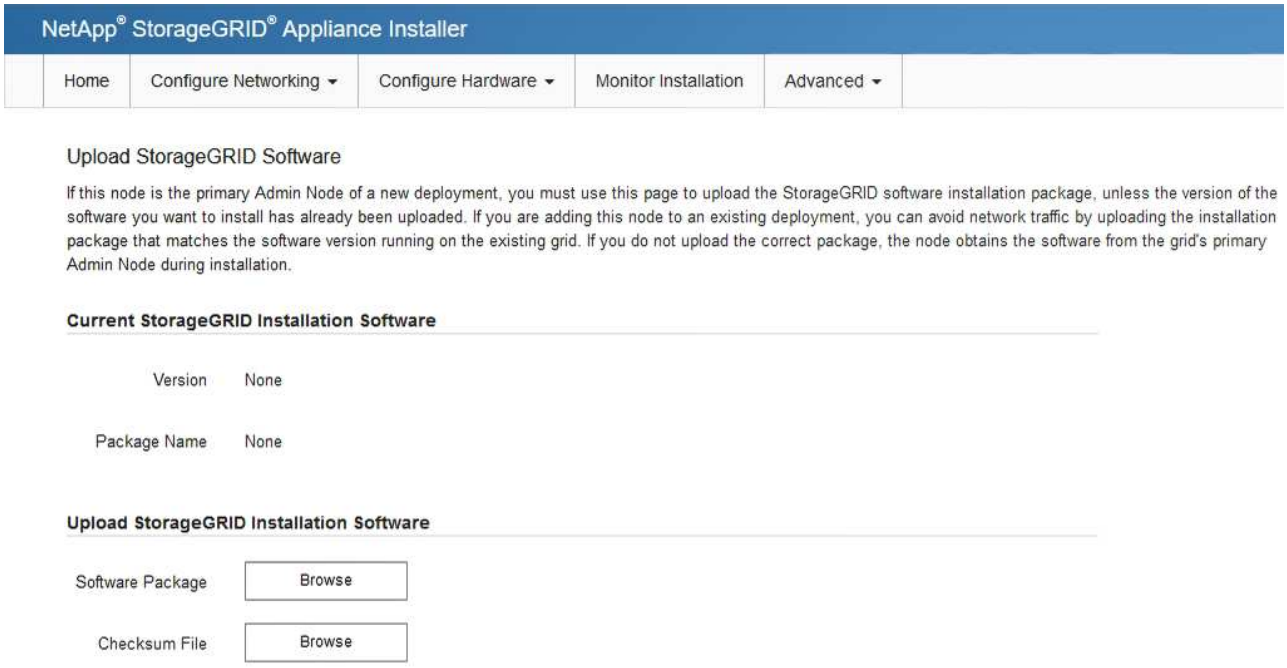
   El nombre del nodo está asignado a este nodo del dispositivo en el sistema StorageGRID. Se muestra en

la página Nodes (ficha Overview) de Grid Manager. Si es necesario, puede cambiar el nombre cuando apruebe el nodo.

5. Opcionalmente, para instalar una versión diferente del software StorageGRID, siga estos pasos:
   a. Descargue el archivo de instalación:https://mysupport.netapp.com/site/products/all/details/storagegrid-appliance/downloads-tab["Descargas de NetApp: Dispositivo de StorageGRID"^].
   b. Extraiga el archivo.
   c. En el instalador del dispositivo StorageGRID, seleccione **Avanzado cargar software StorageGRID**.
   d. Haga clic en **Eliminar** para eliminar el paquete de software actual.



   e. Haga clic en **examinar** para ver el paquete de software que descargó y extrajo y, a continuación, haga clic en **examinar** para ver el archivo de suma de comprobación.

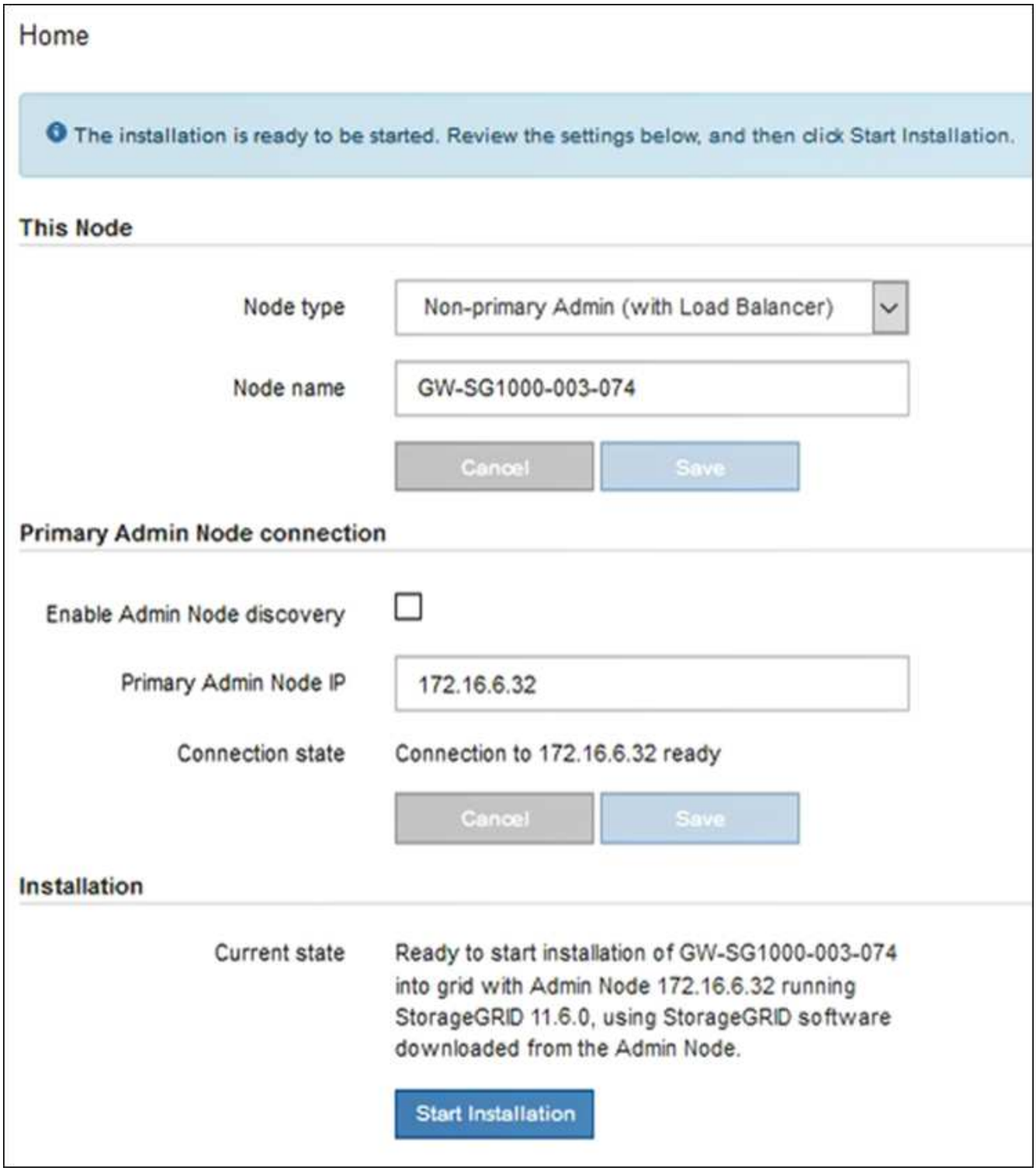


   f. Seleccione **Inicio** para volver a la página de inicio.
6. En la sección instalación, confirme que el estado actual es "Listo para iniciar la instalación de `node name`

En el grid con el nodo de administrador principal `admin_ip` " Y que el botón **Iniciar instalación** 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 instalación y mantenimiento del aparato.

7. 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.

8. Si el grid incluye varios nodos de dispositivo, repita los pasos anteriores con cada dispositivo.

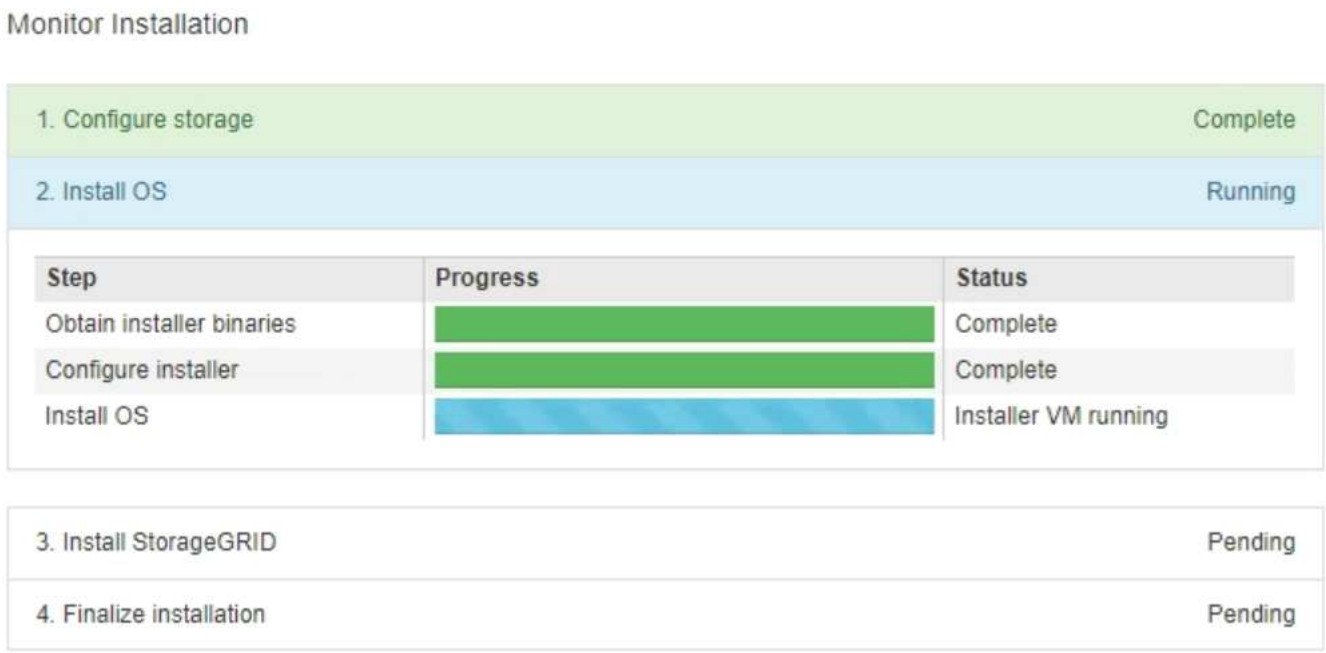
Supervisar la instalación del dispositivo de servicios

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.

> El instalador garantiza que no se vuelvan a ejecutar las tareas completadas en una instalación anterior. 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 de "Shided."

2. Revise el progreso de las dos primeras etapas de instalación.
   - **1. Configurar almacenamiento**

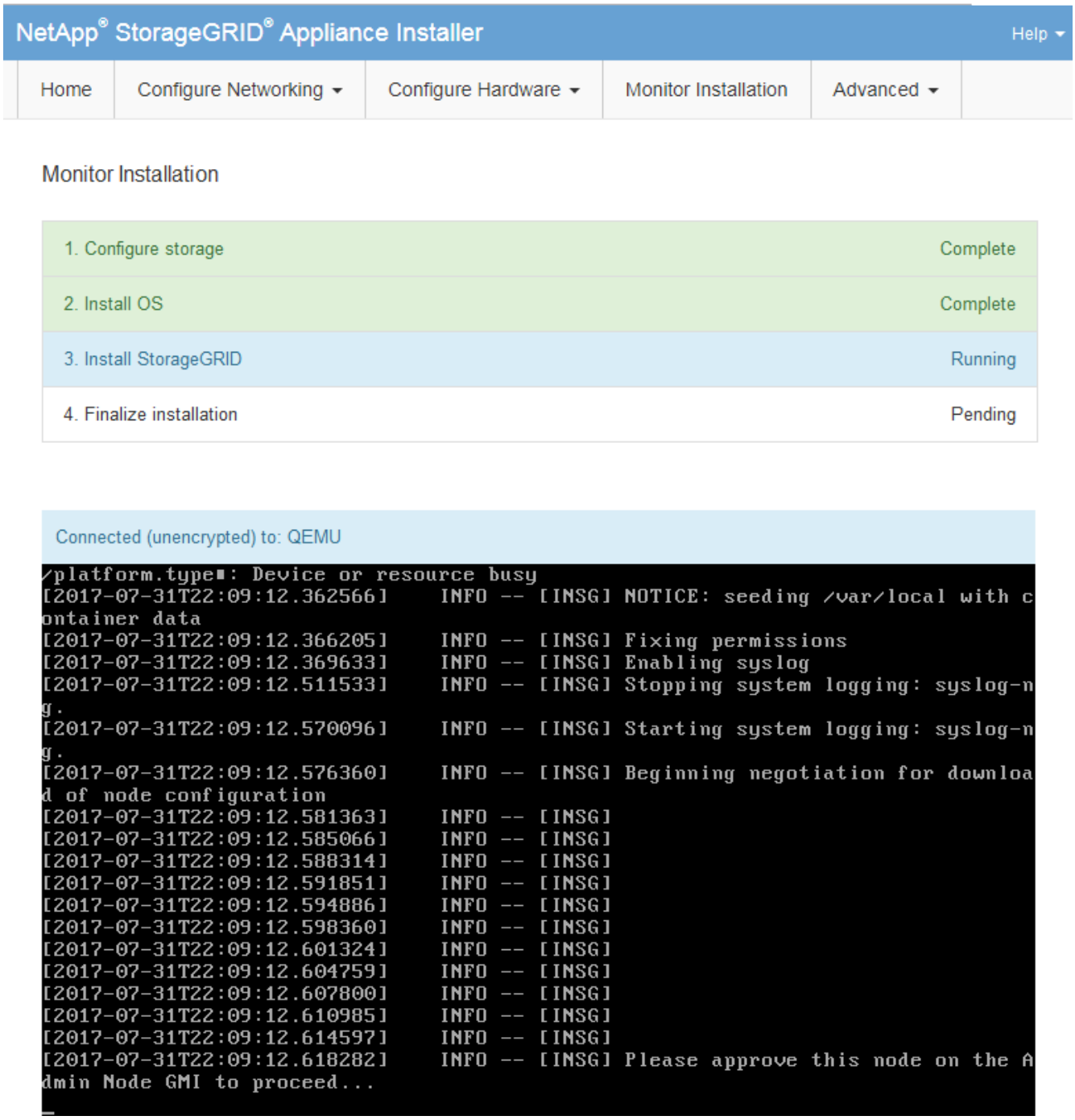
     Durante esta fase, el instalador borra toda la configuración existente de las unidades del dispositivo y configura la configuración del host.

   - **2. Instalar OS**

     Durante esta fase, el instalador copia la imagen del sistema operativo base para StorageGRID en el dispositivo.

3. Continúe supervisando el progreso de la instalación hasta que se produzca uno de los siguientes procesos:
    - Para todos los nodos de dispositivo excepto el nodo de administración principal, la fase de instalación de 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. Vaya al paso siguiente.
    - Para la instalación del nodo de administración principal del dispositivo, no es necesario aprobar el nodo. El dispositivo se reinicia. Puede omitir el paso siguiente.

> Durante la instalación de un nodo de administración principal del dispositivo, aparece una quinta fase (consulte el ejemplo de captura de pantalla que muestra cuatro fases). Si la quinta fase está en curso durante más de 10 minutos, actualice la página web manualmente.



4. Vaya al Administrador de grid del nodo Administrador principal, apruebe el nodo de cuadrícula pendiente y complete el proceso de instalación de StorageGRID.

   Al hacer clic en **instalar** desde Grid Manager, se completa la fase 3 y comienza la fase 4, **Finalizar instalación**. Cuando finalice la fase 4, el dispositivo se reiniciará.

Automatización de la instalación y configuración de dispositivos (SG100 y SG1000)

Puede automatizar la instalación y configuración de sus dispositivos y la configuración de todo el sistema StorageGRID.

Acerca de esta tarea

Automatizar la instalación y la configuración puede ser útil para poner en marcha varias instancias de StorageGRID o una instancia de StorageGRID grande y compleja.

Para automatizar la instalación y configuración, utilice una o varias de las siguientes opciones:

- Cree un archivo JSON que especifique las opciones de configuración para los dispositivos. Cargue el archivo JSON con el instalador de dispositivos StorageGRID.

  Puede usar el mismo archivo para configurar más de un dispositivo.

- Utilice la StorageGRID`configure-sga.py` Script Python para automatizar la configuración de sus dispositivos.
- Utilice scripts Python adicionales para configurar otros componentes de todo el sistema StorageGRID (la "cuadrícula").

Puede utilizar directamente los scripts Python de automatización de StorageGRID o bien puede usarlos como ejemplos de cómo utilizar la API DE REST de instalación de StorageGRID en las herramientas de puesta en marcha de grid y de configuración que desarrolla usted mismo. Consulte las instrucciones para Descarga y extracción de los archivos de instalación de StorageGRID.

Automatice la configuración del dispositivo con StorageGRID Appliance Installer

Puede automatizar la configuración de un dispositivo mediante un archivo JSON que contiene la información de configuración. El archivo se carga con el instalador de dispositivos de StorageGRID.

Lo que necesitará

- El dispositivo debe tener el firmware más reciente compatible con StorageGRID 11.5 o superior.
- Debe estar conectado al instalador de dispositivos de StorageGRID en el dispositivo que esté configurando mediante un navegador web compatible.

Acerca de esta tarea

Puede automatizar las tareas de configuración de los dispositivos, como la configuración de las siguientes opciones:

- Redes de grid, red de administración y direcciones IP de red de cliente
- Interfaz BMC
- Enlaces de red
  - Modo de enlace de puerto
  - Modo de enlace de red
  - Velocidad de enlace

La configuración del dispositivo con un archivo JSON cargado suele ser más eficaz que realizar la configuración manualmente mediante múltiples páginas en el instalador del dispositivo StorageGRID, especialmente si tiene que configurar muchos nodos. Debe aplicar el archivo de configuración para cada nodo de uno en uno.

> Los usuarios con experiencia que desean automatizar tanto la instalación como la configuración de sus dispositivos pueden hacerlo utilice el script configure-sga.py.

Pasos

1. Genere el archivo JSON mediante uno de los siguientes métodos:
   - La "Aplicación ConfigBuilder".
   - La configure-sga.py secuencia de comandos de configuración del dispositivo. Puede descargar la secuencia de comandos desde el instalador del dispositivo StorageGRID (**Ayuda secuencia de comandos de configuración del dispositivo**).

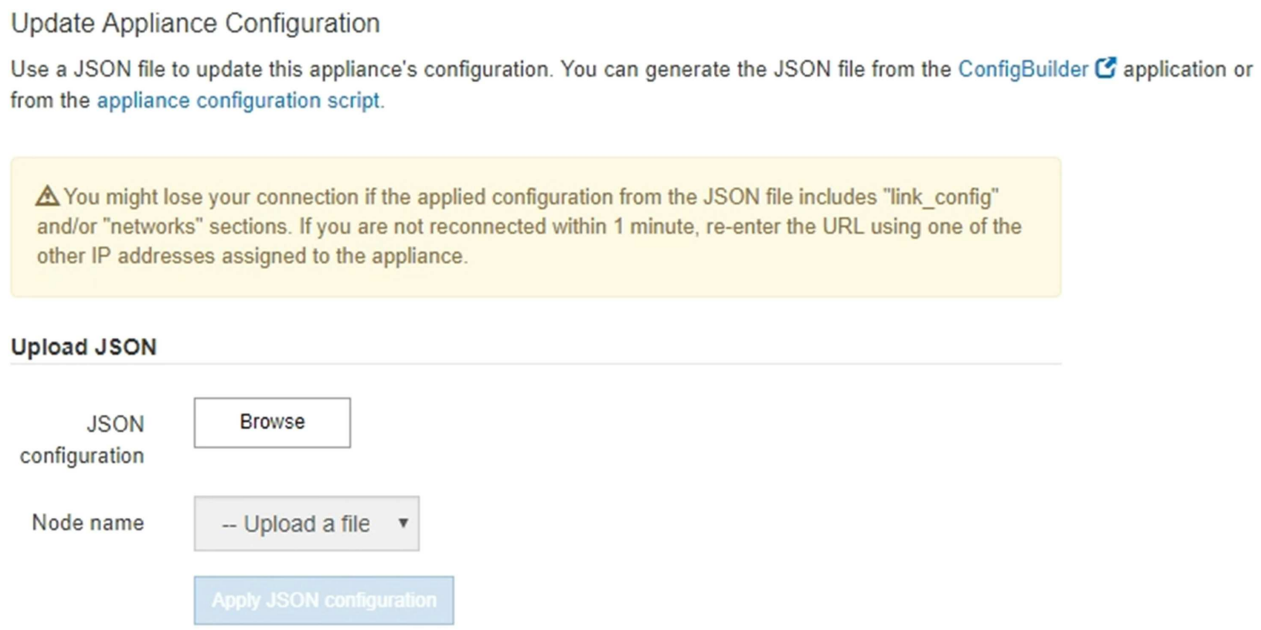
     Los nombres de nodos en el archivo JSON deben seguir estos requisitos:

     - Debe ser un nombre de host válido que contenga al menos 1 y no más de 32 caracteres
     - Puede usar letras, números y guiones
     - No se puede iniciar o finalizar con un guión
     - No puede contener solo números

     > Asegúrese de que los nombres de nodo (los nombres de nivel superior) del archivo JSON son únicos o de que no pueda configurar más de un nodo mediante el archivo JSON.

2. Seleccione **Avanzado** > **Actualizar configuración del dispositivo**.

   Aparece la página Actualizar configuración del dispositivo.

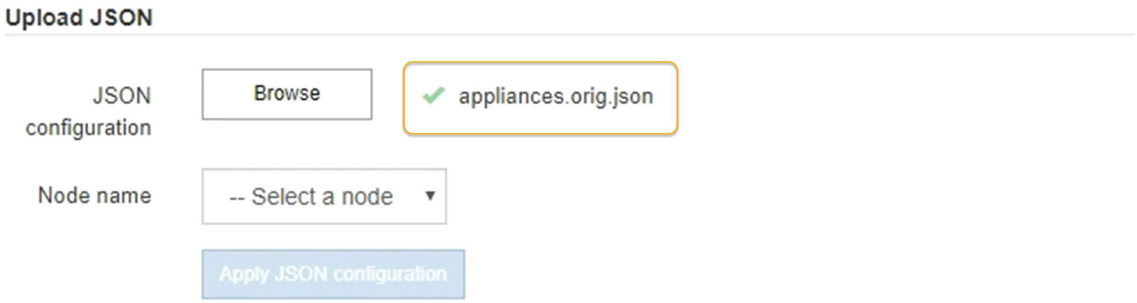


3. Seleccione el archivo JSON con la configuración que desea cargar.
   a. Seleccione **examinar**.
   b. Localice y seleccione el archivo.

c. Seleccione **Abrir**.

El archivo se carga y se valida. Una vez completado el proceso de validación, se muestra el nombre del archivo junto a una Marca de verificación verde.

> Es posible que pierda la conexión con el dispositivo si la configuración del archivo JSON incluye secciones de "link_config", "Networks" o ambas. Si no vuelve a conectarse en 1 minuto, vuelva a introducir la URL del dispositivo utilizando una de las otras direcciones IP asignadas al dispositivo.

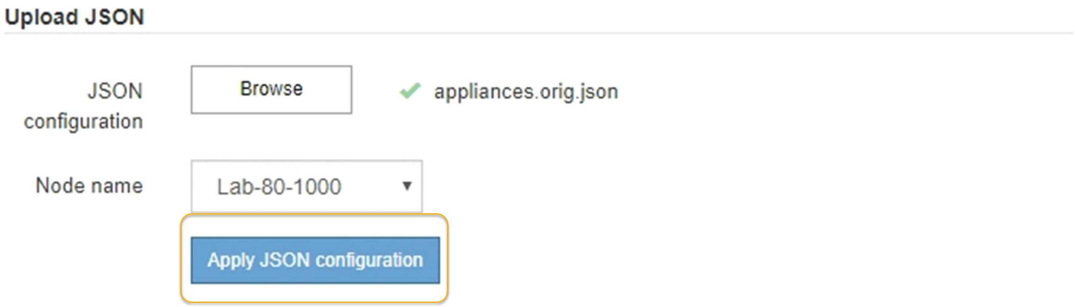


La lista desplegable **Nombre de nodo** se rellena con los nombres de nodo de nivel superior definidos en el archivo JSON.

> Si el archivo no es válido, el nombre del archivo se muestra en rojo y se muestra un mensaje de error en un banner amarillo. El archivo no válido no se ha aplicado al dispositivo. Puede utilizar ConfigBuilder para asegurarse de tener un archivo JSON válido.

4. Seleccione un nodo de la lista de la lista desplegable **Nombre de nodo**.

   El botón **aplicar configuración JSON** está activado.



5. Seleccione **aplicar configuración JSON**.

   La configuración se aplica al nodo seleccionado.

Automatice la instalación y configuración de los nodos de los dispositivos con un script configure-sga.py

Puede utilizar el `configure-sga.py` Script para automatizar muchas de las tareas de instalación y configuración para los nodos del dispositivo StorageGRID, incluida la

instalación y configuración de un nodo de administración principal. Esta secuencia de comandos puede ser útil si tiene un gran número de dispositivos que configurar. También puede usar el script para generar un archivo JSON que contenga información de configuración del dispositivo.

Lo que necesitará

- 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 nodo de administración principal mediante el instalador de dispositivos de StorageGRID.
- Si está instalando el nodo de administrador principal, conoce su dirección IP.
- Si va a instalar y configurar otros nodos, el nodo de administrador principal se ha implementado y conoce su dirección IP.
- Para todos los nodos que no sean el nodo de administración principal, todas las subredes de red de cuadrícula que aparecen en la página Configuración de IP del instalador de dispositivos StorageGRID se han definido en la lista de subredes de redes de cuadrícula del nodo de administración principal.
- Ha descargado el `configure-sga.py` archivo. El archivo se incluye en el archivo de instalación o puede acceder a él haciendo clic en **Ayuda** > **secuencia de comandos de instalación del dispositivo** en el instalador del dispositivo StorageGRID.

> Este procedimiento es para usuarios avanzados con cierta experiencia usando interfaces de línea de comandos. Como alternativa, puede hacerlo Use el instalador del dispositivo StorageGRID para automatizar la configuración.

Pasos

1. Inicie sesión en el equipo Linux que está utilizando para ejecutar el script Python.
2. Para obtener ayuda general sobre la sintaxis de la secuencia de comandos y ver una lista de los parámetros disponibles, introduzca lo siguiente:

   ```
   configure-sga.py --help
   ```

   La `configure-sga.py` el script utiliza cinco subcomandos:

   - `advanced` Para interacciones avanzadas con dispositivos StorageGRID, incluida la configuración del BMC y la creación de un archivo JSON con la configuración actual del dispositivo
   - `configure` Para configurar los parámetros de modo RAID, nombre del nodo y red
   - `install` Para iniciar una instalación de StorageGRID
   - `monitor` Para supervisar una instalación de StorageGRID
   - `reboot` para reiniciar el dispositivo

     Si introduce un argumento de subcomando (avanzado, configure, instale, monitor o reboot) seguido del `--help` opción usted obtendrá un texto de ayuda diferente que proporciona más detalles sobre las opciones disponibles dentro de ese subcomando:
     `configure-sga.py` *`subcommand`* `--help`

3. Para confirmar la configuración actual del nodo del dispositivo, introduzca lo siguiente donde *`SGA-`*

install-ip Es cualquiera de las direcciones IP del nodo del dispositivo:
`configure-sga.py configure SGA-INSTALL-IP`

Los resultados muestran información de IP actual del dispositivo, incluida la dirección IP del nodo de administración principal e información sobre las redes de administración, grid y cliente.

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200

  StorageGRID Appliance
    Name:        LAB-SGA-2-30
    Node type:   storage

  StorageGRID primary Admin Node
    IP:        172.16.1.170
    State:     unknown
    Message:   Initializing...
    Version:   Unknown

  Network Link Configuration
    Link Status
          Link      State      Speed (Gbps)
          ----      -----      -----
          1         Up         10
          2         Up         10
          3         Up         10
          4         Up         10
          5         Up         1
          6         Down       N/A

    Link Settings
        Port bond mode:      FIXED
        Link speed:          10GBE

        Grid Network:        ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
```

```
            MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

        Admin Network:       ENABLED
            Bonding mode:    no-bond
            MAC Addresses:   00:80:e5:29:70:f4

        Client Network:      ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

  Grid Network
    CIDR:      172.16.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:8A
    Gateway:   172.16.0.1
    Subnets:   172.17.0.0/21
               172.18.0.0/21
               192.168.0.0/21
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

#############################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#############################################################
```

4. Si necesita cambiar alguno de los valores de la configuración actual, utilice `configure` subcomando para actualizarlos. Por ejemplo, si desea cambiar la dirección IP que utiliza el dispositivo para conectarse al nodo de administración principal `172.16.2.99`, introduzca lo siguiente:
   `configure-sga.py configure --admin-ip 172.16.2.99` *`SGA-INSTALL-IP`*
5. Si desea realizar un backup de la configuración del dispositivo en un archivo JSON, utilice Advanced y. `backup-file` subcomandos. Por ejemplo, si desea realizar una copia de seguridad de la configuración

de un dispositivo con dirección IP *SGA-INSTALL-IP* a un archivo llamado `appliance-SG1000.json`, introduzca lo siguiente:
`configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP`

El archivo JSON que contiene la información de configuración se escribe en el mismo directorio desde el que se ejecutó la secuencia de comandos.

> Compruebe que el nombre del nodo de nivel superior del archivo JSON generado coincida con el nombre del dispositivo. No haga ningún cambio en este archivo a menos que sea un usuario con experiencia y que tenga una profunda comprensión de las API de StorageGRID.

6. Cuando esté satisfecho con la configuración del dispositivo, utilice `install` y.. `monitor` subcomandos para instalar el dispositivo:
`configure-sga.py install --monitor SGA-INSTALL-IP`
7. Si desea reiniciar el dispositivo, introduzca lo siguiente:
`configure-sga.py reboot SGA-INSTALL-IP`

Automatice la configuración de StorageGRID

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

Lo que necesitará

- 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 con el Administrador de grid 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
```

Después de terminar

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 ha especificado que se deben generar contraseñas aleatorias, debe extraer 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 general sobre la instalación de API de REST

StorageGRID proporciona dos API REST para realizar tareas de instalación: La API de instalación de StorageGRID y la API del instalador de dispositivos de StorageGRID.

Ambas API utilizan 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 (notación de

objetos JavaScript).

> 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 configura inicialmente el sistema StorageGRID y en el caso de que deba realizar una recuperación de nodo de administrador principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de API, vaya a la página web de instalación del nodo de administración principal y seleccione **Ayuda** > **Documentación de 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.
- **Sites** — Operaciones de configuración a nivel de sitio. Puede crear, ver, eliminar y modificar un sitio.

API del instalador de dispositivos de StorageGRID

Se puede acceder a la API del instalador de dispositivos de StorageGRID a través de HTTPS desde `Controller_IP:8443`.

Para acceder a la documentación de la API, vaya al instalador del dispositivo StorageGRID en el dispositivo y seleccione **Ayuda** > **Documentación de la API** en la barra de menús.

La API del instalador de dispositivos de StorageGRID incluye las siguientes secciones:

- **Clone** — Operaciones para configurar y controlar la clonación de nodos.
- **Cifrado** — Operaciones para administrar el cifrado y ver el estado del cifrado.
- **Configuración del hardware** — Operaciones para configurar los ajustes del sistema en el hardware conectado.

- **Instalación** — Operaciones para iniciar la instalación del aparato y para supervisar el estado de instalación.
- **Redes** — Operaciones relacionadas con la configuración de red de Grid, Admin y Cliente para un dispositivo StorageGRID y los ajustes de puerto de dispositivo.
- **Setup** — Operaciones para ayudar con la instalación inicial del dispositivo incluyendo solicitudes para obtener información sobre el sistema y actualizar el IP principal del nodo de administración.
- **SOPORTE** — Operaciones para reiniciar el controlador y obtener registros.
- **Upgrade** — Operaciones relacionadas con la actualización del firmware del dispositivo.
- **Uploadsg** — Operaciones para cargar archivos de instalación de StorageGRID.

Solucionar problemas de instalación de hardware (SG100 y SG1000)

Si encuentra problemas durante la instalación, es posible que le sea útil revisar información sobre la solución de problemas relacionados con la configuración del hardware y los problemas de conectividad.

Ver los códigos de arranque del dispositivo

Cuando se enciende el aparato, el BMC registra una serie de códigos de inicio. Puede ver estos códigos en una consola gráfica que está conectada al puerto de gestión del BMC.

Lo que necesitará

- Sabe cómo acceder al panel de BMC.
- Si desea utilizar Serial-Over-LAN (sol), tendrá experiencia utilizando las aplicaciones de la consola sol de IPMI.

Pasos

1. Seleccione uno de los siguientes métodos para ver los códigos de arranque del controlador del dispositivo y recopilar el equipo necesario.

Método	Equipo necesario
Consola VGA	• Monitor compatible con VGA • Cable VGA
KVM	• Cable RJ-45
Puerto serie	• Cable serie DB-9 • Terminal serie virtual
SOL	• Terminal serie virtual

2. Si está utilizando una consola VGA, siga estos pasos:
   a. Conecte un monitor compatible con VGA al puerto VGA de la parte posterior del dispositivo.

b. Ver los códigos mostrados en el monitor.

3. Si está utilizando BMC KVM, realice estos pasos:
   a. Conéctese al puerto de administración de BMC e inicie sesión en la interfaz web de BMC.
   b. Seleccione **Control remoto**.
   c. Inicie el KVM.
   d. Ver los códigos en el monitor virtual.
4. Si utiliza un puerto serie y un terminal, realice los siguientes pasos:
   a. Conecte el puerto serie DB-9 de la parte posterior del dispositivo.
   b. Utilice la configuración `115200 8-N-1`.
   c. Ver los códigos impresos en el terminal de serie.
5. Si va a utilizar sol, realice los siguientes pasos:
   a. Conéctese a IPMI sol mediante la dirección IP del BMC y las credenciales de inicio de sesión.

   > Si no ha cambiado la contraseña de la cuenta raíz de BMC, el valor predeterminado de fábrica puede ser "calvin".

   ```
   ipmitool -I lanplus -H BMC_Port_IP -U root -P Password sol activate
   ```

   b. Ver los códigos en el terminal de serie virtual.
6. Utilice la tabla para buscar los códigos del aparato.

Codificación	Lo que indica
HOLA	Se ha iniciado la secuencia de comandos de inicio maestra.
HP	El sistema comprueba si es necesario actualizar el firmware de la tarjeta de interfaz de red (NIC).
RB	El sistema se reinicia después de aplicar las actualizaciones de firmware.
P F	Se completaron las comprobaciones de actualización del firmware del subsistema de hardware. Se están iniciando los servicios de comunicación entre controladoras.
HC	El sistema comprueba si hay datos de instalación de StorageGRID existentes.
HO	El dispositivo StorageGRID se está ejecutando.
HA	StorageGRID está ejecutando.

Información relacionada

Acceda a la interfaz de BMC

Ver códigos de error del dispositivo

Si se produce un error de hardware cuando el dispositivo arranca, el BMC registra un código de error. Según sea necesario, puede ver estos códigos de error mediante la interfaz del BMC y, a continuación, trabajar con el soporte técnico para resolver el problema.

Lo que necesitará

- Sabe cómo acceder al panel de BMC.

Pasos

1. En el panel de control del BMC, seleccione **Código POST del BIOS**.
2. Revise la información que se muestra para el código actual y el código anterior.

   Si se muestra alguno de los siguientes códigos de error, trabaje con el soporte técnico para resolver el problema.

Codificación	Lo que indica
0x0e	No se ha encontrado el microcódigo
0x0F	No se ha cargado el microcódigo
0x50	Error de inicialización de la memoria. Tipo de memoria no válido o velocidad de memoria incompatible.
0x51	Error de inicialización de la memoria. Error en la lectura del SPD.
0x52	Error de inicialización de la memoria. El tamaño de la memoria no es válido o los módulos de memoria no coinciden.
0x53	Error de inicialización de la memoria. No se detectó memoria utilizable.
0x54	Error de inicialización de memoria no especificada
0x55	Memoria no instalada
0x56	Tipo o velocidad de CPU no válida
0x57	Discordancia de CPU

Codificación	Lo que indica
0x58	Fallo de la autoprueba de CPU o posible error de caché de CPU
0x59	No se ha encontrado el micro-código de la CPU, o la actualización del micro-código ha fallado
0x5A	Error interno de CPU
0x5b	Restablecer PPI no está disponible
0x5c	Fallo de autocomprobación PEI Phase BMC
0xD0	Error de inicialización de la CPU
0xD1	Error de inicialización del puente norte
0xD2	Error de inicialización del puente sur
0xd3	Algunos protocolos de arquitectura no están disponibles
0xD4	Error de asignación de recursos PCI. De recursos.
0xD5	No hay espacio para la ROM de opción heredada
0xD6	No se han encontrado dispositivos de salida de consola
0xD7	No se han encontrado dispositivos de entrada de consola
0xD8	Contraseña no válida
0xD9	Error al cargar la opción de arranque (LoadImage devolvió un error)
0xDA	Error en la opción de inicio (error de Startimage devuelto)
0xDB	Error en la actualización de Flash
0xDC	El protocolo de restablecimiento no está disponible
0xDD	Error de autoprueba de DXE Phase BMC

Codificación	Lo que indica
0xE8	MRC: ERR_NO_MEMORY
0xE9	MRC: ERR_LT_LOCK
0xEA	MRC: ERR_DDR_INIT
0xEB	MRC: ERR_MEM_TEST
0xEC	MRC: ERR_VENDOR_SPECIFIC
0xED	MRC: ERR_DIMM_COMPAT
0xEE	MRC: ERR_MRC_COMPATIBILIDAD
0xEF	MRC: ERR_MRC_STRUCT
0xF0	MRC: ERR_SET_VDD
0xF1	MRC: ERR_IOT_MEM_BUFFER
0xF2	MRC: ERR_RC_INTERNAL
0xF3	MRC: ERR_INVALID_REG_ACCESS
0xF4	MRC: ERR_SET_MC_FREQ
0xF5	MRC: ERR_READ_MC_FREQ
0x70	MRC: ERR_DIMM_CHANNEL
0x74	MRC: ERR_BIST_CHECK
0xF6	MRC: ERR_SMBUS
0xF7	MRC: ERR_PCU
0xF8	MRC: ERR_NGN
0xF9	MRC: ERR_INTERLEAVE_FAILURE

La configuración del hardware parece bloquearse (SG100 y SG1000)

Es posible que el instalador de dispositivos StorageGRID no esté disponible si los

errores de hardware o de cableado impiden que el dispositivo complete el procesamiento de arranque.

Pasos

1. Revise los LED del dispositivo y los códigos de inicio y error que aparecen en el BMC.
2. Si necesita ayuda para resolver un problema, póngase en contacto con el soporte técnico.

Información relacionada

Ver los códigos de arranque del dispositivo

Ver códigos de error del dispositivo

Resolución de problemas de conexión (SG100 y SG1000)

Si tiene problemas de conexión durante la instalación del dispositivo StorageGRID, debe ejecutar los pasos de acción correctiva indicados.

No se puede conectar al dispositivo

Si no puede conectarse al dispositivo de servicios, puede haber un problema de red o puede que la instalación del hardware no se haya completado correctamente.

Pasos

1. Intente hacer ping al dispositivo con la dirección IP del dispositivo :
   `ping services_appliance_IP`
2. Si no recibe respuesta del ping, confirme que está utilizando la dirección IP correcta.

   Puede utilizar la dirección IP del dispositivo en la red de grid, la red de administración o la red de cliente.
3. Si la dirección IP es correcta, compruebe el cableado del dispositivo, los transceptores QSFP o SFP y la configuración de red.
4. Si dispone de acceso físico al dispositivo, puede utilizar una conexión directa a la IP local permanente de enlace `169.254.0.1` para comprobar la configuración de redes de la controladora y actualizarla si es necesario. Para obtener instrucciones detalladas, consulte el paso 2 de la Acceda al instalador de dispositivos de StorageGRID.

   Si esto no se resuelve el problema, póngase en contacto con el soporte técnico.
5. Si el ping se ha realizado correctamente, abra un explorador Web.
6. Introduzca la URL para el instalador de dispositivos de StorageGRID:
   `https://appliances_controller_IP:8443`

   Aparece la página de inicio.

Reinicie el dispositivo de servicios mientras se está ejecutando el instalador de dispositivos de StorageGRID

Es posible que tenga que reiniciar el dispositivo de servicios mientras el instalador de dispositivos de StorageGRID está en ejecución. Por ejemplo, es posible que deba reiniciar el dispositivo de servicios si la instalación falla.

Acerca de esta tarea

Este procedimiento sólo se aplica cuando el dispositivo de servicios ejecuta el instalador de dispositivos StorageGRID. Una vez finalizada la instalación, este paso ya no funciona porque el instalador de dispositivos StorageGRID ya no está disponible.

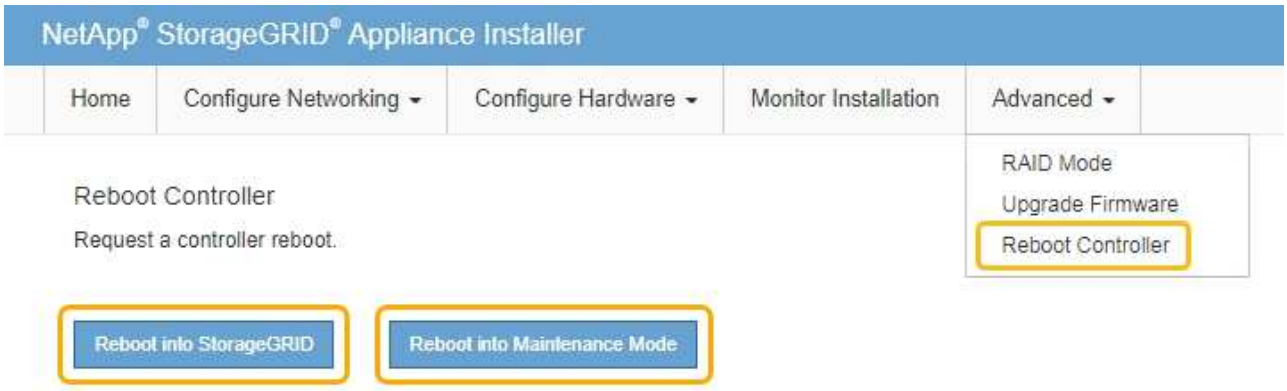
Pasos

1. En la barra de menús del instalador del dispositivo StorageGRID, haga clic en **Avanzado Reiniciar controlador**.

   Se muestra la página Reiniciar controladora.

2. En el instalador del dispositivo StorageGRID, haga clic en **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



   El dispositivo de servicios se reinicia.

Mantenga el dispositivo

Es posible que deba realizar procedimientos de mantenimiento en el dispositivo. En los procedimientos de esta sección se asume que el dispositivo ya se ha implementado como nodo de puerta de enlace o como nodo de administración en un sistema StorageGRID.

Coloque el dispositivo en modo de mantenimiento

Debe colocar el aparato en modo de mantenimiento antes de realizar procedimientos de mantenimiento específicos.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso de mantenimiento o acceso raíz. Para obtener más detalles, consulte las instrucciones para administrar StorageGRID.

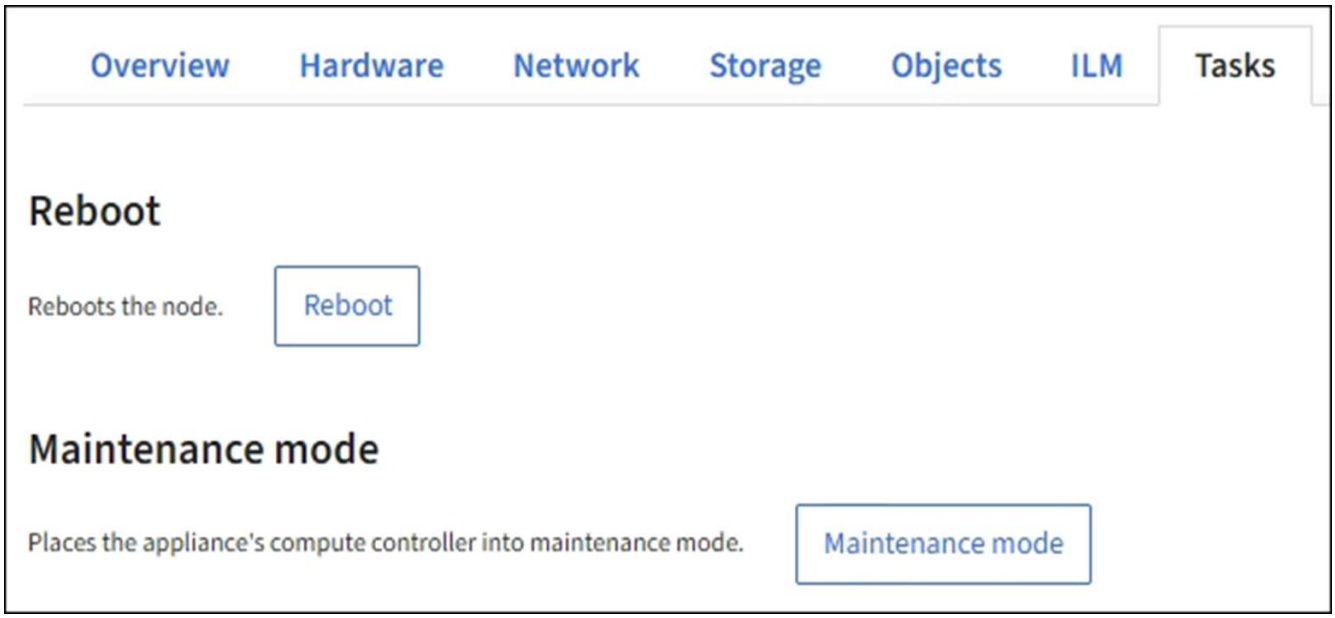
Acerca de esta tarea

En raras ocasiones, una vez que se coloca un dispositivo StorageGRID en modo de mantenimiento puede hacer que el dispositivo no esté disponible para el acceso remoto.

> La contraseña de la cuenta de administrador y las claves de host SSH para un dispositivo StorageGRID en modo de mantenimiento siguen siendo las mismas que en el momento en que el dispositivo estaba en servicio.

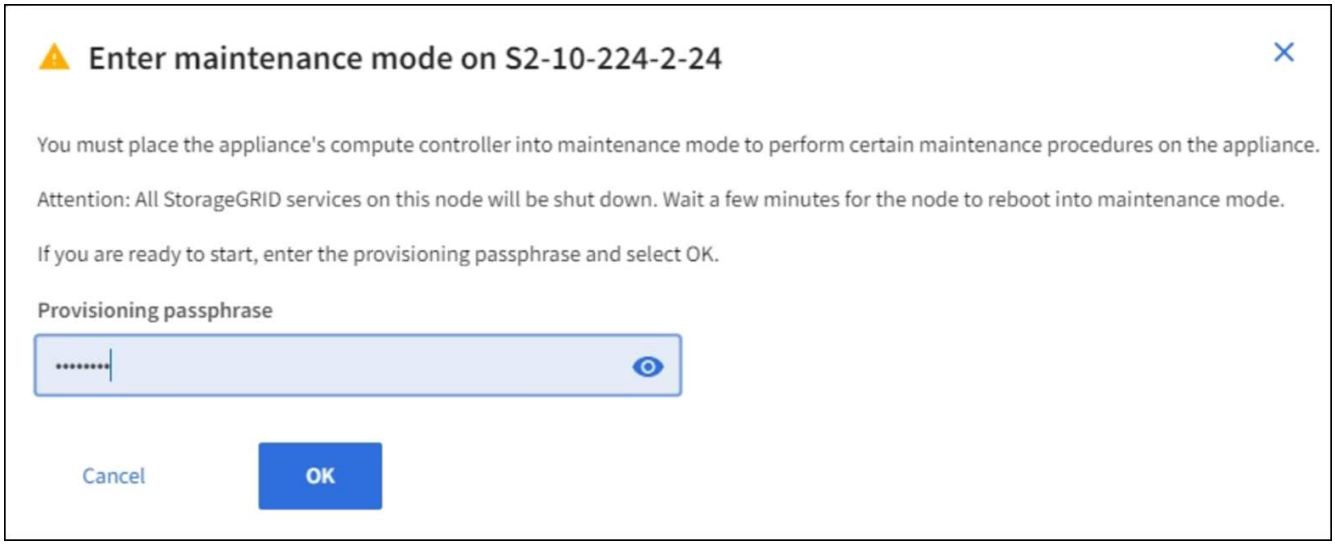
Pasos

1. En Grid Manager, seleccione **NODES**.
2. En la vista de árbol de la página Nodes, seleccione Appliance Storage Node.
3. Seleccione la ficha **tareas**.



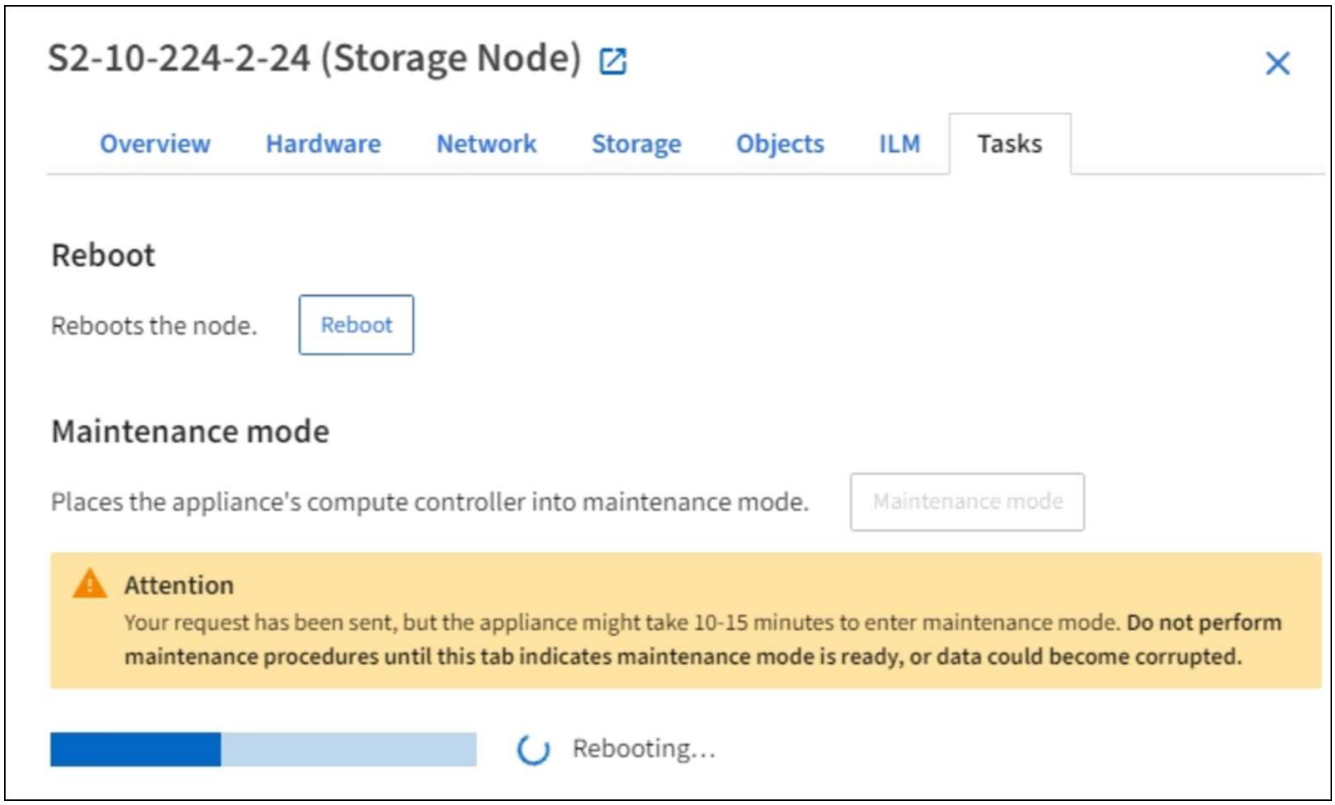
4. Seleccione **modo de mantenimiento**.

   Se muestra un cuadro de diálogo de confirmación.

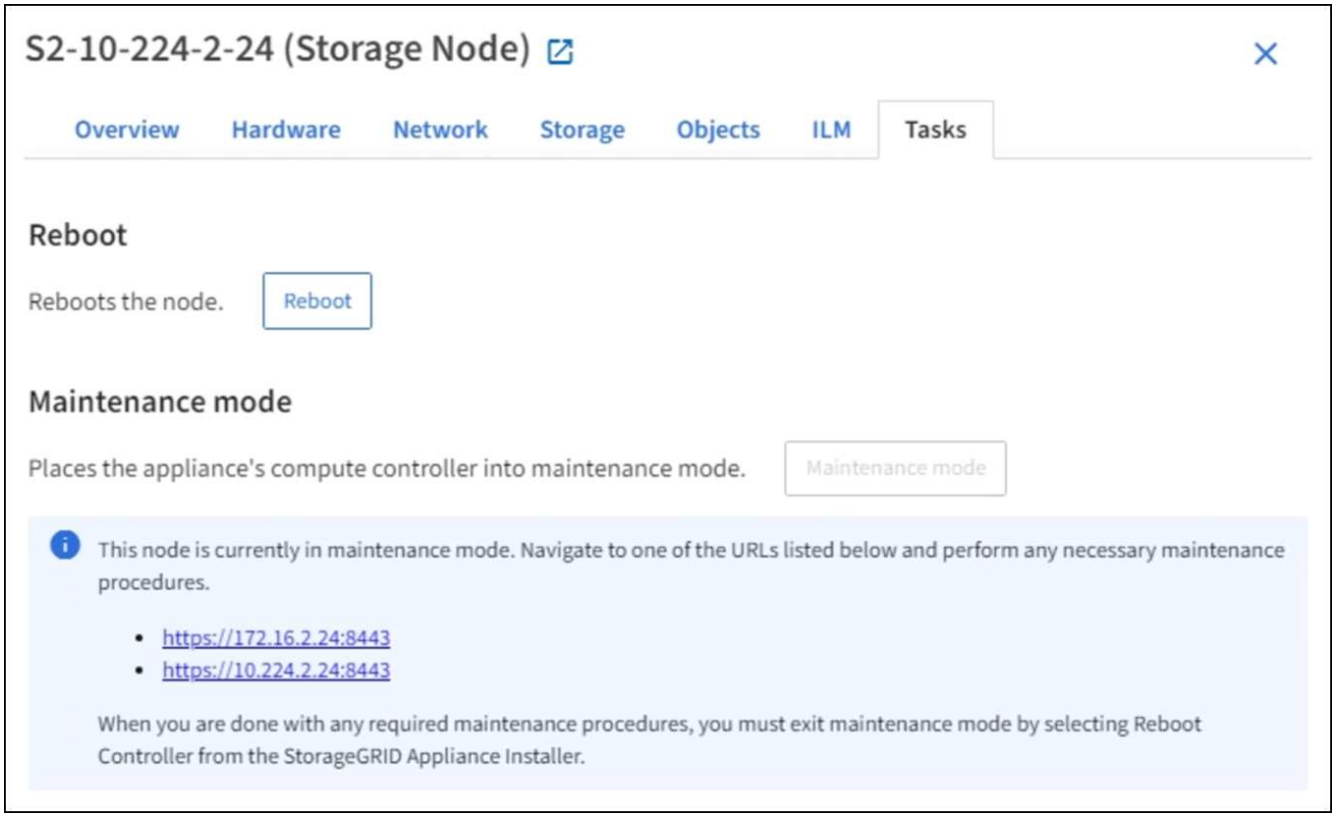


5. Introduzca la contraseña de aprovisionamiento y seleccione **Aceptar**.

   Una barra de progreso y una serie de mensajes, incluidos "solicitud enviada", "detención de StorageGRID" y "reinicio", indican que el dispositivo está llevando a cabo los pasos necesarios para entrar en el modo de mantenimiento.



   Cuando el dispositivo se encuentra en modo de mantenimiento, un mensaje de confirmación enumera las URL que puede utilizar para acceder al instalador de dispositivos de StorageGRID.



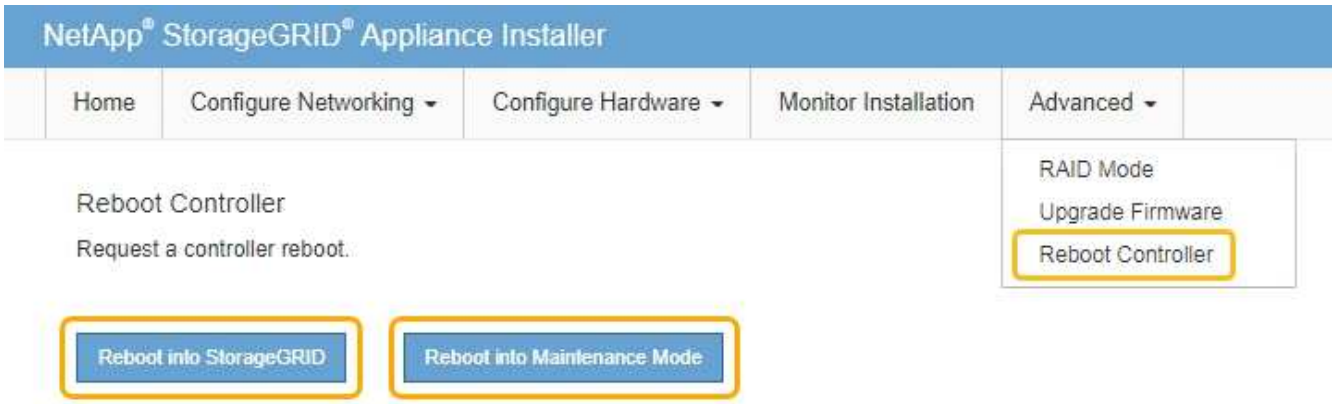
6. Para acceder al instalador de dispositivos de StorageGRID, busque cualquiera de las direcciones URL que se muestren.

   Si es posible, utilice la dirección URL que contiene la dirección IP del puerto de red de administración del dispositivo.

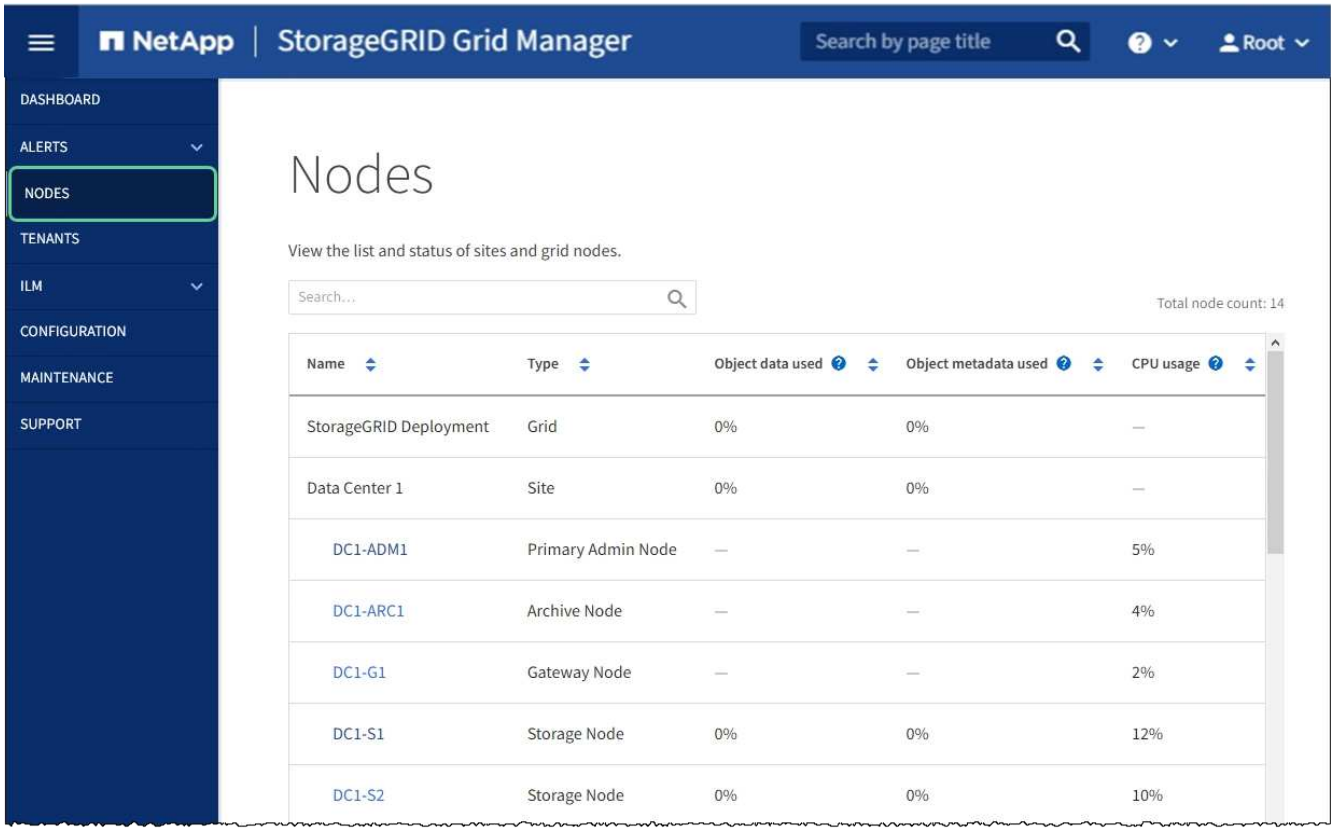
   > Si tiene una conexión directa con el puerto de gestión del dispositivo, utilice `https://169.254.0.1:8443` Para acceder a la página del instalador de dispositivos de StorageGRID.

7. En el instalador de dispositivos StorageGRID, confirme que el dispositivo está en modo de mantenimiento.

8. Realice las tareas de mantenimiento necesarias.
9. Después de completar las tareas de mantenimiento, salga del modo de mantenimiento y reanude el funcionamiento normal del nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione **Reiniciar en StorageGRID**.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Encender y apagar el LED de identificación de la controladora

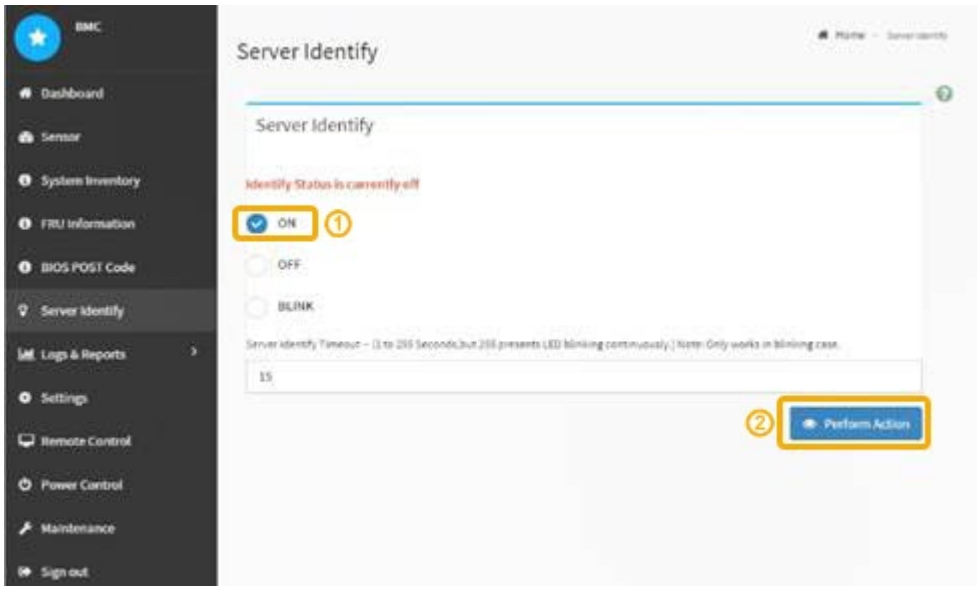
El LED de identificación azul de la parte frontal y trasera de la controladora se puede encender para ayudar a localizar el dispositivo en un centro de datos.

Lo que necesitará

Debe tener la dirección IP del BMC del controlador que desea identificar.

Pasos

1. Acceda a la interfaz del BMC del controlador.
2. Seleccione **Server Identify**.
3. Seleccione **ON** y, a continuación, seleccione **realizar acción**.



Resultado

Los LED de identificación azules se iluminan en la parte frontal (mostrada) y en la parte posterior del controlador.

> Si hay un panel frontal instalado en la controladora, es posible que le resulte difícil ver el LED de identificación frontal.

Después de terminar

Para apagar el controlador Identify LED:

- Pulse el interruptor Identify LED del panel frontal del controlador.
- En la interfaz del controlador BMC, seleccione **Server Identify**, seleccione **OFF** y, a continuación, seleccione **realizar acción**.

Los LED azules de identificación de la parte frontal y trasera del controlador se apagan.

Información relacionada

Ubique la controladora en el centro de datos

Acceda a la interfaz de BMC

Ubique la controladora en el centro de datos

Localice la controladora para que pueda realizar tareas de mantenimiento o actualizaciones del hardware.

Lo que necesitará

- Ha determinado qué controlador requiere mantenimiento.
- (Opcional) para localizar la controladora en el centro de datos, Encienda el LED de identificación azul.

Pasos

1. Encuentre la controladora que requiere mantenimiento en el centro de datos.
   - Busque un LED de identificación azul iluminado en la parte frontal o posterior de la controladora.

     El LED de identificación frontal se encuentra detrás del panel frontal de la controladora y puede ser difícil ver si el panel frontal está instalado.

   - Compruebe si las etiquetas adjuntas a la parte frontal de cada controlador tienen un número de pieza coincidente.
2. Retire el embellecedor frontal del controlador, si se ha instalado, para acceder a los controles e indicadores del panel frontal.

3. Opcional: Apague el LED azul de identificación si lo ha utilizado para localizar el controlador.
   - Pulse el interruptor Identify LED del panel frontal del controlador.
   - Use la interfaz del BMC del controlador.

Apague el aparato de servicios

Apague el dispositivo de servicios para realizar el mantenimiento del hardware.

Lo que necesitará

- Ha localizado físicamente el dispositivo de servicios que requiere mantenimiento en el centro de datos.

  Ubicar la controladora en un centro de datos

- El aparato se ha estado se pone en modo de mantenimiento.

Acerca de esta tarea

Para evitar interrupciones del servicio, apague el dispositivo de servicios durante un periodo de mantenimiento programado cuando normalmente se esperan periodos de interrupción del servicio.

Pasos

1. Cuando el aparato se haya puesto en modo de mantenimiento, apague el aparato:

   > Debe realizar un apagado controlado del dispositivo introduciendo los comandos especificados a continuación. Si apaga el dispositivo con el interruptor de encendido, se perderán datos.

   a. Inicie sesión en el nodo de la cuadrícula mediante PuTTY u otro cliente ssh:
      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. Apague el aparato de servicios:
      `shutdown -h now`

      Este comando puede tardar hasta 10 minutos en completarse.

2. Utilice uno de los siguientes métodos para verificar que el aparato está apagado:
   - Observe el LED de alimentación de la parte frontal del aparato y confirme que está apagado.
   - Compruebe la página Power Control de la interfaz del BMC para confirmar que el aparato está apagado.

Sustituya el aparato de servicios

Es posible que deba sustituir el aparato si no funciona de forma óptima o si ha fallado.

Lo que necesitará

- Tiene un aparato de repuesto con el mismo número de pieza que el aparato que va a sustituir.
- Tiene etiquetas para identificar cada cable que está conectado al dispositivo.
- Ya tienes ubicación física del aparato.
- El aparato se ha estado se colocó en modo de mantenimiento.

Acerca de esta tarea

No se podrá acceder al nodo StorageGRID mientras sustituye el dispositivo. Si el aparato funciona lo suficiente, puede realizar un apagado controlado al inicio de este procedimiento.

> Si va a sustituir el dispositivo antes de instalar el software StorageGRID, es posible que no pueda acceder al instalador de dispositivos StorageGRID inmediatamente después de completar este procedimiento. Aunque puede acceder al instalador del dispositivo StorageGRID desde otros hosts de la misma subred que el dispositivo, no puede acceder al mismo desde hosts de otras subredes. Esta condición debe resolverse dentro de los 15 minutos (cuando se agota cualquier entrada de caché ARP para el tiempo original del dispositivo) o puede borrar la condición de inmediato mediante la purga manual de todas las entradas antiguas de la caché ARP desde el enrutador o la puerta de enlace local.

Pasos

1. Cuando el aparato se haya puesto en modo de mantenimiento, apague el aparato.
   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. Apague el aparato:
      `shutdown -h now`
2. Utilice uno de estos dos métodos para verificar que el aparato está apagado:
   - El LED del indicador de alimentación de la parte frontal del aparato está apagado.
   - La página Power Control de la interfaz del BMC indica que el aparato está apagado.
3. Si las redes StorageGRID conectadas al dispositivo utilizan servidores DHCP, actualice los ajustes de DNS/red y dirección IP.
   a. Busque la etiqueta de dirección MAC en la parte frontal del dispositivo y determine la dirección MAC para el puerto de red de administración.

      > La etiqueta de dirección MAC incluye la dirección MAC para el puerto de gestión del BMC.

      Para determinar la dirección MAC del puerto de red de administración, debe agregar **2** al número hexadecimal de la etiqueta. Por ejemplo, si la dirección MAC de la etiqueta termina en **09**, la dirección MAC del puerto de administración finalizará en **0B**. Si la dirección MAC de la etiqueta termina en **(*y*)FF**, la dirección MAC del puerto de administración finalizará en **(*y*+1)01**. Puede realizar este cálculo fácilmente abriendo Calculadora en Windows, establecerlo en modo Programador, seleccionando hex,

escribiendo la dirección MAC y, a continuación, escribiendo **+ 2 =**.

b. Solicite al administrador de red que asocie el DNS/red y la dirección IP del dispositivo que ha quitado con la dirección MAC del dispositivo de reemplazo.

> Debe asegurarse de que todas las direcciones IP del dispositivo original se han actualizado antes de aplicar alimentación al dispositivo de sustitución. De lo contrario, el dispositivo obtendrá nuevas direcciones IP de DHCP cuando se arranca y es posible que no pueda volver a conectarse a StorageGRID. Este paso se aplica a todas las redes StorageGRID conectadas al dispositivo.

> Si el dispositivo original utilizaba una dirección IP estática, el dispositivo nuevo adoptará automáticamente las direcciones IP del dispositivo que ha quitado.

4. Retire y sustituya el aparato:

   a. Etiquete los cables y desconecte los cables y cualquier transceptor de red.

   > Para evitar un rendimiento degradado, no gire, pliegue, pellizque ni pellizque los cables.

   b. Retire el dispositivo que ha fallado del armario o rack.

   c. Transfiera las dos fuentes de alimentación, ocho ventiladores de refrigeración y dos SSD del dispositivo con error al dispositivo de reemplazo.

      Siga las instrucciones proporcionadas para sustituir estos componentes.

   d. Instale el dispositivo de repuesto en el armario o rack.

   e. Reemplace los cables y cualquier transceptor óptico.

   f. Encienda el dispositivo y supervise los LED del dispositivo y los códigos de inicio.

      Utilice la interfaz de BMC para supervisar el estado de inicio.

5. Confirme que el nodo del dispositivo aparece en Grid Manager y que no aparece ninguna alerta.

Información relacionada

Instalar el dispositivo en un armario o rack (SG100 y SG1000)

Ver los indicadores de estado de los aparatos SG100 y SG1000

Ver los códigos de arranque del dispositivo

Sustituya una o ambas fuentes de alimentación en el dispositivo de servicios

El dispositivo de servicios tiene dos fuentes de alimentación para redundancia. Si uno de los suministros de alimentación falla, debe reemplazarla por Lo antes posible. para garantizar que la controladora de computación tenga alimentación redundante. Ambas fuentes de alimentación que funcionan en la controladora deben ser del mismo modelo y vatios.

Lo que necesitará

- Ya tienes ubicación física del controlador con la fuente de alimentación que se debe sustituir.

- Si solo va a sustituir un suministro de alimentación:
  - Ha desembalado la unidad de suministro de alimentación de repuesto y se ha asegurado de que es el mismo modelo y vataje que la unidad de suministro de alimentación que desea sustituir.
  - Ha confirmado que la otra fuente de alimentación está instalada y en funcionamiento.
- Si va a sustituir ambos suministros de alimentación al mismo tiempo:
  - Ha desembalado las unidades de suministro de alimentación de repuesto y se ha asegurado de que sean del mismo modelo y vataje.

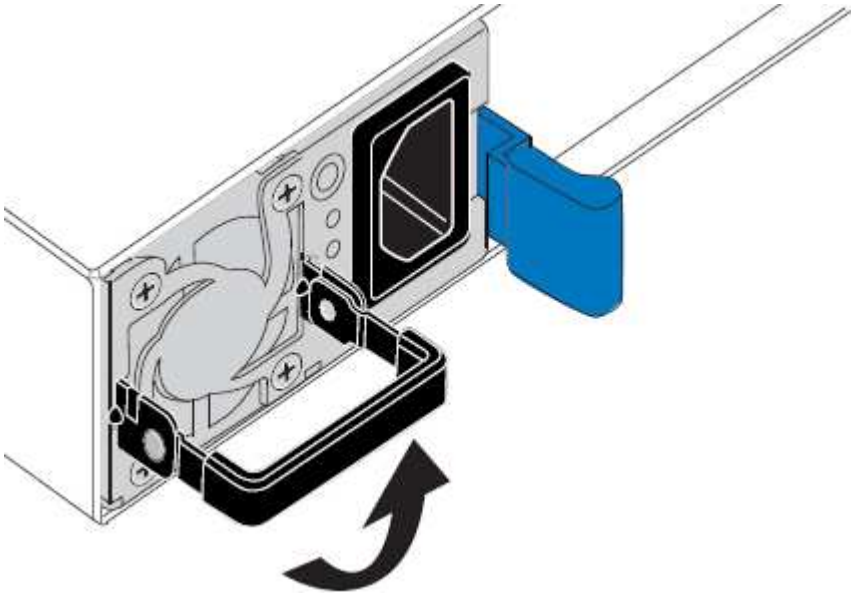
Acerca de esta tarea

La figura muestra las dos unidades de alimentación del SG100, a las que se puede acceder desde la parte posterior del aparato.

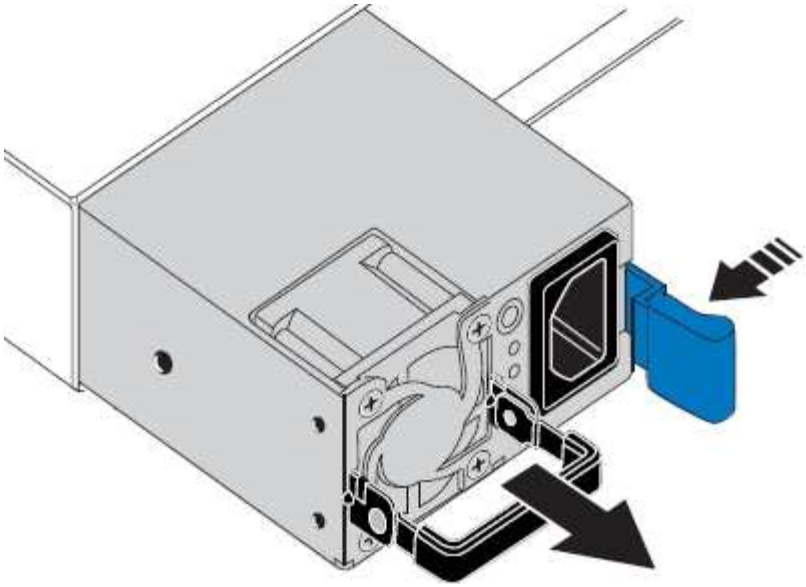
Las fuentes de alimentación del SG1000 son idénticas.

Pasos

1. Si sólo va a sustituir una fuente de alimentación, no es necesario apagar el aparato. Vaya a la Desenchufe el cable de alimentación paso. Si va a sustituir ambas fuentes de alimentación al mismo tiempo, haga lo siguiente antes de desconectar los cables de alimentación:
   a. Coloque el dispositivo en modo de mantenimiento.
   b. Apague el aparato.
2. desenchufe el cable de alimentación de cada fuente de alimentación que vaya a sustituirse.
3. Levante la palanca de leva en el primer suministro que se va a sustituir.



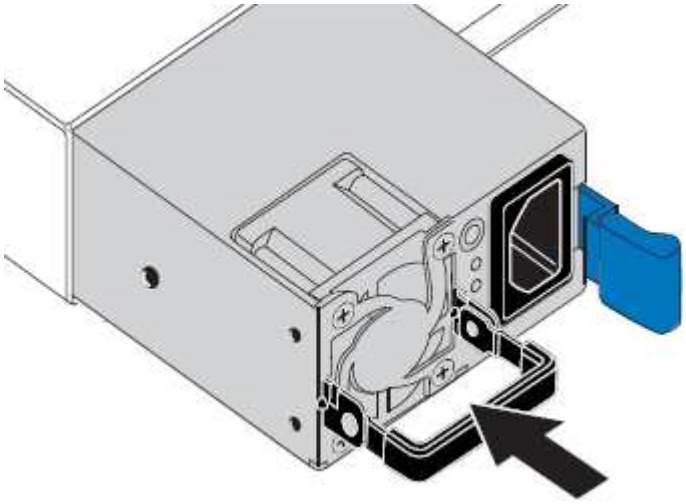
4. Presione el pestillo azul y saque la fuente de alimentación.



5. Con el pestillo azul a la derecha, deslice la fuente de alimentación de repuesto hacia el chasis.

   Ambas fuentes de alimentación deben ser del mismo modelo y vataje.

   Asegúrese de que el pestillo azul está en el lado derecho cuando deslice la unidad de sustitución en.



6. Empuje la palanca de leva hacia abajo para fijar la fuente de alimentación de repuesto.
7. Si va a sustituir ambas fuentes de alimentación, repita los pasos 2 a 6 para sustituir la segunda fuente de alimentación.
8. Conecte los cables de alimentación a las unidades sustituidas y aplique alimentación.
9. Si colocó el aparato en modo de mantenimiento, salga del modo de mantenimiento. En el instalador del dispositivo StorageGRID, seleccione **Avanzado Reiniciar controlador** y, a continuación, seleccione **Reiniciar en StorageGRID**.

Sustituya el ventilador del dispositivo de servicios

El aparato de servicios tiene ocho ventiladores de refrigeración. Si uno de los ventiladores falla, debe reemplazarla por Lo antes posible. para que el dispositivo tenga la refrigeración adecuada.

Lo que necesitará

- Ha desembalado el ventilador de repuesto.
- Ya tienes ubicación física del aparato.
- Ha confirmado que los otros ventiladores están instalados y en ejecución.
- Ya tienes puso el aparato en modo de mantenimiento.

Acerca de esta tarea

No se podrá acceder al nodo del dispositivo mientras sustituye el ventilador.

La fotografía muestra un ventilador para el aparato de servicios. Se puede acceder a los ventiladores de refrigeración después de retirar la cubierta superior del aparato.

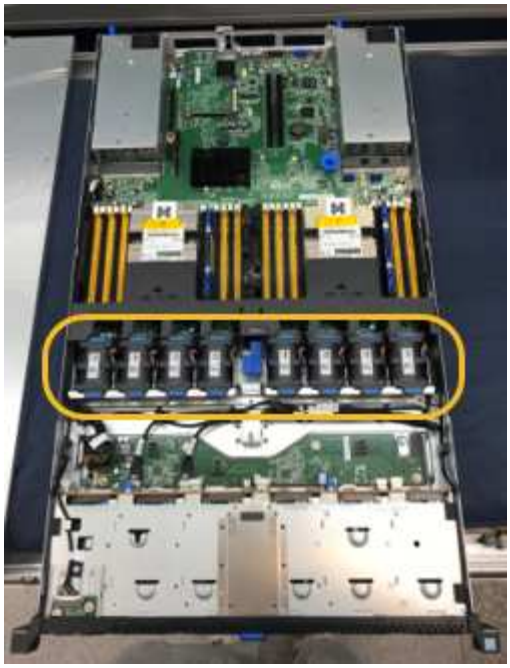
> Cada una de las dos unidades de suministro de alimentación también contiene un ventilador. Estos ventiladores no están incluidos en este procedimiento.

Pasos

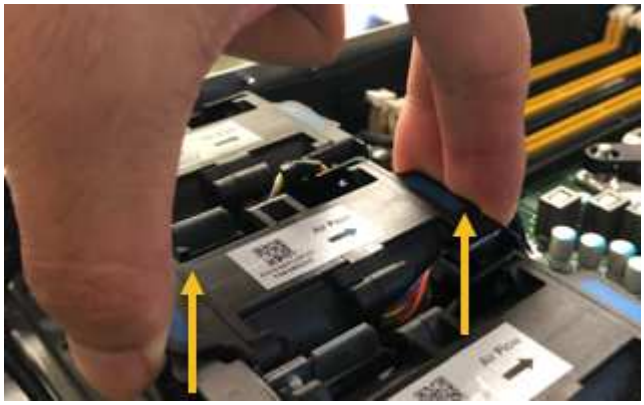
1. Cuando el aparato se haya puesto en modo de mantenimiento, apague el aparato.
   a. Inicie sesión en el nodo de grid:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando 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. Apague el aparato de servicios:
      `shutdown -h now`
2. Utilice uno de estos dos métodos para comprobar que la alimentación del dispositivo de servicios está desactivada:
   - El LED del indicador de alimentación de la parte frontal del aparato está apagado.
   - La página Power Control de la interfaz del BMC indica que el aparato está apagado.
3. Tire del aparato para extraerlo del rack.
4. Levante el pestillo de la cubierta superior y retire la cubierta del aparato.
5. Localice el ventilador que falló.

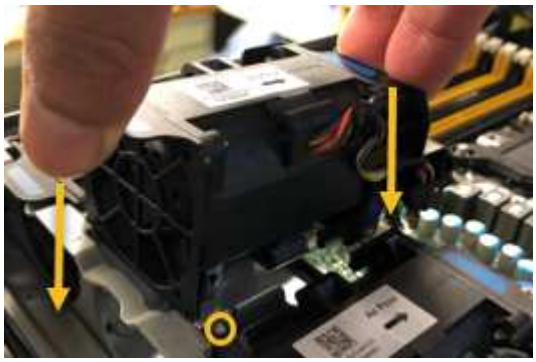


6. Levante el ventilador fallido para sacarlo del chasis.

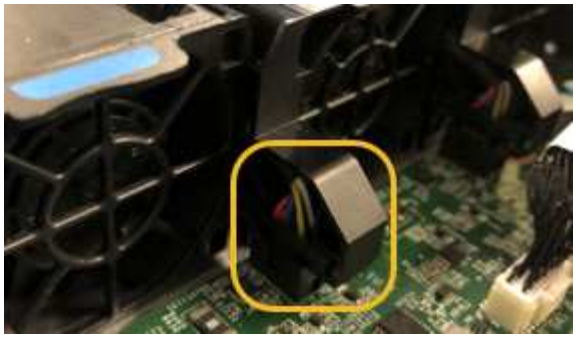


7. Deslice el ventilador de repuesto en la ranura abierta del chasis.

   Alinee el borde del ventilador con el pasador guía. El pasador está en un círculo en la fotografía.



8. Presione firmemente el conector del ventilador en la placa de circuitos.



9. Vuelva a colocar la cubierta superior en el aparato y presione el pestillo hacia abajo para fijar la cubierta en su lugar.
10. Encienda el dispositivo y supervise los LED del controlador y los códigos de arranque.

    Utilice la interfaz de BMC para supervisar el estado de inicio.

11. Confirme que el nodo del dispositivo aparece en Grid Manager y que no aparece ninguna alerta.

Sustituya la unidad en el dispositivo de servicios

Los SSD del dispositivo de servicios contienen el sistema operativo StorageGRID. Además, cuando el dispositivo se configura como un nodo de administración, los SSD también contienen registros de auditoría, métricas y tablas de bases de datos. Las unidades se reflejan con RAID1 para redundancia. Si una de las unidades falla, es necesario reemplazarla por Lo antes posible. para garantizar la redundancia.

Lo que necesitará

- Ya tienes ubicación física del aparato.
- Ha comprobado qué unidad ha fallado, teniendo en cuenta que el LED izquierdo parpadea en color ámbar.

> Si elimina la unidad de trabajo, descerá el nodo del dispositivo. Consulte la información sobre la visualización de los indicadores de estado para verificar el fallo.

- Ha obtenido la unidad de reemplazo.
- Ha obtenido la protección ESD adecuada.

Pasos

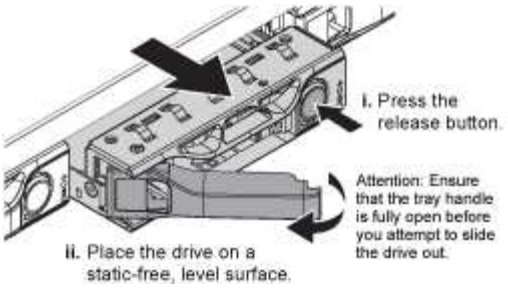
1. Compruebe que el LED izquierdo de la unidad parpadea en color ámbar.

   También puede utilizar Grid Manager para supervisar el estado de los SSD. Seleccione **NODES**. A continuación, seleccione **`Appliance Node` Hardware**. Si se produce un error en una unidad, el campo Storage RAID Mode contiene un mensaje acerca de qué unidad ha fallado.

2. Envuelva el extremo de la correa de la muñequera ESD alrededor de su muñeca y fije el extremo de la pinza a una masa metálica para evitar descargas estáticas.
3. Desembale la unidad de repuesto y configúrela en una superficie nivelada y sin estática cerca del aparato.

   Guarde todos los materiales de embalaje.

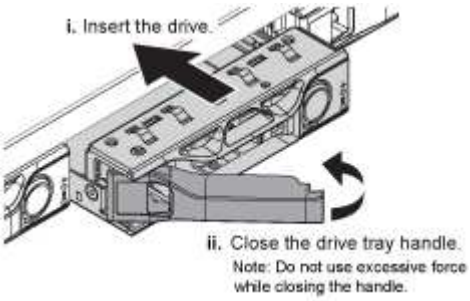
4. Pulse el botón de liberación de la unidad con error.



La palanca de los muelles de accionamiento se abre parcialmente y la unidad se libera de la ranura.

5. Abra el asa, deslice la unidad hacia fuera y colóquela en una superficie nivelada y sin estática.
6. Presione el botón de liberación de la unidad de reemplazo antes de insertarla en la ranura de la unidad.

   Los muelles de pestillo se abren.



7. Inserte la unidad de reemplazo en la ranura y, a continuación, cierre el asa de la unidad.

   No ejerza una fuerza excesiva mientras cierra la palanca.

   Cuando la unidad se inserta por completo, se oye un clic.

   La unidad se reconstruye automáticamente con datos reflejados de la unidad en funcionamiento. Puede comprobar el estado de la reconstrucción mediante Grid Manager. Seleccione **NODES**. A continuación, seleccione **`Appliance Node` Hardware**. El campo Storage RAID Mode contiene un mensaje de «reforma» hasta que la unidad se reconstruya por completo.

8. Póngase en contacto con el soporte técnico acerca del reemplazo de la unidad.

   El soporte técnico proporciona instrucciones para devolver la unidad con error.

Cambiar la configuración del vínculo de servicio del dispositivo

Puede cambiar la configuración del enlace Ethernet del dispositivo de servicios. Puede cambiar el modo de enlace de puerto, el modo de enlace de red y la velocidad del enlace.

Lo que necesitará

- Ya tienes puso el aparato en modo de mantenimiento.

En raras ocasiones, una vez que se coloca un dispositivo StorageGRID en modo de mantenimiento puede hacer que el dispositivo no esté disponible para el acceso remoto.

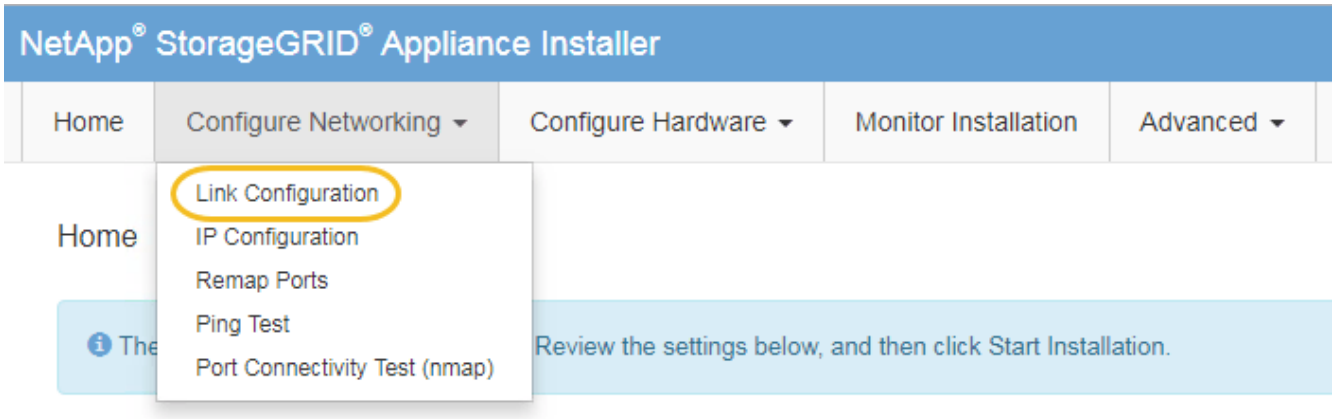
Acerca de esta tarea

Entre las opciones para cambiar la configuración del enlace Ethernet del dispositivo de servicios se incluyen las siguientes:

- Cambiando **modo de enlace de puerto** de fijo a agregado, o de agregado a fijo
- Cambio del **modo de enlace de red** de Active-Backup a LACP o de LACP a Active-Backup
- Habilitar o deshabilitar el etiquetado de VLAN, o cambiar el valor de una etiqueta de VLAN
- Cambio de la velocidad de enlace

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Configurar la red Configuración del enlace**.



2. Realice los cambios deseados en la configuración del enlace.

   Para obtener más información sobre las opciones, consulte Configure los enlaces de red.

3. Cuando esté satisfecho con sus selecciones, haga clic en **Guardar**.

   > Puede perder la conexión si ha realizado cambios en la red o el enlace que está conectado a través de. Si no vuelve a conectarse en un minuto, vuelva a introducir la URL del instalador de dispositivos StorageGRID utilizando una de las otras direcciones IP asignadas al dispositivo:
   > **`https://services_appliance_IP:8443`**

4. Realice los cambios necesarios en las direcciones IP del dispositivo.

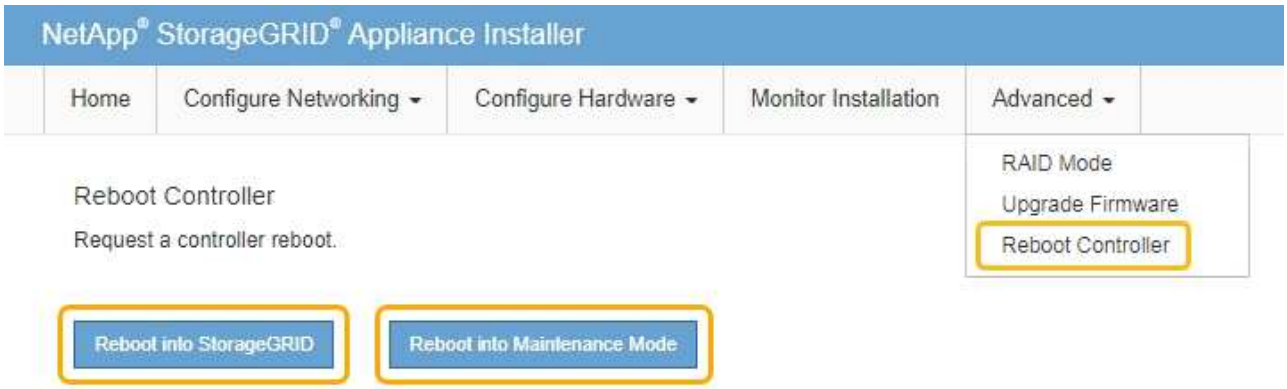
   Si ha realizado cambios en la configuración de VLAN, es posible que la subred del dispositivo haya cambiado. Si necesita cambiar las direcciones IP del dispositivo, consulte Configure las direcciones IP de StorageGRID.

5. Seleccione **Configurar redes Prueba de ping** en el menú.
6. Utilice la herramienta Ping Test para comprobar la conectividad a las direcciones IP en cualquier red que pudiera haber sido afectada por los cambios de configuración de vínculos que haya realizado al configurar el dispositivo.

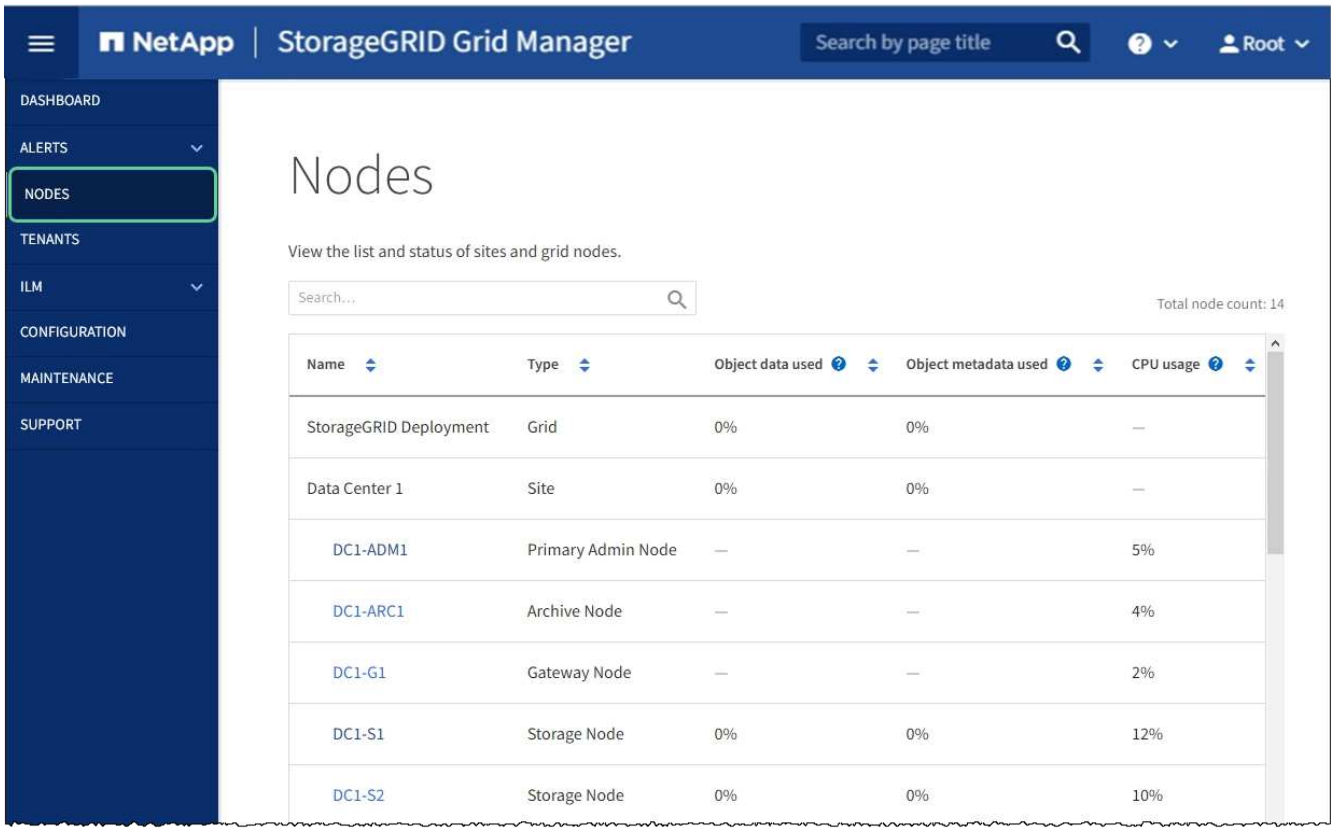
   Además de cualquier otra prueba que elija realizar, confirme que puede hacer ping a la dirección IP de red de cuadrícula del nodo de administración principal y a la dirección IP de red de cuadrícula de al menos otro nodo. Si es necesario, vuelva a las instrucciones para configurar los enlaces de red y corrija cualquier problema.

7. Una vez que esté satisfecho de que los cambios en la configuración del enlace funcionan, reinicie el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



   El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Cambie la configuración de MTU

Puede cambiar la configuración de MTU que asigne al configurar las direcciones IP para el nodo del dispositivo.

> **Acerca de esta tarea**
>
> 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. Los valores de MTU no tienen que ser iguales para todos los tipos de red.

Para cambiar la configuración de MTU sin reiniciar el nodo del dispositivo, Utilice la herramienta Cambiar IP.

Si la red de cliente o administrador no se configuró en el instalador de dispositivos de StorageGRID durante la instalación inicial, Cambie la configuración de MTU con el modo de mantenimiento.

Cambie la configuración de MTU mediante la herramienta Cambiar IP

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo para utilizar la herramienta Cambiar IP.

Pasos

Acceda a la herramienta Cambiar IP y actualice la configuración de MTU como se describe en Cambie la

configuración de red de los nodos.

Cambie la configuración de MTU con el modo de mantenimiento

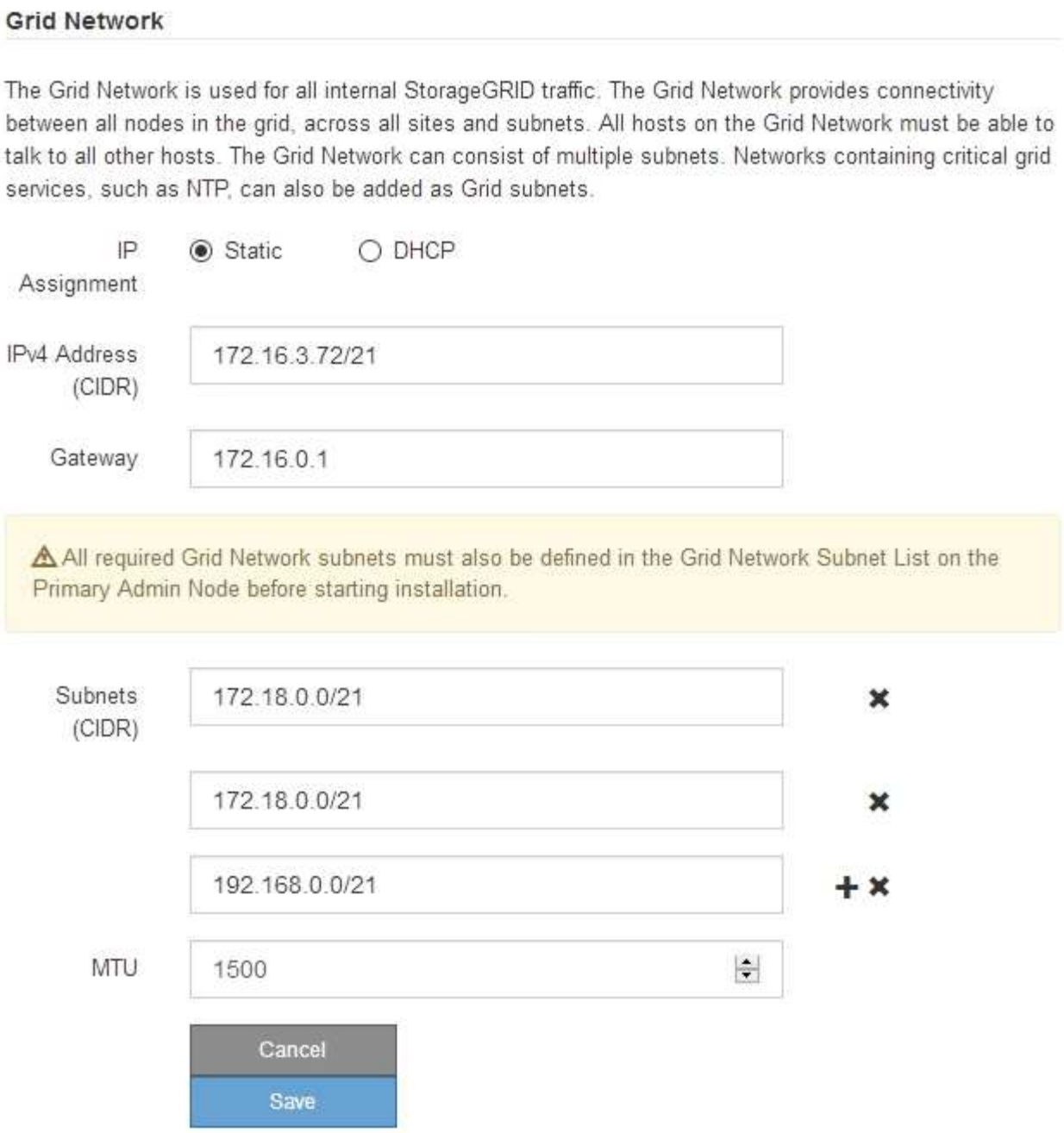
Cambie la configuración de MTU mediante el modo de mantenimiento si no puede acceder a estas opciones con la herramienta Cambiar IP.

Lo que necesitará

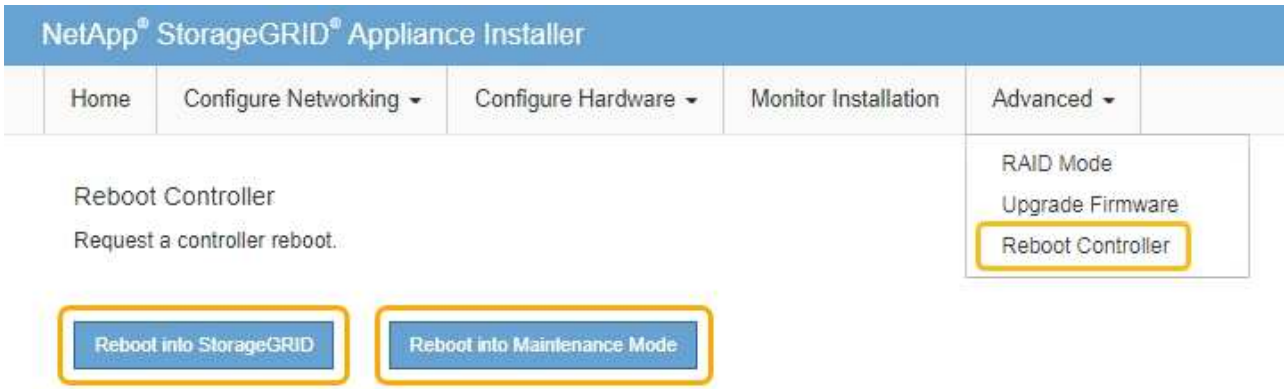
- Ya tienes puso el aparato en modo de mantenimiento.

Pasos

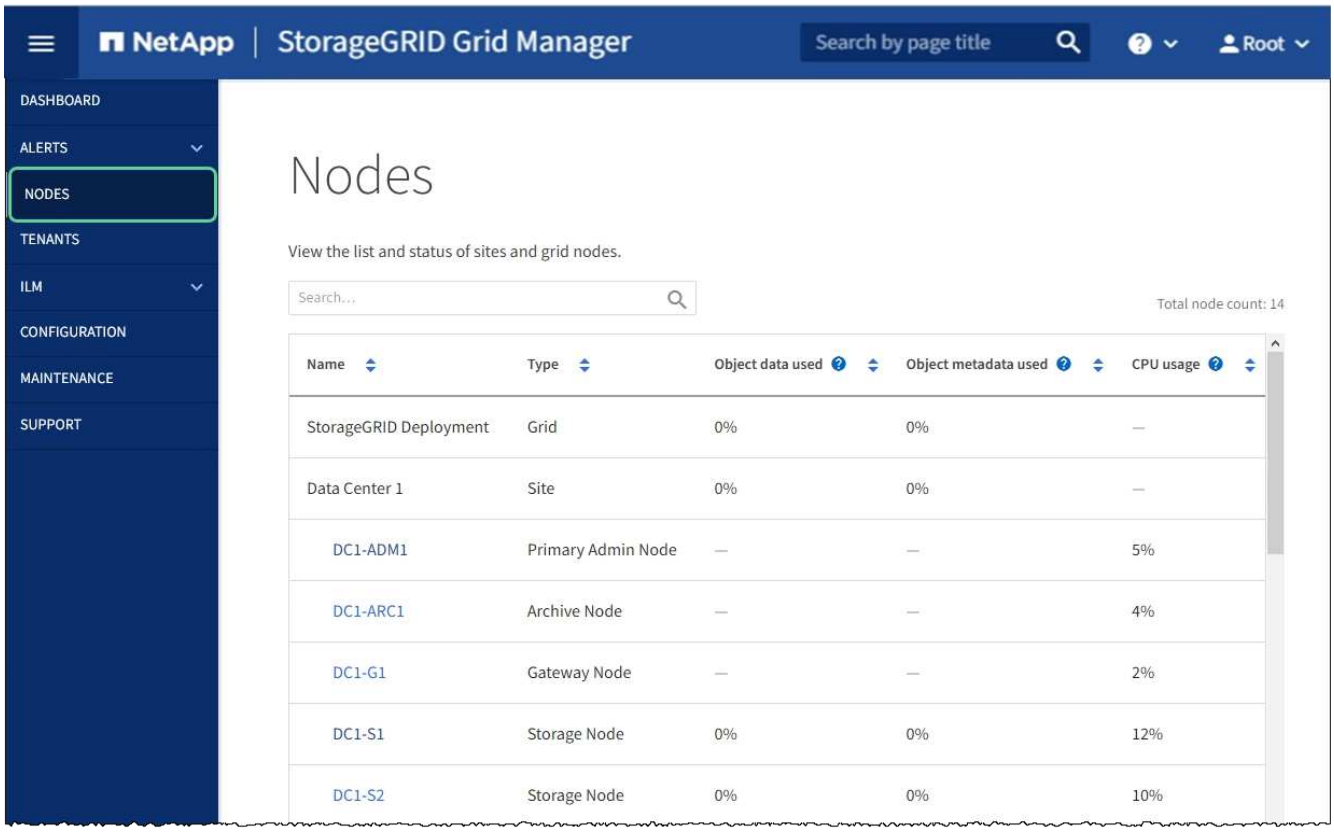
1. En el instalador del dispositivo StorageGRID, seleccione **Configurar redes** > **Configuración IP**.
2. Realice los cambios deseados en la configuración de MTU para la red de grid, la red de administración y la red de cliente.



3. Cuando esté satisfecho con los ajustes, seleccione **Guardar**.
4. Reiniciar el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:
   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Administre StorageGRID

Comprobar la configuración del servidor DNS

Puede comprobar y cambiar temporalmente los servidores del sistema de nombres de dominio (DNS) que está utilizando actualmente este nodo de dispositivo.

Lo que necesitará

- Ya tienes puso el aparato en modo de mantenimiento.

Acerca de esta tarea

Es posible que deba cambiar la configuración del servidor DNS si un dispositivo cifrado no puede conectarse con el servidor de gestión de claves (KMS) o un clúster KMS porque el nombre de host del KMS se especificó como un nombre de dominio en lugar de una dirección IP. Cualquier cambio realizado en la configuración de DNS del dispositivo es temporal y se pierde al salir del modo de mantenimiento. Para que estos cambios sean permanentes, especifique los servidores DNS en Grid Manager (**MAINTENANCE** > **Network** > **servidores DNS**).

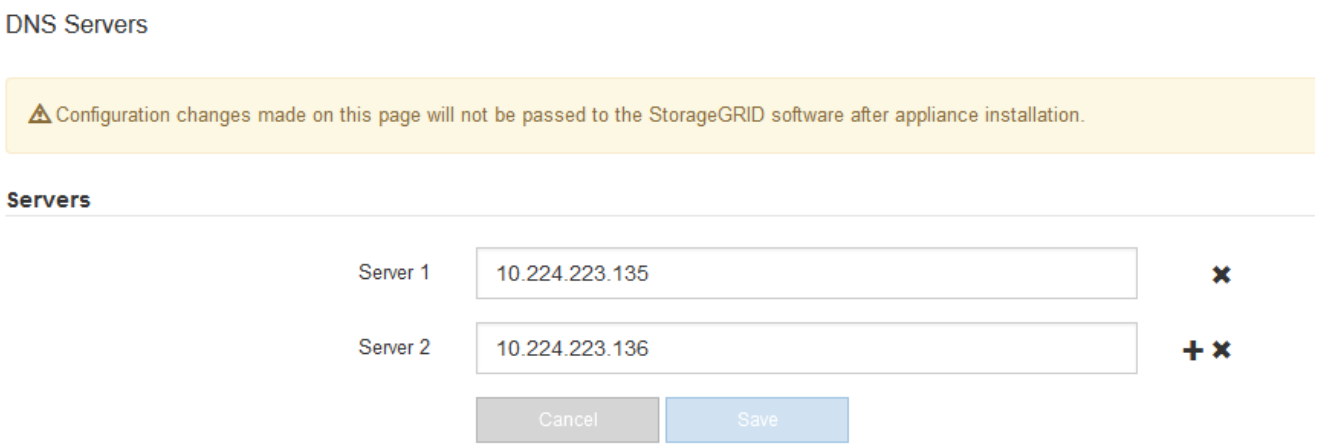
- Los cambios temporales en la configuración DNS sólo son necesarios para los dispositivos cifrados por nodo en los que el servidor KMS se define mediante un nombre de dominio completo, en lugar de una dirección IP, para el nombre de host.
- Cuando un dispositivo cifrado por nodo se conecta a un KMS mediante un nombre de dominio, debe conectarse a uno de los servidores DNS definidos para la cuadrícula. A continuación, uno de estos servidores DNS convierte el nombre de dominio en una dirección IP.
- Si el nodo no puede llegar a un servidor DNS para la cuadrícula, o si cambió la configuración de DNS para toda la cuadrícula cuando un nodo de dispositivo cifrado por nodo estaba sin conexión, el nodo no podrá conectarse al KMS. Los datos cifrados en el dispositivo no se pueden descifrar hasta que se resuelva el problema de DNS.

Para resolver un problema de DNS que impide la conexión de KMS, especifique la dirección IP de uno o más servidores DNS en el instalador de dispositivos de StorageGRID. Estas configuraciones temporales de DNS permiten que el dispositivo se conecte al KMS y descifre los datos en el nodo.

Por ejemplo, si el servidor DNS de la cuadrícula cambia mientras un nodo cifrado estaba desconectado, el nodo no podrá llegar al KMS cuando vuelva a conectarse, ya que sigue utilizando los valores DNS anteriores. La introducción de la nueva dirección IP del servidor DNS en el instalador de dispositivos de StorageGRID permite que una conexión KMS temporal descifre los datos del nodo.

Pasos

1. En el instalador de dispositivos StorageGRID, seleccione **Configurar redes** > **Configuración de DNS**.
2. Compruebe que los servidores DNS especificados sean correctos.



3. Si es necesario, cambie los servidores DNS.

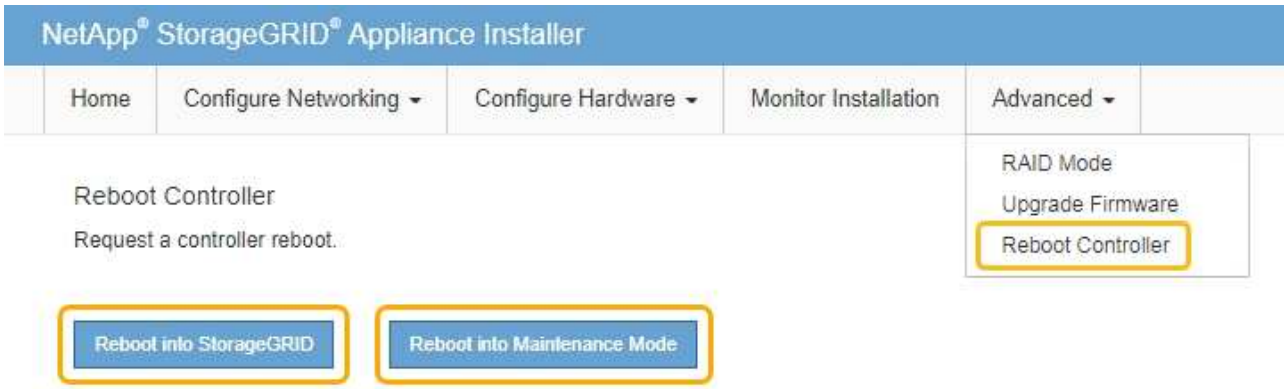
> Los cambios realizados en la configuración de DNS son temporales y se pierden al salir del modo de mantenimiento.

4. Cuando esté satisfecho con la configuración temporal de DNS, seleccione **Guardar**.

   El nodo utiliza la configuración del servidor DNS especificada en esta página para volver a conectarse al KMS, lo que permite descifrar los datos del nodo.

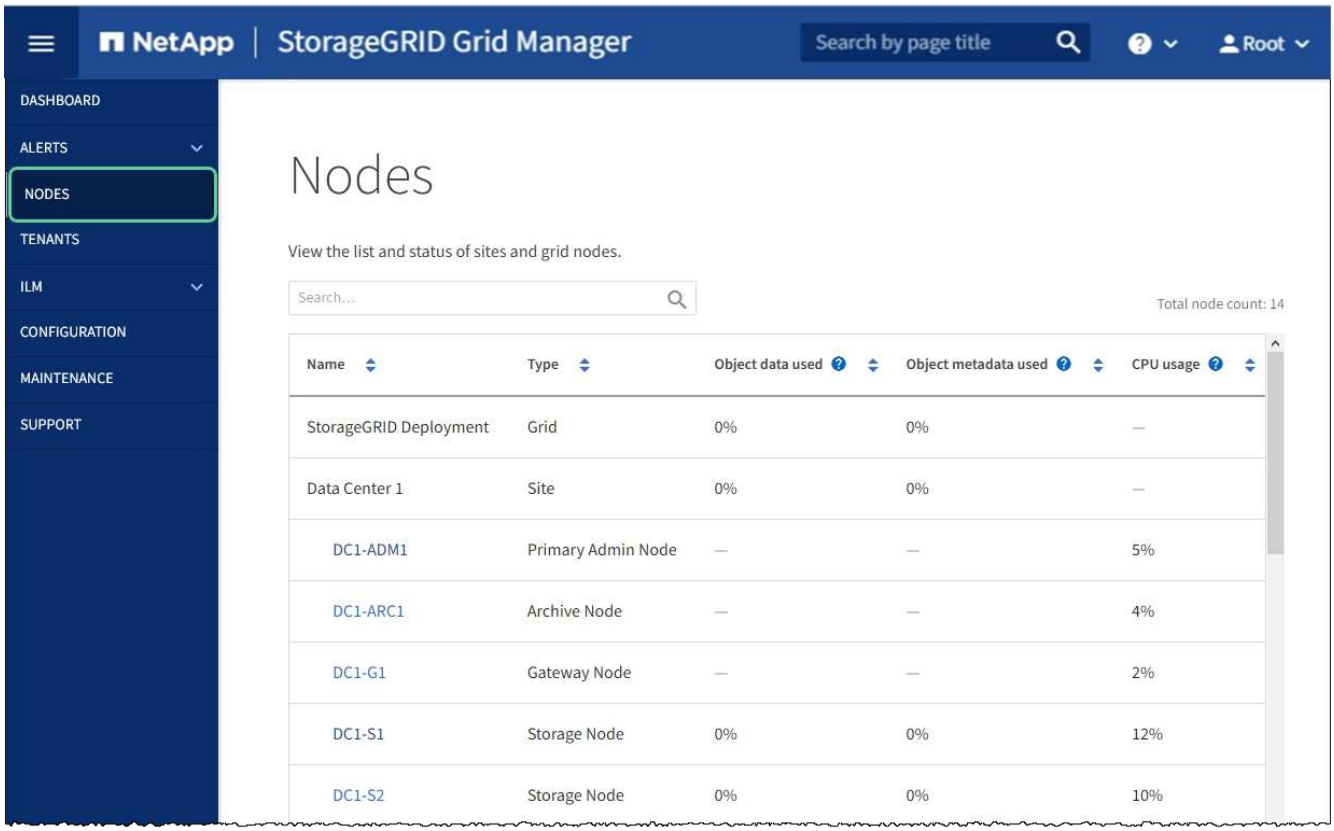
5. Tras descifrar los datos del nodo, reinicie el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



> Cuando el nodo se reinicia y se vuelve a unir a la cuadrícula, utiliza los servidores DNS de todo el sistema enumerados en Grid Manager. Después de volver a unirse a la cuadrícula, el dispositivo ya no utilizará los servidores DNS temporales especificados en el instalador de dispositivos StorageGRID mientras el dispositivo estaba en modo de mantenimiento.

El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Supervisión del cifrado de nodos en modo de mantenimiento (SG100 y SG1000)

Si habilitó el cifrado de nodos para el dispositivo durante la instalación, puede supervisar el estado de cifrado del nodo de cada nodo de dispositivo, incluidos el estado del cifrado del nodo y detalles del servidor de gestión de claves (KMS).

Lo que necesitará

- Ha habilitado el cifrado de nodos para el dispositivo durante la instalación. No se puede habilitar el cifrado de nodos después de que el dispositivo se haya instalado.
- Ya tienes puso el aparato en modo de mantenimiento.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Configurar hardware** > **cifrado de nodos**.

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption ☑

Save

Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate >

Client certificate >

Clear KMS Key

Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

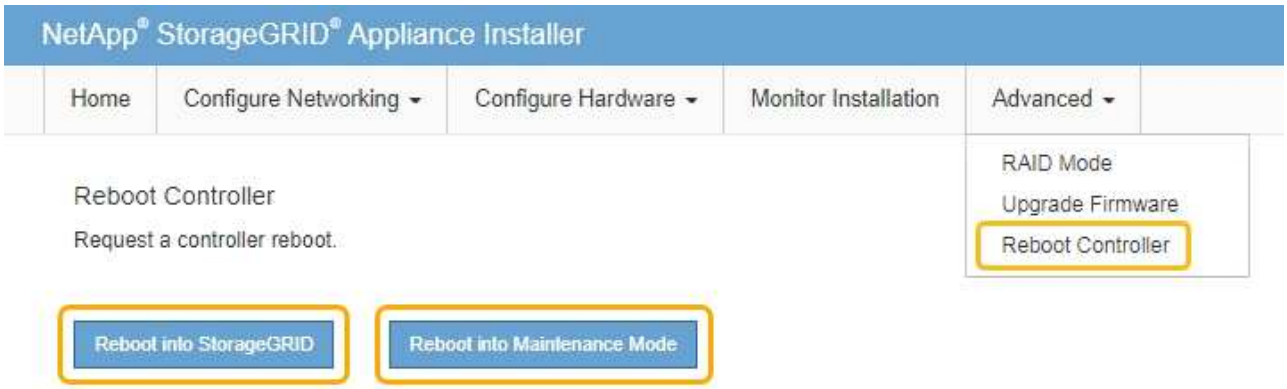
La página cifrado de nodos incluye tres secciones:

- El estado de cifrado muestra si el cifrado de nodos está habilitado o deshabilitado para el dispositivo.
- Detalles del servidor de gestión de claves muestra información sobre el KMS que se utiliza para cifrar el dispositivo. Puede expandir las secciones de certificados de servidor y cliente para ver los detalles y el estado del certificado.
  - Para solucionar problemas con los propios certificados, como renovar certificados caducados, consulte Instrucciones para configurar KMS.
  - Si hay problemas inesperados al conectarse a los hosts KMS, compruebe que Los servidores del sistema de nombres de dominio (DNS) son correctos y eso la red del dispositivo está configurada correctamente.
  - Si no puede resolver problemas de certificado, póngase en contacto con el soporte técnico.
- Clear KMS Key deshabilita el cifrado de nodos para el dispositivo, elimina la asociación entre el dispositivo y el servidor de gestión de claves configurado para el sitio StorageGRID y elimina todos los datos del dispositivo. Debe Borre la clave KMS Antes de poder instalar el dispositivo en otro sistema

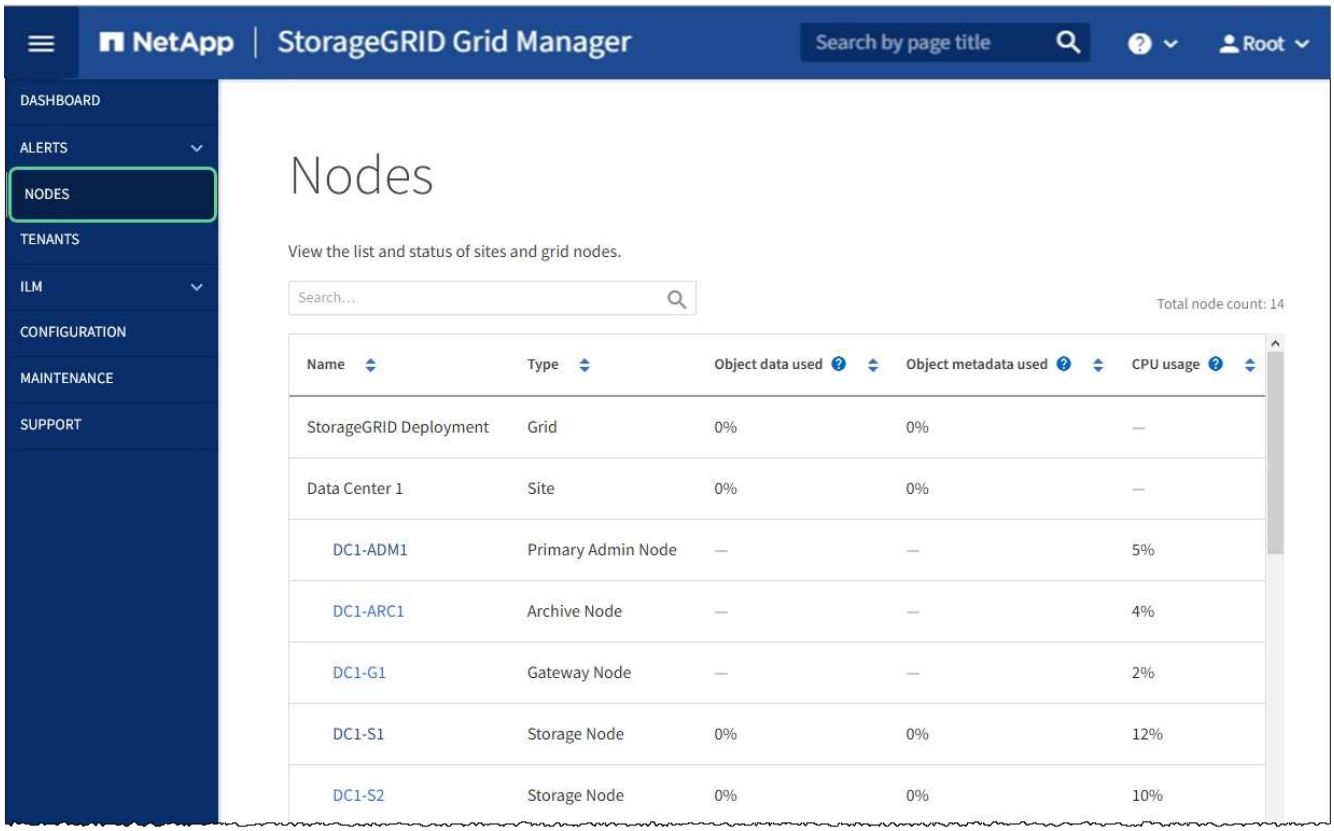
StorageGRID.

> Al borrar la configuración de KMS se eliminan los datos del dispositivo, lo que hace que no se pueda acceder a ellos de forma permanente. Estos datos no se pueden recuperar.

2. Cuando haya terminado de comprobar el estado de cifrado de nodo, reinicie el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:
   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de poder volver a unirse a la cuadrícula.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Administre StorageGRID

Borrar configuración de servidor de gestión de claves

Al borrar la configuración del servidor de gestión de claves (KMS), se deshabilita el cifrado de nodos en el dispositivo. Tras borrar la configuración de KMS, los datos del dispositivo se eliminan de forma permanente y ya no se puede acceder a ellos. Estos datos no se pueden recuperar.

Lo que necesitará

Si necesita conservar datos en el dispositivo, debe realizar un procedimiento de retirada del nodo o clonar el nodo antes de borrar la configuración de KMS.

> Cuando se borra KMS, los datos del dispositivo se eliminan de forma permanente y ya no se puede acceder a ellos. Estos datos no se pueden recuperar.

Retire el nodo para mover los datos que contiene a otros nodos de la cuadrícula.

Acerca de esta tarea

Al borrar la configuración de KMS del dispositivo, se deshabilita el cifrado de nodos y se elimina la asociación entre el nodo del dispositivo y la configuración de KMS del sitio StorageGRID. Los datos del dispositivo se eliminan y el dispositivo se deja en estado previo a la instalación. Este proceso no se puede revertir.

Debe borrar la configuración de KMS:

- Antes de poder instalar el dispositivo en otro sistema StorageGRID, que no utiliza un KMS o que utiliza un

KMS diferente.

> No borre la configuración de KMS si piensa volver a instalar un nodo de dispositivo en un sistema StorageGRID que utilice la misma clave KMS.

- Antes de poder recuperar y volver a instalar un nodo en el que se perdió la configuración de KMS y la clave KMS no se puede recuperar.
- Antes de devolver cualquier aparato que se haya utilizado anteriormente en su centro.
- Después de retirar un dispositivo con el cifrado de nodos habilitado.

> Retire el dispositivo antes de borrar KMS para mover sus datos a otros nodos del sistema StorageGRID. La eliminación de KMS antes de retirar el dispositivo provocará la pérdida de datos y podría hacer que el dispositivo deje de funcionar.

Pasos

1. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.

   `https://`*`Controller_IP`*`:8443`

   `Controller_IP` Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Configurar hardware** > **cifrado de nodos**.

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption ☑

Save

Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate >

Client certificate >

Clear KMS Key

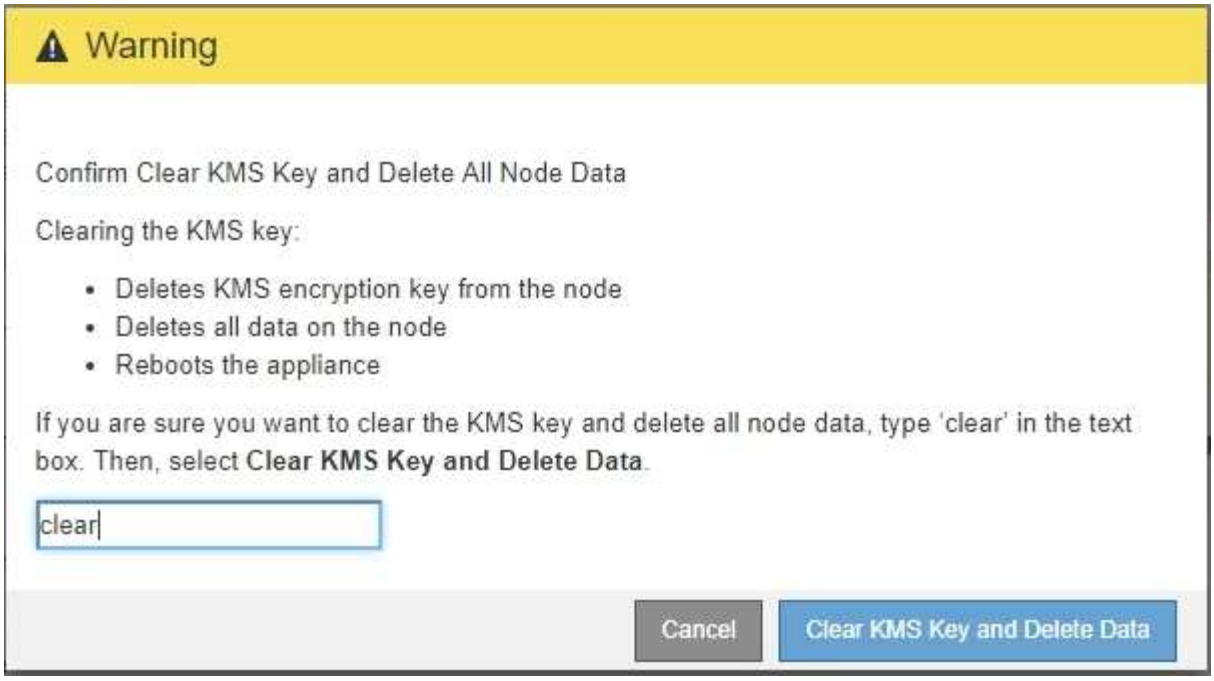
Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

> Si se borra la configuración de KMS, los datos del dispositivo se eliminarán permanentemente. Estos datos no se pueden recuperar.

3. En la parte inferior de la ventana, seleccione **Borrar clave KMS y Eliminar datos**.
4. Si está seguro de que desea borrar la configuración de KMS, escriba `clear` + y seleccione **Borrar clave KMS y Eliminar datos**.



La clave de cifrado KMS y todos los datos se eliminan del nodo y el dispositivo se reinicia. Esto puede tardar hasta 20 minutos.

5. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.
   `https://Controller_IP:8443`

   `Controller_IP` Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

6. Seleccione **Configurar hardware** > **cifrado de nodos**.
7. Compruebe que el cifrado de nodos está desactivado y que la información de claves y certificados de **Detalles del servidor de administración de claves** y el control **Borrar clave KMS y Eliminar datos** se eliminan de la ventana.

   El cifrado de nodos no se puede volver a habilitar en el dispositivo hasta que se vuelva a instalar en una cuadrícula.

Después de terminar

Una vez que el dispositivo se haya reiniciado y haya verificado que se ha borrado KMS y que el dispositivo está en estado previo a la instalación, puede quitar físicamente el dispositivo del sistema de StorageGRID. Consulte instrucciones para preparar el aparato para su reinstalación.

Información relacionada

Administre StorageGRID

Dispositivos de almacenamiento SG6000

Dispositivos SG6000: Descripción general

Los dispositivos SG6000 de StorageGRID son plataformas informáticas y de almacenamiento integradas que funcionan como nodos de almacenamiento en un sistema StorageGRID. Estos dispositivos se pueden utilizar en un entorno de grid híbrido que combina nodos de almacenamiento de dispositivos y nodos de almacenamiento virtuales (basados en software).

Los dispositivos SG6000 ofrecen las siguientes características:

- Disponible en tres modelos:
  - SG6060, que incluye 60 unidades, admite bandejas de expansión y utiliza controladoras E2800A.
  - SG606060X, que incluye 60 unidades, admite bandejas de expansión y utiliza controladoras E2800B.

    El SG6060 y SG606060X tienen las mismas especificaciones y funciones, a excepción de la ubicación de los puertos de interconexión en las controladoras de almacenamiento.

  - SGF6024, que ofrece 24 unidades de estado sólido (SSD).
- Integre los elementos de computación y almacenamiento para un nodo de almacenamiento de StorageGRID.
- Incluya el instalador de dispositivos StorageGRID para simplificar la puesta en marcha y la configuración del nodo de almacenamiento.
- Incluir System Manager de SANtricity para gestionar y supervisar las controladoras de almacenamiento y las unidades.
- Incluya una controladora de gestión en placa base (BMC) para supervisar y diagnosticar el hardware en la controladora de computación.
- Admite hasta cuatro conexiones de 10 GbE o 25 GbE a la red Grid y a la red cliente de StorageGRID.
- Admite unidades de estándar de procesamiento de información federal (FIPS). Cuando estas unidades se usan con la función Drive Security en SANtricity System Manager, se evita el acceso no autorizado a los datos.

Aparatos SG6060 y SG6060X

Los dispositivos SG6060 y SG606060X de StorageGRID incluyen una controladora de computación y una bandeja de controladoras de almacenamiento con dos controladoras de almacenamiento y 60 unidades. Opcionalmente, se pueden añadir bandejas de expansión de 60 unidades a ambos dispositivos. No existen diferencias funcionales ni de especificación entre el SG6060 y SG6060X, a excepción de la ubicación de los puertos de interconexión en el controlador de almacenamiento.

Componentes SG6060 y SG6060X

Los dispositivos SG6060 y SG660X incluyen los siguientes componentes:

Componente	Descripción
Controladora de computación	Controlador SG6000-CN, un servidor de unidad de un rack (1U) que incluye: • 40 núcleos (80 subprocesos) • 192 GB DE MEMORIA RAM • Hasta 4 × 25 Gbps de ancho de banda total de Ethernet • 4 × interconexión Fibre Channel (FC) de 16 Gbps • Controlador de administración en placa base (BMC) que simplifica la administración del hardware • Sistemas de alimentación redundantes

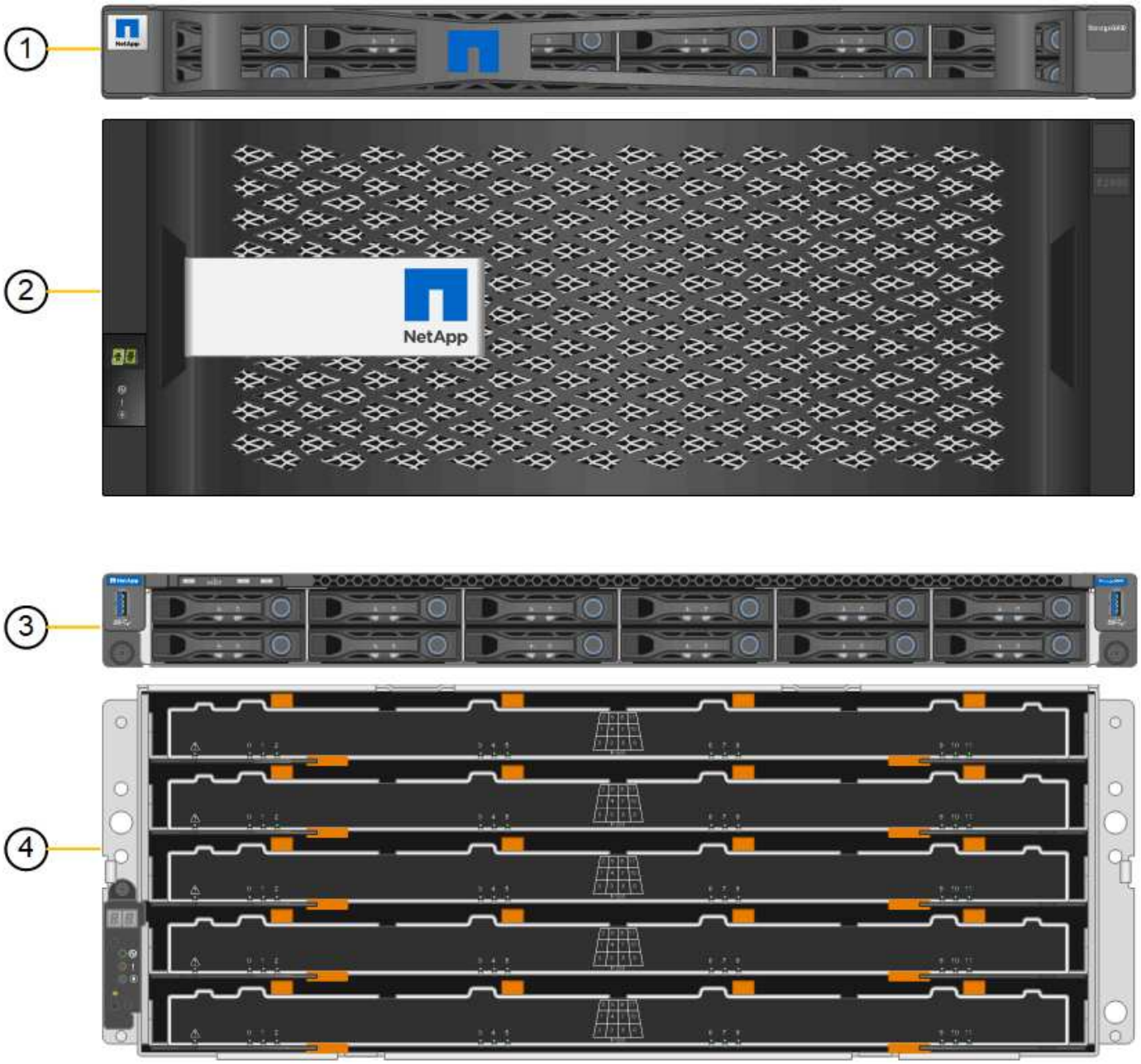
Bandeja de controladoras de almacenamiento	Bandeja de controladoras E-Series E2860 (cabina de almacenamiento), una bandeja 4U que incluye:
	• Dos controladoras serie E2800 (configuración doble) para proporcionar compatibilidad con conmutación al nodo de respaldo de una controladora de almacenamiento
	  ◦ El E2800SG6060 contiene controladoras de almacenamiento
	  ◦ El SG606060X contiene controladoras de almacenamiento E2800B
	• Bandeja de unidades de cinco cajones que aloja sesenta unidades de 3.5 pulgadas (2 unidades de estado sólido o SSD y 58 unidades NL-SAS)
	• Sistemas de alimentación y ventiladores redundantes

Opcional: Bandejas de ampliación del almacenamiento **Nota:** las bandejas de expansión se pueden instalar durante la implementación inicial o agregar más adelante.	Compartimento DE460C de E-Series, una bandeja de 4U que incluye: • Dos módulos de entrada/salida (IOM) • Cinco cajones, cada uno de ellos tiene 12 unidades NL-SAS, para un total de 60 unidades • Sistemas de alimentación y ventiladores redundantes Cada dispositivo SG6060 y SG606060X puede tener una o dos bandejas de expansión para un total de 180 unidades.

Diagramas SG6060 y 60X

Los frentes del SG6060 y del SG6060X son idénticos. En la siguiente figura, se muestra el frente de SG6060, que incluye una controladora de computación de 1U y una bandeja 4U que contiene dos controladoras de almacenamiento y 60 unidades en cinco cajones de unidades.

Vista frontal SG6060

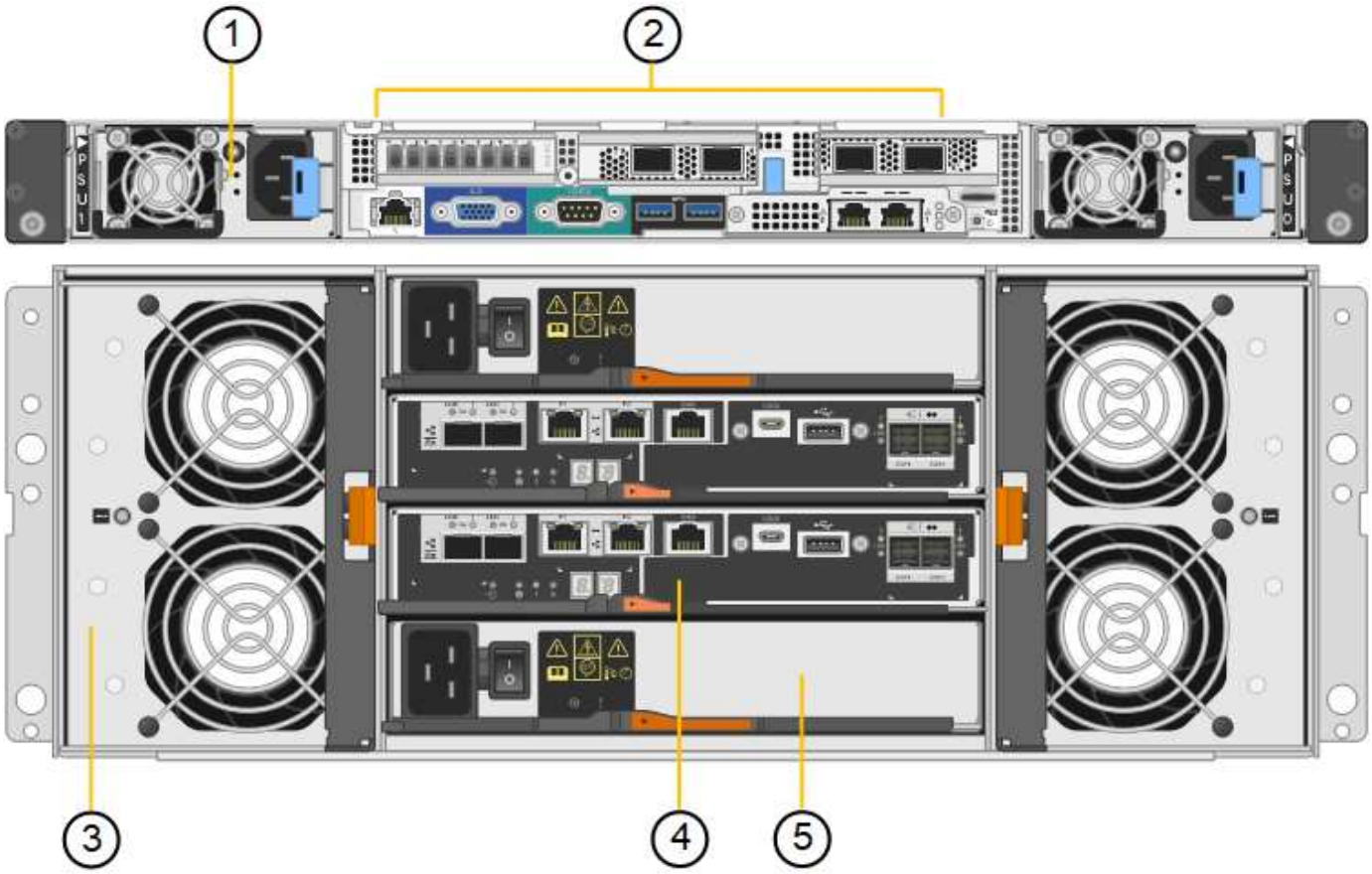


Llamada	Descripción
1	Controlador de computación SG6000-CN con marco frontal
2	Bandeja de controladoras E2860 con cubierta frontal (la bandeja de expansión opcional muestra idéntica)
3	Se ha eliminado el controlador informático SG6000-CN con marco frontal
4	Bandeja de controladoras E2860 con cubierta protectora frontal retirada (la bandeja de expansión opcional muestra idéntica)

Las siguientes figuras muestran la parte posterior de los sistemas SG6060 y SG6060X, incluidas las

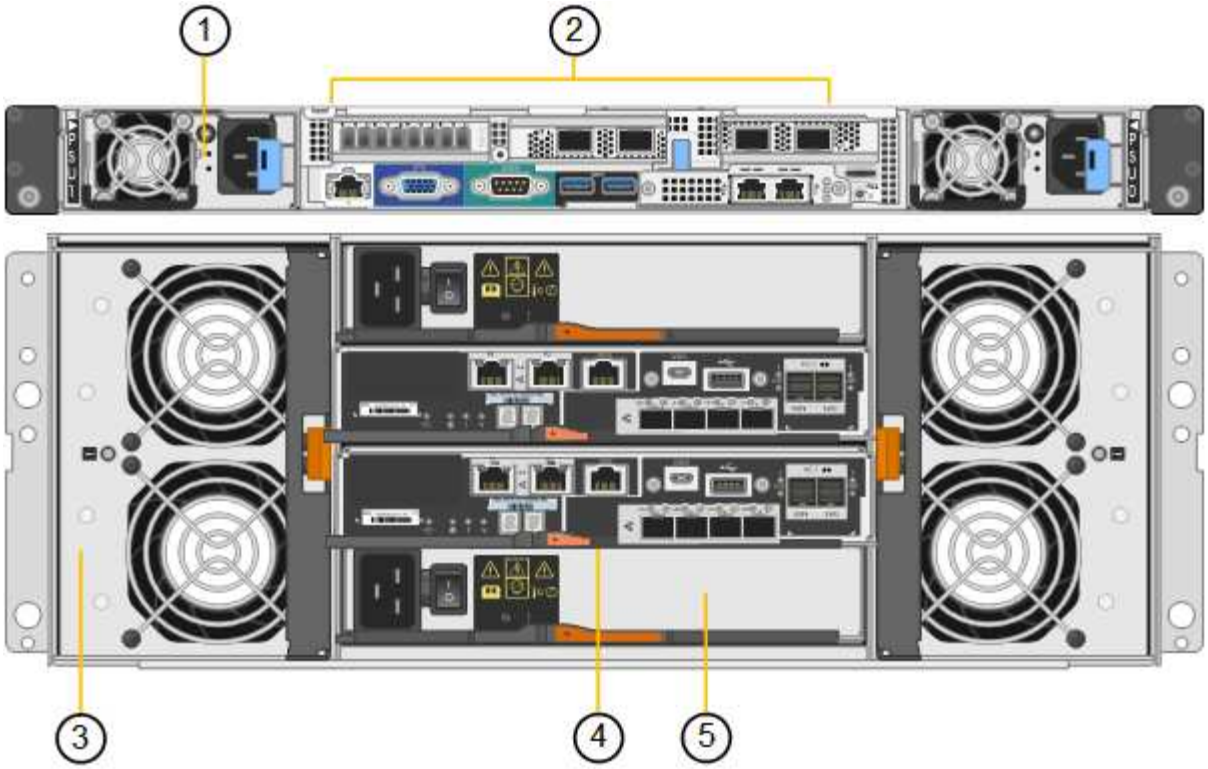
controladoras de computación y de almacenamiento, los ventiladores y los suministros de alimentación.

Vista posterior SG6060



Llamada	Descripción
1	Fuente de alimentación (1 de 2) para el controlador informático SG6000-CN
2	Conectores para el controlador de computación SG6000-CN
3	Ventilador (1 de 2) para bandeja de controladoras E2860
4	La controladora de almacenamiento E-Series E2800A (1 de 2) y sus conectores
5	Suministro de alimentación (1 de 2) para la bandeja de controladoras E2860

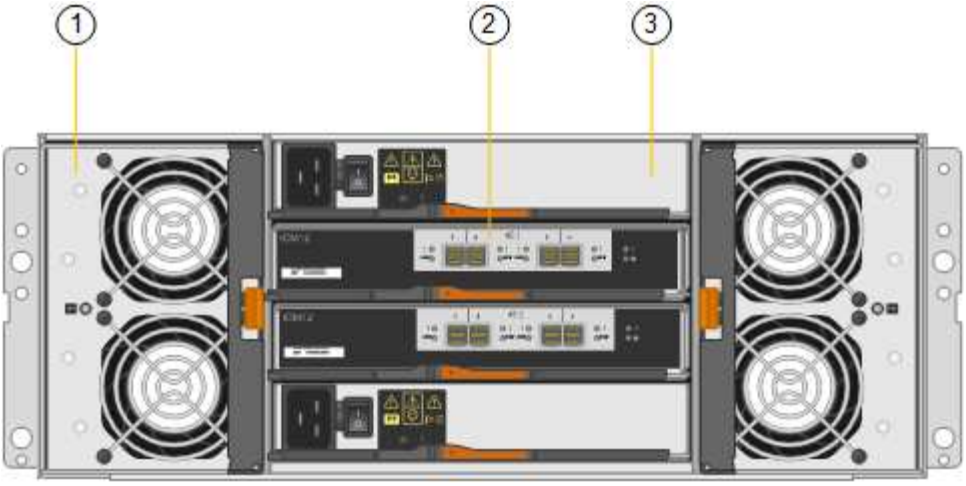
- SG6060X vista trasera*



Llamada	Descripción
1	Fuente de alimentación (1 de 2) para el controlador informático SG6000-CN
2	Conectores para el controlador de computación SG6000-CN
3	Ventilador (1 de 2) para bandeja de controladoras E2860
4	La controladora de almacenamiento E-Series E2800B (1 de 2) y sus conectores
5	Suministro de alimentación (1 de 2) para la bandeja de controladoras E2860

SG6060 y estante de expansión SG6060X

En esta figura, se muestra la parte posterior de la bandeja de expansión opcional para el SG6060 y SG6060X, incluidos los módulos de entrada/salida (IOM), los ventiladores y los suministros de alimentación. Cada SG6060 y SG6060X puede instalarse con una o dos bandejas de expansión, que pueden incluirse en la instalación inicial o añadirse posteriormente.



Llamada	Descripción
1	Ventilador (1 de 2) para estante de expansión
2	Iom (1 de 2) para la bandeja de expansión
3	Fuente de alimentación (1 de 2) para la bandeja de expansión

Descripción general de SGF6024

StorageGRIDSGF6024 incluye una controladora informático y una bandeja de controladoras de almacenamiento que tiene 24 unidades de estado sólido.

Componentes SGF6024

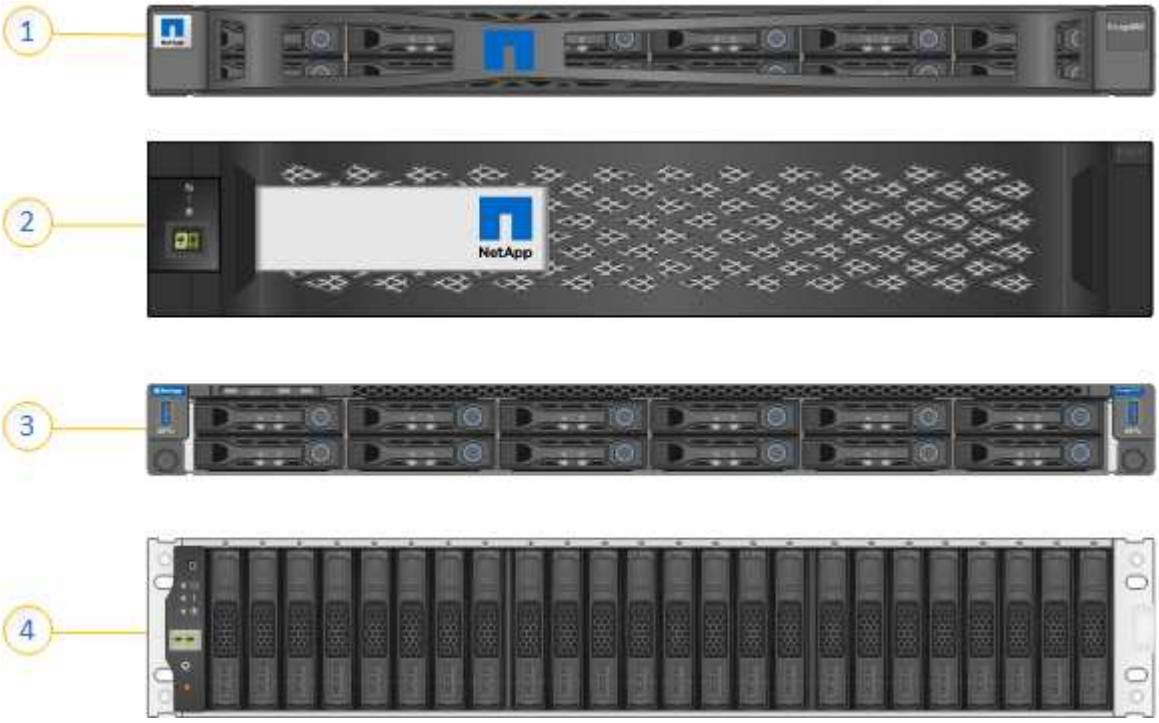
El aparato SGF6024 incluye los siguientes componentes:

Componente	Descripción
Controladora de computación	Controlador SG6000-CN, un servidor de unidad de un rack (1U) que incluye: • 40 núcleos (80 subprocesos) • 192 GB DE MEMORIA RAM • Hasta 4 × 25 Gbps de ancho de banda total de Ethernet • 4 × interconexión Fibre Channel (FC) de 16 Gbps • Controlador de administración en placa base (BMC) que simplifica la administración del hardware • Sistemas de alimentación redundantes

Componente	Descripción
Cabina flash (bandeja de controladora)	Cabina flash EF570 de E-Series (también conocida como bandeja de controladoras), una bandeja 2U que incluye: • Dos controladoras E-Series EF570 (configuración doble) para proporcionar compatibilidad con conmutación al nodo de respaldo de una controladora de almacenamiento • 24 unidades de estado sólido (también conocidas como unidades SSD o flash) • Sistemas de alimentación y ventiladores redundantes

Diagramas SGF6024

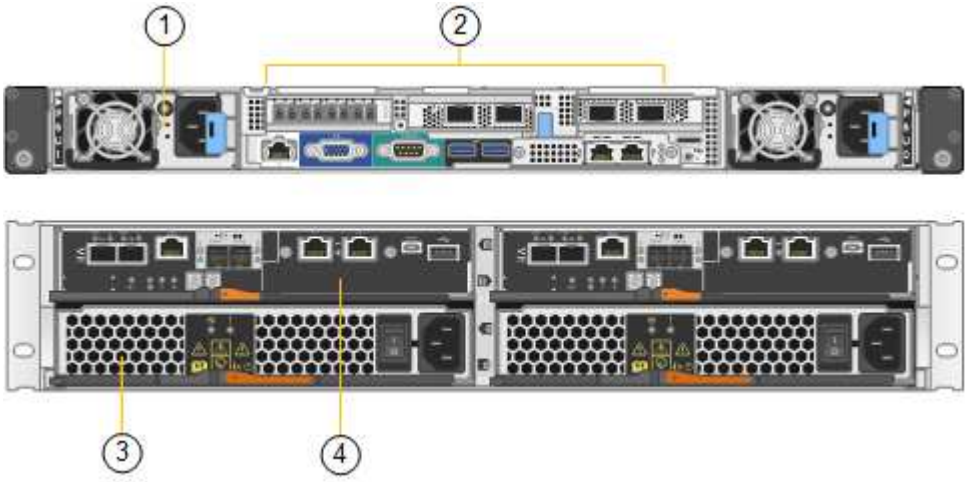
En esta figura, se muestra el frente del SGF6024, que incluye un controlador de computación 1U y un compartimento 2U con dos controladoras de almacenamiento y 24 unidades flash.



Llamada	Descripción
1	Controlador de computación SG6000-CN con marco frontal
2	Cabina flash EF570 con cubierta frontal
3	Se ha eliminado el controlador informático SG6000-CN con marco frontal

Llamada	Descripción
4	Se quitó la cabina flash EF570 con el bisel frontal

En esta figura, se muestra la parte posterior del SGF6024, incluidos los controladores de computación y almacenamiento, los ventiladores y los suministros de alimentación.



Llamada	Descripción
1	Fuente de alimentación (1 de 2) para el controlador informático SG6000-CN
2	Conectores para el controlador de computación SG6000-CN
3	Fuente de alimentación (1 de 2) para cabina flash EF570
4	La controladora de almacenamiento EF570 E-Series (1 de 2) y sus conectores

Controladoras en dispositivos SG6000

Cada modelo del dispositivo SG6000 de StorageGRID incluye un controlador de computación SG6000-CN en un compartimento 1U y controladoras de almacenamiento E-Series dúplex en una carcasa 2U o 4U, según el modelo. Revise los diagramas para obtener más información sobre cada tipo de controladora.

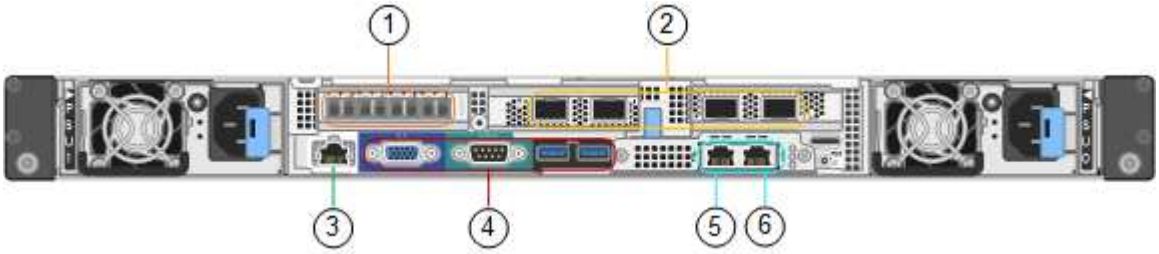
Todos los dispositivos: Controlador de computación SG6000-CN

- Proporciona recursos de computación para el dispositivo.
- Incluye el instalador de dispositivos StorageGRID.

> El software StorageGRID no está preinstalado en el dispositivo. Este software se recupera del nodo de administración cuando se implementa el dispositivo.

- Se puede conectar a las tres redes StorageGRID, incluidas la red de cuadrícula, la red de administración y la red de cliente.
- Se conecta a las controladoras de almacenamiento E-Series y funciona como iniciador.

Esta figura muestra los conectores de la parte posterior del SG6000-CN.



	Puerto	Tipo	Uso
1	Puertos de interconexión 1-4	Fibre Channel (FC) de 16 GB/s con óptica integrada	Conecte la controladora SG6000-CN a las controladoras E2800 (dos conexiones a cada E2800).
2	Puertos de red 1-4	10-GbE o 25-GbE, según el tipo de transceptor cable o SFP, la velocidad del switch y la velocidad de enlace configurada	Conéctese a la red de red y a la red de cliente para StorageGRID.
3	Puerto de gestión de BMC	1 GbE (RJ-45).	Conéctese al controlador de administración de la placa base SG6000-CN.
4	Puertos de diagnóstico y soporte	• VGA • Serie, 115200 8-N-1 • USB	Reservado para uso del soporte técnico.
5	Puerto de red de administrador 1	1 GbE (RJ-45).	Conecte el SG6000-CN a la red de administración para StorageGRID.

	Puerto	Tipo	Uso
6	Puerto de red de administrador 2	1 GbE (RJ-45).	Opciones: • Bond con el puerto de gestión 1 para una conexión redundante con la red de administrador para StorageGRID. • Deje sin cables y disponible para acceso local temporal (IP 169.254.0.1). • Durante la instalación, utilice el puerto 2 para la configuración de IP si las direcciones IP asignadas por DHCP no están disponibles.

SG6060 y SG606060X: Controladoras de almacenamiento de la serie E2800

- Dos controladoras para admitir conmutación al nodo de respaldo.
- Gestione el almacenamiento de datos en las unidades.
- Funcionan como controladoras E-Series estándar en una configuración doble.
- Incluya software de sistema operativo SANtricity (firmware de la controladora).
- Incluir System Manager de SANtricity para supervisar hardware de almacenamiento y gestionar alertas, la función AutoSupport y la función Drive Security.
- Conéctese al controlador SG6000-CN y proporcione acceso al almacenamiento.

El SG6060 y SG606060 utilizan controladoras de almacenamiento de la serie E2800.

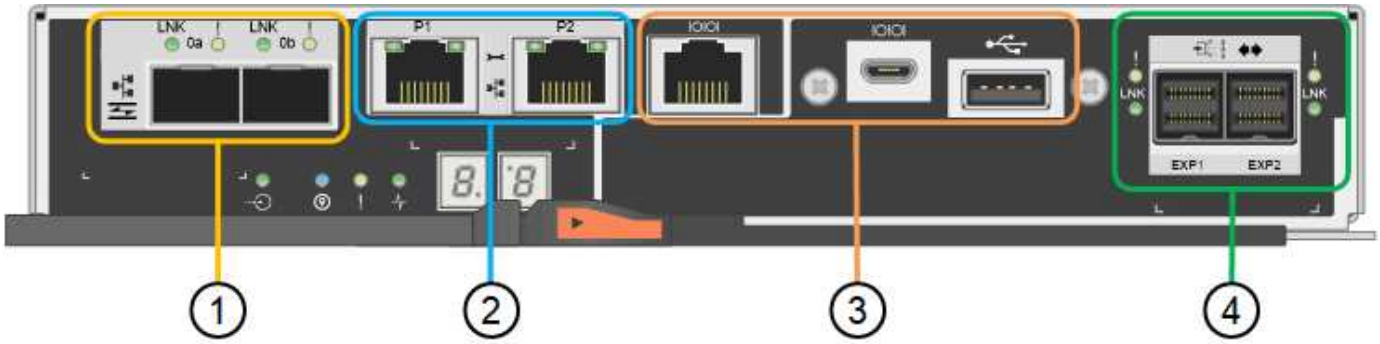
Dispositivo	Controladora
SG6060	Dos controladoras de almacenamiento E2800A
SG606060X	Dos controladoras de almacenamiento E2800B

El E2800A no tiene HIC, y el E2800B tiene una HIC de cuatro puertos. Las controladoras de almacenamiento E2800A y E2800B son idénticas en las especificaciones y funcionan excepto la ubicación de los puertos de interconexión.

No use E2800A y E2800B en el mismo dispositivo.

Las siguientes figuras muestran los conectores en la parte posterior de cada una de las controladoras de la serie E2800.

E2800A Storage Controller

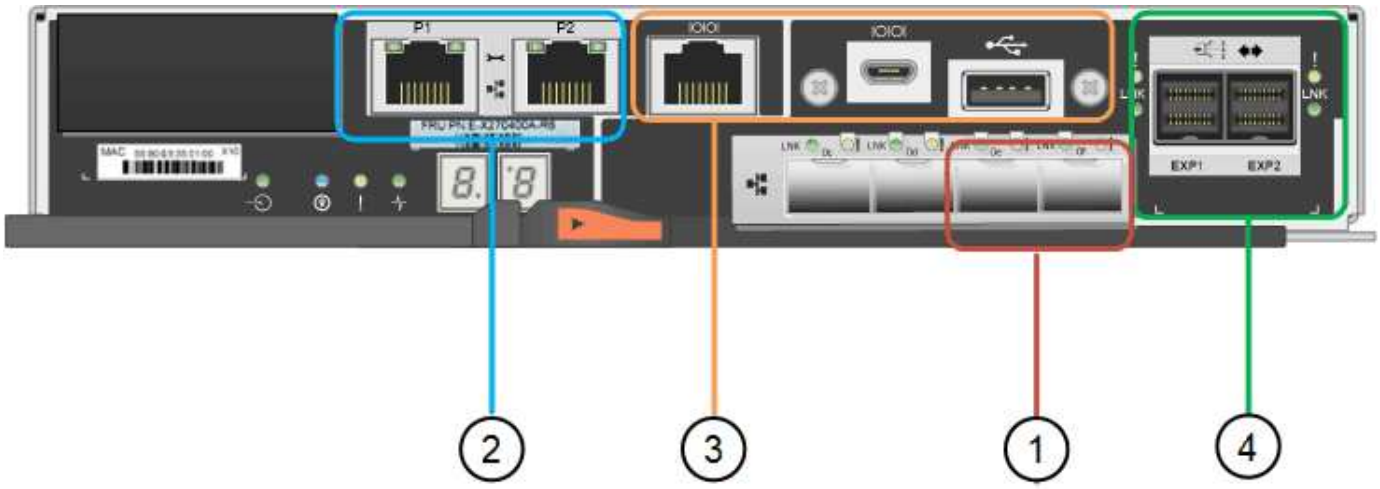


	Puerto	Tipo	Uso
1	Puertos de interconexión 1 y 2	SFPA óptico FC de 16 GB/s	Conecte cada uno de los controladores E2800A al controlador SG6000-CN. Hay cuatro conexiones al controlador SG6000-CN (dos de cada E2800A).

	Puerto	Tipo	Uso
2	Puertos de gestión 1 y 2	Ethernet de 1 GB (RJ-45)	• Opciones del puerto 1: ◦ Conéctese a una red de gestión para habilitar el acceso TCP/IP directo a System Manager de SANtricity ◦ Deje sin cables para guardar un puerto del switch y una dirección IP. Acceda a SANtricity System Manager usando las interfaces de usuario del instalador de Grid Manager o Storage Grid Appliance. **Nota**: Algunas funciones opcionales de SANtricity, como sincronización NTP para marcas de hora de registro precisas, no están disponibles cuando elige dejar el puerto 1 sin cable. **Nota**: Se requiere StorageGRID 11.5 o superior, y SANtricity 11.70 o superior, cuando salga del Puerto 1 sin cables. • El puerto 2 está reservado para uso del soporte técnico.
3	Puertos de diagnóstico y soporte	• Puerto serie RJ-45 • Puerto serie micro USB • Puerto USB	Reservado para uso del soporte técnico.

	Puerto	Tipo	Uso
4	Puertos de expansión de unidad 1 y 2	SAS de 12 GB/s	Conecte los puertos con los puertos de expansión de unidades en los IOM de la bandeja de expansión.

E2800B Storage Controller



	Puerto	Tipo	Uso
1	Puertos de interconexión 1 y 2	SFPA óptico FC de 16 GB/s	Conecte cada uno de los controladores E2800B al controlador SG6000-CN. Hay cuatro conexiones al controlador SG6000-CN (dos de cada E2800B).

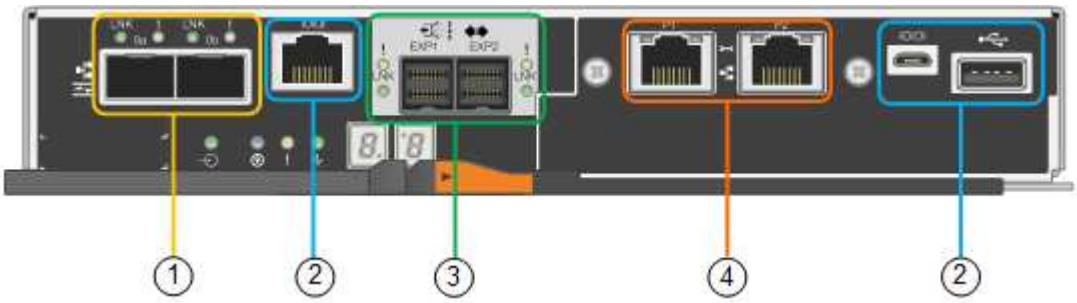
	Puerto	Tipo	Uso
2	Puertos de gestión 1 y 2	Ethernet de 1 GB (RJ-45)	• Opciones del puerto 1: ◦ Conéctese a una red de gestión para habilitar el acceso TCP/IP directo a System Manager de SANtricity ◦ Deje sin cables para guardar un puerto del switch y una dirección IP. Acceda a SANtricity System Manager usando las interfaces de usuario del instalador de Grid Manager o Storage Grid Appliance. **Nota**: Algunas funciones opcionales de SANtricity, como sincronización NTP para marcas de hora de registro precisas, no están disponibles cuando elige dejar el puerto 1 sin cable. **Nota**: Se requiere StorageGRID 11.5 o superior, y SANtricity 11.70 o superior, cuando salga del Puerto 1 sin cables. • El puerto 2 está reservado para uso del soporte técnico.
3	Puertos de diagnóstico y soporte	• Puerto serie RJ-45 • Puerto serie micro USB • Puerto USB	Reservado para uso del soporte técnico.

	Puerto	Tipo	Uso
4	Puertos de expansión de unidad 1 y 2	SAS de 12 GB/s	Conecte los puertos con los puertos de expansión de unidades en los IOM de la bandeja de expansión.

SGF6024: Controladores de almacenamiento EF570

- Dos controladoras para admitir conmutación al nodo de respaldo.
- Gestione el almacenamiento de datos en las unidades.
- Funcionan como controladoras E-Series estándar en una configuración doble.
- Incluya software de sistema operativo SANtricity (firmware de la controladora).
- Incluir System Manager de SANtricity para supervisar hardware de almacenamiento y gestionar alertas, la función AutoSupport y la función Drive Security.
- Conéctese al controlador SG6000-CN y proporcione acceso al almacenamiento flash.

En esta figura, se muestran los conectores de la parte posterior de cada una de las controladoras EF570.

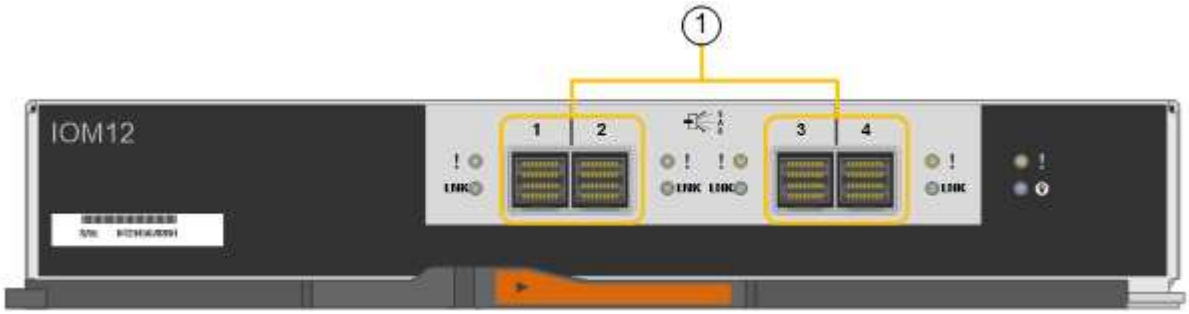


	Puerto	Tipo	Uso
1	Puertos de interconexión 1 y 2	SFPA óptico FC de 16 GB/s	Conecte cada una de las controladoras EF570 al controlador SG6000-CN. Existen cuatro conexiones al controlador SG6000-CN (dos de cada EF570).
2	Puertos de diagnóstico y soporte	• Puerto serie RJ-45 • Puerto serie micro USB • Puerto USB	Reservado para uso del soporte técnico.
3	Puertos de expansión de unidades	SAS de 12 GB/s	No se utiliza. El dispositivo SGF6024 no es compatible con bandejas de unidades de expansión.

	Puerto	Tipo	Uso
4	Puertos de gestión 1 y 2	Ethernet de 1 GB (RJ-45)	• El puerto 1 se conecta a la red en la que se accede a System Manager de SANtricity en un explorador. • El puerto 2 está reservado para uso del soporte técnico.

SG6060 y SG606060X: Módulos de entrada/salida para bandejas de expansión opcionales

La bandeja de expansión contiene dos módulos de I/o (IOM) que se conectan a las controladoras de almacenamiento o a otras bandejas de expansión.



	Puerto	Tipo	Uso
1	Puertos de expansión de unidades 1-4	SAS de 12 GB/s	Conecte cada puerto a las controladoras de almacenamiento o a la bandeja de expansión adicional (si la hubiera).

Información general sobre la instalación y la implementación

Puede instalar uno o varios dispositivos de almacenamiento StorageGRID cuando implemente StorageGRID por primera vez, o bien puede añadir nodos de almacenamiento del dispositivo más adelante como parte de una ampliación. Es posible que también se deba instalar un nodo de almacenamiento del dispositivo como parte de una operación de recuperación.

Lo que necesitará

El sistema StorageGRID está utilizando la versión necesaria del software StorageGRID.

Dispositivo	Versión de StorageGRID requerida
SG6060 y SG606060 sin bandejas de ampliación	11.1.1 o posterior

Dispositivo	Versión de StorageGRID requerida
SG6060 y SG6060X con bandejas de expansión (uno o dos)	11.3 o posterior **Nota:** Si agrega estantes de expansión después de la implementación inicial, debe utilizar la versión 11.4 o posterior.
SGF6024	11.3 o posterior

Tareas de instalación e implementación

Añadir un dispositivo de almacenamiento StorageGRID a un sistema StorageGRID incluye cuatro pasos principales:

1. Preparación de la instalación:
    - Preparación del sitio de instalación
    - Desembalaje de las cajas y comprobación del contenido
    - Obtención de equipos y herramientas adicionales
    - Recopilación de direcciones IP e información de red
    - Opcional: Configurar un servidor de gestión de claves (KMS) externo si planea cifrar todos los datos del dispositivo. Consulte detalles sobre la gestión de claves externas en las instrucciones para administrar StorageGRID.
2. Instalar el hardware:
    - Registrar el hardware
    - Instalación del dispositivo en un armario o rack
    - Instalar las unidades
    - Instalación de bandejas de expansión opcionales (solo en el modelo SG6060 y SG6060X; máximo de dos bandejas de expansión)
    - Cableado del aparato
    - Conexión de los cables de alimentación y alimentación
    - Ver los códigos de estado de inicio
3. Configurar el hardware:
    - Acceso a SANtricity System Manager para configurar los ajustes de SANtricity System Manager
    - Acceder al instalador de dispositivos StorageGRID, establecer una dirección IP estática para el puerto de administración 1 en la controladora de almacenamiento y configurar los ajustes de IP de enlace y red necesarios para conectarse a las redes StorageGRID
    - Acceso a la interfaz del controlador de administración de la placa base (BMC) en el controlador SG6000-CN
    - Opcional: Habilitar el cifrado de nodos si tiene previsto utilizar un KMS externo para cifrar los datos del dispositivo.
    - Opcional: Cambiar el modo RAID.
4. Poner en marcha el dispositivo como nodo de almacenamiento:

Tarea	Instrucciones
Poner en marcha un nodo de almacenamiento del dispositivo en un nuevo sistema StorageGRID	Ponga en marcha el nodo de almacenamiento del dispositivo
Añadir un nodo de almacenamiento del dispositivo a un sistema StorageGRID existente	Instrucciones para ampliar un sistema StorageGRID
Poner en marcha un nodo de almacenamiento del dispositivo como parte de una operación de recuperación de nodo de almacenamiento	Instrucciones para recuperación y mantenimiento

Información relacionada

Preparación de la instalación (SG6000)

Instalación del hardware (SG6000)

Configuración del hardware (SG6000)

Amplíe su grid

Recuperación y mantenimiento

Administre StorageGRID

Preparación de la instalación (SG6000)

Para preparar la instalación de un dispositivo StorageGRID es necesario preparar el sitio y obtener todo el hardware, cables y herramientas necesarios. También debe recopilar información sobre las direcciones IP y la red.

Información relacionada

Requisitos del navegador web

Sitio de preparación (SG6000)

Antes de instalar el dispositivo, debe asegurarse de que el sitio y el armario o rack que desee usar cumplan con las especificaciones de un dispositivo StorageGRID.

Pasos

1. Confirmar que el emplazamiento cumple los requisitos de temperatura, humedad, rango de altitud, flujo de aire, disipación de calor, cableado, alimentación y conexión a tierra. Si desea obtener más información, consulte Hardware Universe de NetApp.
2. Confirme que su ubicación ofrece una potencia de CA de 240 voltios para el SG6060 o una potencia de CA de 120 voltios para el SGF6024.
3. Obtenga un armario o rack de 19 pulgadas (48.3 cm) para colocar bandejas de este tamaño (sin cables):

Tipo de bandeja	Altura	Anchura	Profundidad	Peso máximo
Bandeja de controladores E2860 para SG6060	6.87 pda (17.46 cm)	17.66 pda (44.86 cm)	38.25 pda (97.16 cm)	250 lb. (113 kg)
Estante de expansión opcional para SG6060 (uno o dos)	6.87 pda (17.46 cm)	17.66 pda (44.86 cm)	38.25 pda (97.16 cm)	250 lb. (113 kg)
Estante del controlador EF570 para SGF6024	3.35 pda (8.50 cm)	17.66 pda (44.86 cm)	19.00 pda (48.26 cm)	51.74 lb. (23.47 kg)
Controlador SG6000-CN para cada aparato	1.70 pda (4.32 cm)	17.32 pda (44.0 cm)	32.0 pda (81.3 cm)	39 lb. (17.7 kg)

4. Decida dónde va a instalar el aparato.

Al instalar la bandeja de controladoras E2860 o las bandejas de expansión opcionales, instale el hardware desde la parte inferior hasta la parte superior del rack o armario para evitar que el equipo se vuelque. Para garantizar que el equipo más pesado se encuentra en la parte inferior del armario o bastidor, instale el controlador SG6000-CN encima de la bandeja de controladores E2860 y las bandejas de expansión.

Antes de realizar la instalación, compruebe que los cables ópticos de 0,5 m que se suministran con el aparato o los cables que suministra, tienen la longitud suficiente para el diseño planificado.

Información relacionada

"Hardware Universe de NetApp"

"Herramienta de matriz de interoperabilidad de NetApp"

Cajas de desembalaje (SG6000)

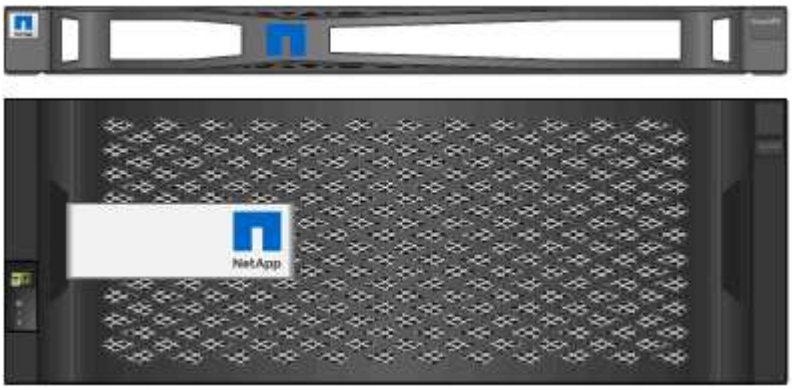
Antes de instalar el aparato StorageGRID, desembale todas las cajas y compare el contenido con los artículos del recibo de embalaje.

SG6060 y SG6060X

- **Controlador SG6000-CN**

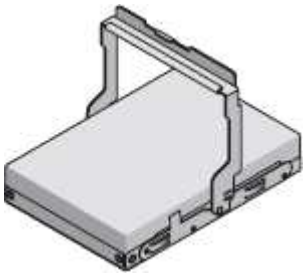
- **Bandeja de controladoras E2860 sin unidades instaladas**

- **Dos biseles delanteros**

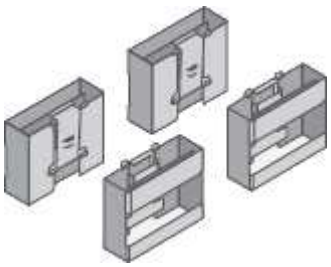


- **Dos kits de rieles con instrucciones**

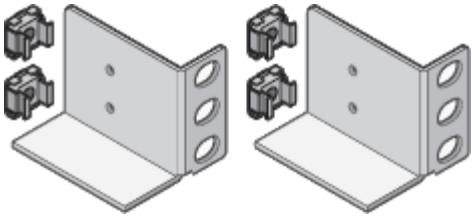
- **60 unidades (2 SSD y 58 NL-SAS)**



- **Cuatro asas**

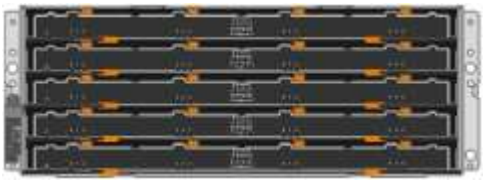


- **Soportes de fondo y tuercas de jaula para la instalación en bastidor de orificio cuadrado**



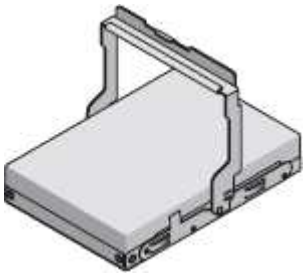
SG6060 y estante de expansión SG6060X

- **Bandeja de expansión sin unidades instaladas**



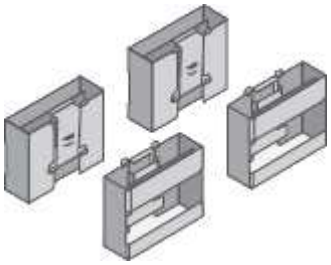
- **Bisel frontal**

- **60 unidades NL-SAS**

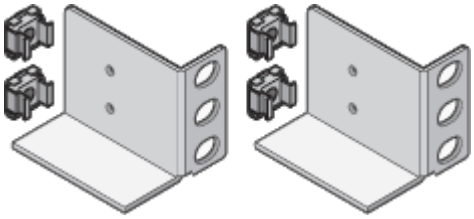


- **Un kit de rieles con instrucciones**

- **Cuatro asas**



- **Soportes de fondo y tuercas de jaula para la instalación en bastidor de orificio cuadrado**



SGF6024

- **Controlador SG6000-CN**

- **Matriz flash EF570 con 24 unidades de estado sólido (flash) instaladas**

- **Dos biseles delanteros**

- **Dos kits de rieles con instrucciones**

- **Tapas de estante**

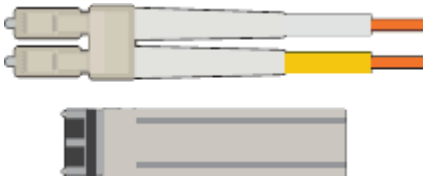
Cables y conectores

El envío del dispositivo StorageGRID incluye los siguientes cables y conectores:

- **Cuatro cables de alimentación para su país**

Es posible que el armario tenga cables de alimentación especiales que utilice en lugar de los cables de alimentación que se suministran con el aparato.

- **Cables ópticos y transceptores SFP**



Cuatro cables ópticos para los puertos de interconexión FC

Cuatro transceptores SFP+, que admiten FC de 16 GB/s.

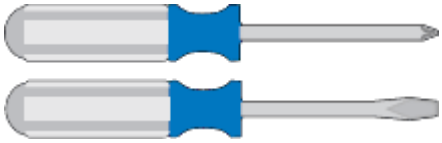
- **Opcional: Dos cables SAS para conectar cada estante de expansión SG6060 o SG6060X**

Obtener equipamiento y herramientas adicionales (SG6000)

Antes de instalar el aparato StorageGRID, confirme que dispone de todos los equipos y herramientas adicionales que necesita.

Necesitará el siguiente equipo adicional para instalar y configurar el hardware:

- **Destornilladores**

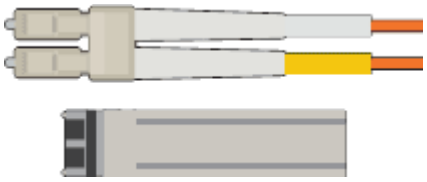


Phillips no 2 destornillador

Destornillador plano medio

- **Muñequera ESD**

- **Cables ópticos y transceptores SFP**



Se necesita una de las siguientes opciones:

  - De uno a cuatro cables Twinax o cables ópticos para los puertos 10/25-GbE que planea utilizar en el controlador SG6000-CN
  - Transceptores SFP+ de uno a cuatro para puertos 10/25-GbE si va a utilizar cables ópticos y velocidad de enlace 10-GbE
  - Transceptores SFP28 hasta cuatro puertos 10/25-GbE si utilizará cables ópticos y velocidad de enlace 25-GbE

- **Cables Ethernet RJ-45 (Cat5/Cat5e/Cat6)**

- **Portátil de servicio**

Navegador web compatible

Puerto 1-GbE (RJ-45)

- **Herramientas opcionales**

Taladro eléctrico con punta Phillips

Linterna

Elevación mecanizada para estantes de 60 unidades

Revisar las conexiones de red del dispositivo (SG6000)

Antes de instalar el dispositivo StorageGRID, debe saber qué redes se pueden conectar al dispositivo.

Al implementar un dispositivo de StorageGRID como nodo de almacenamiento en un sistema StorageGRID, puede conectarlo a las siguientes redes:

- **Red de Grid para StorageGRID**: 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. Se requiere la red de red.
- **Red de administración para StorageGRID**: La Red de administración es una red cerrada que se utiliza para la administración y el mantenimiento del sistema. La red de administración suele ser una red privada y no es necesario que se pueda enrutar entre sitios. La red administrativa es opcional.
- **Red de clientes para StorageGRID:** la red de clientes es una red abierta que se utiliza para proporcionar acceso a las aplicaciones cliente, incluidos S3 y Swift. La red de cliente proporciona acceso de protocolo de cliente a la cuadrícula, de modo que la red de red de red pueda aislarse y protegerse. La red cliente es opcional.
- **Red de administración para el Administrador del sistema SANtricity** (opcional): Esta red proporciona acceso al Administrador del sistema SANtricity en la controladora de almacenamiento, lo que le permite supervisar y gestionar los componentes de hardware en la bandeja de la controladora de almacenamiento. Esta red de gestión puede ser la misma que la Red de administración para StorageGRID, o bien puede ser una red de gestión independiente.

  Si la red opcional de SANtricity System Manager no está conectada, es posible que no pueda utilizar algunas funciones SANtricity.

- **Red de administración de BMC para el controlador SG6000-CN** (opcional): Esta red proporciona acceso al controlador de administración de la placa base en el SG6000-CN, lo que le permite supervisar y gestionar los componentes de hardware en el controlador SG6000-CN. Esta red de gestión puede ser la misma que la Red de administración para StorageGRID, o bien puede ser una red de gestión independiente.

  Si la red de administración opcional de BMC no está conectada, será más difícil realizar algunos procedimientos de soporte y mantenimiento. Puede dejar la red de gestión de BMC sin conexión excepto cuando sea necesario para fines de soporte.

Para obtener información detallada acerca de las redes StorageGRID, consulte *Grid primer*.

Información relacionada

Recopilar información de instalación (SG6000)

Aparato de cable (SG6000)

Modos de enlace de puertos para el controlador SG6000-CN

Directrices de red

Modos de enlace de puertos para el controlador SG6000-CN

Al configurar los enlaces de red para SG6000-CN, puede utilizar el enlace de puertos para los puertos 10/25-GbE que se conectan a la red Grid y a la red de cliente opcional,

así como los puertos de gestión de 1-GbE que se conectan a la red de administración opcional. El enlace de puertos ayuda a proteger los datos proporcionando rutas redundantes entre las redes StorageGRID y el dispositivo.

Información relacionada

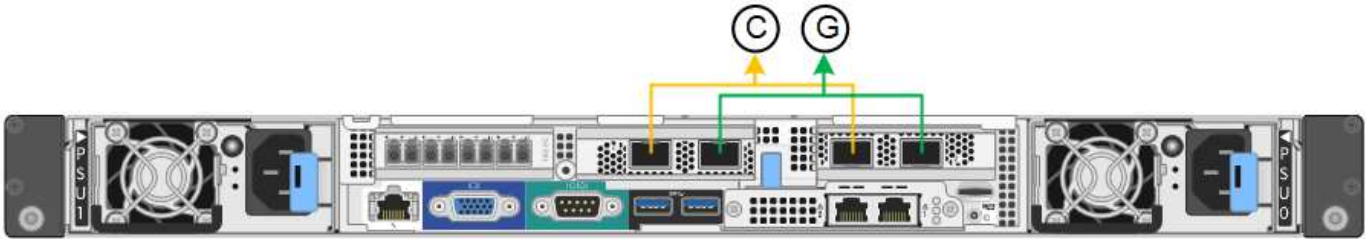
Configuración de enlaces de red (SG6000)

Modos de enlace de red para puertos 10/25-GbE

Los puertos de red de 10/25 GbE del controlador SG6000-CN admiten el modo de enlace de puerto fijo o el modo de enlace de puerto agregado para las conexiones de red de red de Grid y de red de cliente.

Modo de enlace de puerto fijo

El modo fijo es la configuración predeterminada para los puertos de red de 10/25-GbE.



Llamada	Qué puertos están Unidos
C	Los puertos 1 y 3 se unen para la red cliente, si se utiliza esta red.
G	Los puertos 2 y 4 están Unidos para la red de cuadrícula.

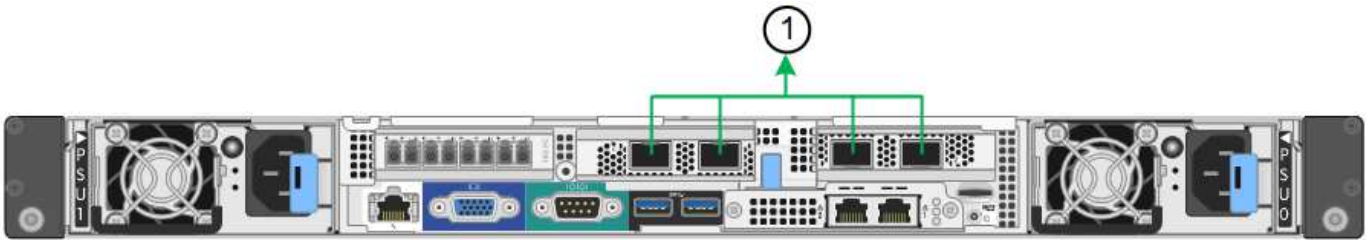
Cuando se utiliza el modo de enlace de puerto fijo, los puertos se pueden enlazar mediante el modo de copia de seguridad activa o el modo de protocolo de control de agregación de enlaces (LACP 802.3ad).

- En el modo activo-backup (predeterminado), solo hay un puerto activo a la vez. Si se produce un error en el puerto activo, su puerto de backup proporciona automáticamente una conexión de conmutación por error. El puerto 4 proporciona una ruta de copia de seguridad para el puerto 2 (red de red de cuadrícula) y el puerto 3 proporciona una ruta de copia de seguridad para el puerto 1 (red de cliente).
- En el modo LACP, cada par de puertos forma un canal lógico entre la controladora y la red, lo que permite un mayor rendimiento. Si un puerto falla, el otro continúa proporcionando el canal. El rendimiento se reduce, pero la conectividad no se ve afectada.

> Si no necesita conexiones redundantes, sólo puede utilizar un puerto para cada red. No obstante, tenga en cuenta que se activará una alerta en el Administrador de grid después de instalar StorageGRID, lo que indica que el enlace está inactivo. Dado que este puerto está desconectado por propósito, puede deshabilitar esta alerta de forma segura. En Grid Manager, seleccione **Alerta Reglas**, seleccione la regla y haga clic en **Editar regla**. A continuación, desactive la casilla de verificación **Activado**.

Modo de enlace de puerto agregado

El modo de enlace de puerto de agregado aumenta de forma significativa las mejoras en cada red StorageGRID y proporciona rutas de conmutación al nodo de respaldo adicionales.



Llamada	Qué puertos están Unidos
1	Todos los puertos conectados se agrupan en un único enlace LACP, lo que permite que todos los puertos se usen para el tráfico de red de grid y de red de cliente.

Si tiene pensado utilizar el modo de enlace de puerto agregado:

- Debe usar el modo de enlace de red LACP.
- Debe especificar una etiqueta de VLAN exclusiva para cada red. Esta etiqueta VLAN se añadirá a cada paquete de red para garantizar que el tráfico de red se dirija a la red correcta.
- Los puertos deben estar conectados a switches que sean compatibles con VLAN y LACP. Si varios switches participan en el enlace LACP, los switches deben ser compatibles con los grupos de agregación de enlaces de varios chasis (MLAG), o equivalentes.
- Debe comprender cómo configurar los switches para que utilicen VLAN, LACP y MLAG, o equivalente.

Si no desea usar los cuatro puertos 10/25-GbE, puede usar uno, dos o tres puertos. El uso de más de un puerto maximiza la posibilidad de que cierta conectividad de red permanezca disponible si falla uno de los puertos 10/25-GbE.

> Si decide utilizar menos de cuatro puertos, tenga en cuenta que puede activarse una alerta * de enlace de dispositivo de servicios* en Grid Manager después de instalar el nodo del dispositivo, lo que indica que se ha desenchufado un cable. Puede deshabilitar con seguridad esta regla de alerta para la alerta activada. En Grid Manager, seleccione **ALERTS** > **Reglas**, seleccione la regla y haga clic en **Editar regla**. A continuación, desactive la casilla de verificación **Activado**.

Modos de enlace de red para puertos de gestión de 1 GbE

Para los dos puertos de gestión de 1 GbE del controlador SG6000-CN, puede elegir el modo de enlace de red independiente o el modo de enlace de red Active-Backup para conectarse a la red de administración opcional.

En modo independiente, solo el puerto de gestión de la izquierda está conectado a la red del administrador. Este modo no proporciona una ruta de acceso redundante. El puerto de gestión de la derecha no está conectado y está disponible para conexiones locales temporales (utiliza la dirección IP 169.254.0.1)

En el modo Active-Backup, ambos puertos de gestión están conectados a la red Admin. Solo hay un puerto activo a la vez. Si se produce un error en el puerto activo, su puerto de backup proporciona automáticamente una conexión de conmutación por error. La vinculación de estos dos puertos físicos en un puerto de gestión

lógica proporciona una ruta redundante a la red de administración.

> Si necesita realizar una conexión local temporal al controlador SG6000-CN cuando los puertos de gestión de 1 GbE están configurados para el modo Active-Backup, retire los cables de ambos puertos de gestión, conecte el cable temporal al puerto de gestión de la derecha y acceda al dispositivo con la dirección IP 169.254.0.1.

Llamada	Modo de enlace de red
A.	Ambos puertos de gestión están Unidos en un puerto de gestión lógico conectado a la red administrativa.
YO	El puerto de la izquierda está conectado a la red de administración. El puerto de la derecha está disponible para conexiones locales temporales (dirección IP 169.254.0.1).

Recopilar información de instalación (SG6000)

Al instalar y configurar el dispositivo StorageGRID, debe tomar decisiones y recopilar información acerca de los puertos del switch Ethernet, las direcciones IP y los modos de enlace de puerto y red.

Acerca de esta tarea

Puede utilizar las siguientes tablas para registrar la información necesaria para cada red que conecte al dispositivo. Estos valores son necesarios para instalar y configurar el hardware.

La información necesaria para conectarse con System Manager de SANtricity en controladoras de almacenamiento

Debe conectar las dos controladoras de almacenamiento del dispositivo (tanto las controladoras serie E2800 como las controladoras EF570) a la red de gestión que se usará para SANtricity System Manager. Los controladores se encuentran en cada dispositivo de la siguiente manera:

- SG6060 y SG606060X: El controlador A está en la parte superior y el controlador B en la parte inferior.
- SGF6024: El controlador A está a la izquierda y el controlador B a la derecha.

Información necesaria	Su valor para la controladora A	Su valor para la controladora B.
Puerto del switch Ethernet se conectará al puerto de gestión 1 (etiquetado como P1 en la controladora E2800A y 0a en la controladora E2800B)		

Información necesaria	Su valor para la controladora A	Su valor para la controladora B.
Dirección MAC para el puerto de gestión 1 (impreso en una etiqueta cerca del puerto P1 en la controladora E2800A y 0a en la controladora E2800B)		
Dirección IP asignada por DHCP para el puerto de gestión 1, si está disponible después de encenderse **Nota:** Si la red que va a conectar al controlador de almacenamiento incluye un servidor DHCP, el administrador de red puede utilizar la dirección MAC para determinar la dirección IP asignada por el servidor DHCP.		
Dirección IP estática que planea usar para el dispositivo en la red de gestión	Para IPv4: • Dirección IPv4: • Máscara de subred: • Puerta de enlace: Para IPv6: • Dirección IPv6: • Dirección IP enrutable: • Dirección IP del enrutador de la controladora de almacenamiento:	Para IPv4: • Dirección IPv4: • Máscara de subred: • Puerta de enlace: Para IPv6: • Dirección IPv6: • Dirección IP enrutable: • Dirección IP del enrutador de la controladora de almacenamiento:
Formato de dirección IP	Elija una opción: • IPv4 • IPv6	Elija una opción: • IPv4 • IPv6
Velocidad y modo doble **Nota:** debe asegurarse de que el conmutador Ethernet de la red de administración de SANtricity System Manager está establecido en Negotiate automático.	Debe ser: • Autonegociar (predeterminado)	Debe ser: • Autonegociar (predeterminado)

Información necesaria para conectar el controlador SG6000-CN a la red Admin

La red de administración de StorageGRID es una red opcional que se utiliza para la administración y el

mantenimiento del sistema. El dispositivo se conecta a la red Admin mediante los siguientes puertos de gestión de 1 GbE en el controlador SG6000-CN.

Información necesaria	Su valor
Red de administrador habilitada	Elija una opción: • No • Sí (predeterminado)
Modo de enlace de red	Elija una opción: • Independiente (predeterminado) • Copia de seguridad activa
Puerto de switch para el puerto izquierdo en el círculo rojo del diagrama (puerto activo predeterminado para el modo de enlace de red independiente)	
Puerto de switch para el puerto derecho en el círculo rojo del diagrama (sólo modo de enlace de red Active-Backup)	
Dirección MAC del puerto de red de administración **Nota:** la etiqueta de dirección MAC situada en la parte frontal del controlador SG6000-CN enumera la dirección MAC del puerto de administración del BMC. Para determinar la dirección MAC del puerto de red de administración, debe agregar **2** al número hexadecimal de la etiqueta. Por ejemplo, si la dirección MAC de la etiqueta termina en **09**, la dirección MAC del puerto de administración finalizará en **0B**. Si la dirección MAC de la etiqueta termina en **(*y*)FF**, la dirección MAC del puerto de administración finalizará en **(*y*+1)01**. Puede realizar este cálculo fácilmente abriendo Calculadora en Windows, establecerlo en modo Programador, seleccionando hex, escribiendo la dirección MAC y, a continuación, escribiendo **+ 2 =**.	

Información necesaria	Su valor
Dirección IP asignada por DHCP para el puerto de red de administración, si está disponible después del encendido **Nota:** puede determinar la dirección IP asignada por DHCP utilizando la dirección MAC para buscar la dirección IP asignada.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Dirección IP estática que piensa usar para el nodo de almacenamiento del dispositivo en la red de administración **Nota:** Si su red no tiene una puerta de enlace, especifique la misma dirección IPv4 estática para la puerta de enlace.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Subredes de red de administración (CIDR)	

Información necesaria para conectar y configurar puertos 10/25-GbE en el controlador SG6000-CN

Los cuatro puertos 10/25-GbE del controlador SG6000-CN se conectan a la red de red StorageGRID y a la red de cliente opcional.

Información necesaria	Su valor
Velocidad de enlace	Elija una opción: • Automático (predeterminado) • 10 GbE • 25 GbE
Modo de enlace de puerto	Elija una opción: • Fijo (predeterminado) • Agregado
Puerto de conmutador para el puerto 1 (red cliente para modo fijo)	
Puerto de conmutador para el puerto 2 (red de cuadrícula para modo fijo)	
Puerto de conmutador para el puerto 3 (red cliente para modo fijo)	
Puerto de conmutador para el puerto 4 (red de cuadrícula para modo fijo)	

Información necesaria para conectar el controlador SG6000-CN a la red Grid

Grid Network para StorageGRID es una red necesaria que se utiliza para todo el tráfico interno de StorageGRID. El dispositivo se conecta a la red Grid mediante los puertos 10/25-GbE del controlador SG6000-CN.

Información necesaria	Su valor
Modo de enlace de red	Elija una opción: • Active-Backup (predeterminado) • LACP (802.3ad)
Etiquetado VLAN habilitado	Elija una opción: • No (predeterminado) • Sí
Etiqueta de VLAN (si el etiquetado de VLAN está habilitado)	Introduzca un valor entre 0 y 4095:
Dirección IP asignada por DHCP para la red de cuadrícula, si está disponible después del encendido	• Dirección IPv4 (CIDR): • Puerta de enlace:
Dirección IP estática que tiene previsto usar para el nodo de almacenamiento del dispositivo en la red de grid **Nota:** Si su red no tiene una puerta de enlace, especifique la misma dirección IPv4 estática para la puerta de enlace.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Subredes de red de cuadrícula (CIDR)	

Información necesaria para conectar el controlador SG6000-CN a la red cliente

La red de cliente para StorageGRID es una red opcional que se suele utilizar para proporcionar acceso al protocolo de cliente al grid. El dispositivo se conecta a la red cliente mediante los puertos 10/25-GbE del controlador SG6000-CN.

Información necesaria	Su valor
Red de cliente habilitada	Elija una opción: • No (predeterminado) • Sí

Información necesaria	Su valor
Modo de enlace de red	Elija una opción: • Active-Backup (predeterminado) • LACP (802.3ad)
Etiquetado VLAN habilitado	Elija una opción: • No (predeterminado) • Sí
Etiqueta de VLAN (si el etiquetado de VLAN está habilitado)	Introduzca un valor entre 0 y 4095:
Dirección IP asignada por DHCP para la red cliente, si está disponible después del encendido	• Dirección IPv4 (CIDR): • Puerta de enlace:
Dirección IP estática que tiene previsto usar para el nodo de almacenamiento del dispositivo en la red cliente **Nota:** Si la red de cliente está activada, la ruta predeterminada del controlador utilizará la puerta de enlace especificada aquí.	• Dirección IPv4 (CIDR): • Puerta de enlace:

Información necesaria para conectar el controlador SG6000-CN a la red de gestión BMC

Puede acceder a la interfaz del BMC en el controlador SG6000-CN utilizando el siguiente puerto de gestión de 1 GbE. Este puerto admite la gestión remota del hardware de la controladora a través de Ethernet mediante el estándar de interfaz de gestión de plataforma inteligente (IPMI).

Información necesaria	Su valor
Puerto del switch Ethernet se conectará al puerto de administración del BMC (con un círculo en el diagrama)	
Dirección IP asignada por DHCP para la red de gestión de BMC, si está disponible después del encendido	• Dirección IPv4 (CIDR): • Puerta de enlace:
La dirección IP estática que planea usar para el puerto de gestión de BMC	• Dirección IPv4 (CIDR): • Puerta de enlace:

Información relacionada

Controladoras en dispositivos SG6000

Revisar las conexiones de red del dispositivo (SG6000)

Modos de enlace de puertos para el controlador SG6000-CN

Aparato de cable (SG6000)

Configure las direcciones IP de StorageGRID

Instalación del hardware (SG6000)

La instalación del hardware implica la instalación del controlador SG6000-CN y la bandeja del controlador de almacenamiento en un armario o rack, la conexión de los cables y la alimentación.

Registre el hardware

El registro del hardware del dispositivo proporciona ventajas de asistencia.

Pasos

1. Localice el número de serie del chasis para la bandeja de la controladora de almacenamiento.

   Puede encontrar el número en el recibo de embalaje, en el correo electrónico de confirmación o en el aparato después de desembalarlo.

   > El dispositivo de almacenamiento tiene varios números de serie. El número de serie de la bandeja de controladoras de almacenamiento es el que debe registrarse y utilizarse si llama al servicio o al soporte de la aplicación.

2. Vaya al sitio de soporte de NetApp en "mysupport.netapp.com".
3. Determine si necesita registrar el hardware:

Si usted es un…	Siga estos pasos…
Cliente existente de NetApp	a. Inicie sesión con su nombre de usuario y contraseña. b. Seleccione **Productos** > **Mis productos**. c. Confirme que el nuevo número de serie aparece en la lista. d. De lo contrario, siga las instrucciones para nuevos clientes de NetApp.

Si usted es un…	Siga estos pasos…
Nuevo cliente de NetApp	a. Haga clic en **Registrar ahora** y cree una cuenta. b. Seleccione **Productos** > **Registrar productos**. c. Introduzca el número de serie del producto y los detalles solicitados. Una vez aprobado el registro, puede descargar el software necesario. El proceso de aprobación puede llevar hasta 24 horas.

SG6060 y SG606060X: Instale bandejas de 60 unidades en el armario o rack

Debe instalar un conjunto de rieles para la bandeja de controladoras E2860 en su armario o rack y, a continuación, deslizar la bandeja de controladoras sobre los rieles. Si va a instalar bandejas de expansión de 60 unidades, aplica el mismo procedimiento.

Lo que necesitará

- Ha revisado el documento de avisos de seguridad que se incluye en la caja y comprende las precauciones para mover e instalar el hardware.
- Tiene las instrucciones incluidas en el kit de raíl.

Cada bandeja de 60 unidades pesa aproximadamente 132 lb (60 kg) sin unidades instaladas. Se necesitan cuatro personas o un elevador mecánico para mover el estante de forma segura.

Para evitar que se dañe el hardware, no mueva nunca la bandeja si hay unidades instaladas. Debe quitar todas las unidades antes de mover la bandeja.

Al instalar la bandeja de controladoras E2860 o las bandejas de expansión opcionales, instale el hardware desde la parte inferior hasta la parte superior del rack o armario para evitar que el equipo se vuelque. Para garantizar que el equipo más pesado se encuentra en la parte inferior del armario o bastidor, instale el controlador SG6000-CN encima de la bandeja de controladores E2860 y las bandejas de expansión.

Antes de realizar la instalación, compruebe que los cables ópticos de 0,5 m que se suministran con el aparato o los cables que suministra, tienen la longitud suficiente para el diseño planificado.

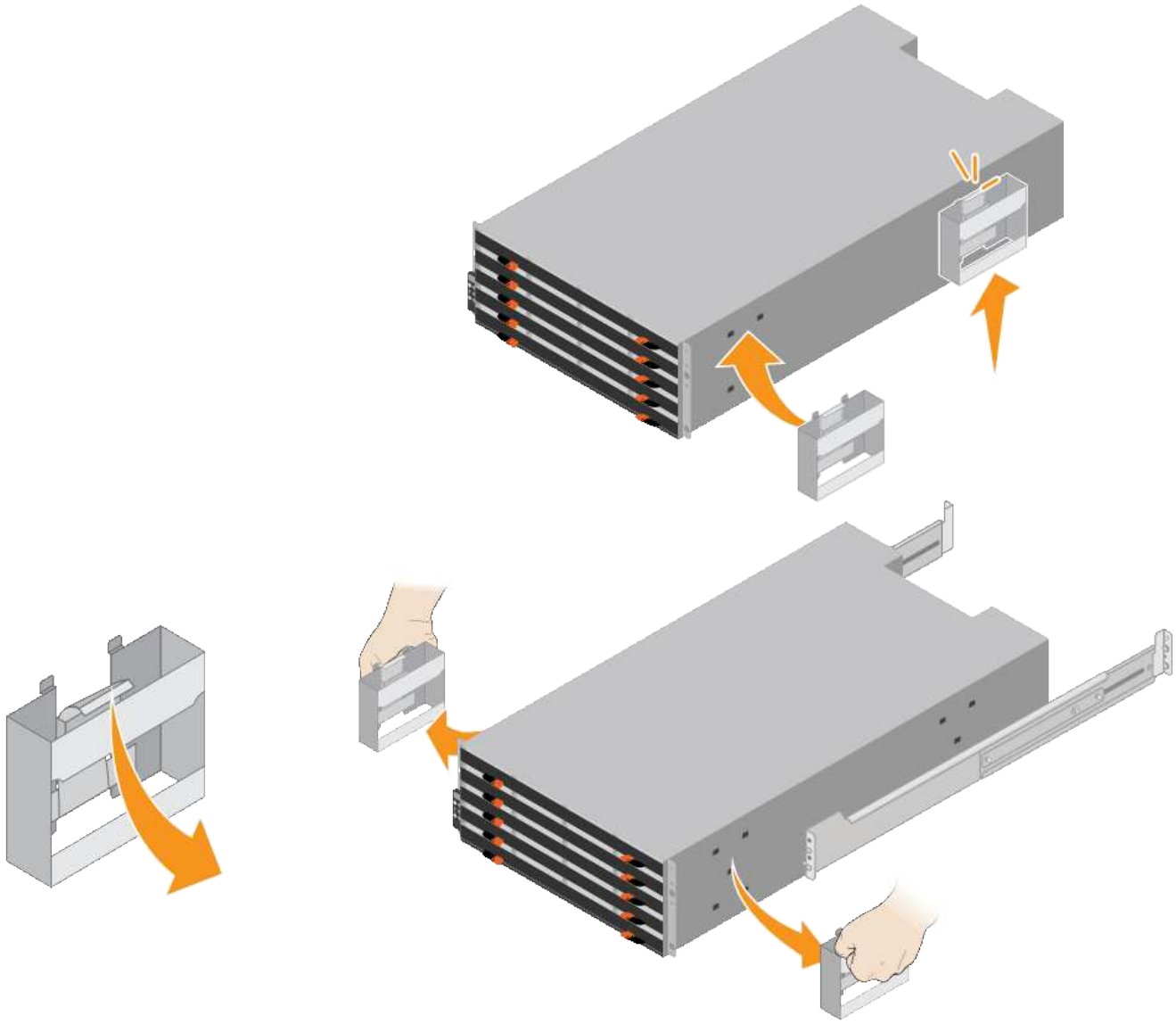
Pasos

1. Siga con cuidado las instrucciones del kit de raíl para instalar los rieles en su armario o rack.

   En el caso de armarios con orificios cuadrados, primero debe instalar las tuercas de jaula proporcionadas para asegurar la parte delantera y trasera de la estantería con tornillos.

2. Retire la caja de embalaje exterior del aparato. A continuación, pliegue las solapas de la caja interior.
3. Si está levantando el aparato a mano, fije las cuatro asas a los lados del chasis.

Empuje cada asa hasta que encaje en su sitio.



4. Coloque la parte posterior de la bandeja (el extremo con los conectores) en los rieles.
5. Apoye la estantería desde la parte inferior y deslícela en el armario. Si está utilizando las asas, utilice los cierres para separar un asa a la vez mientras desliza el estante en.

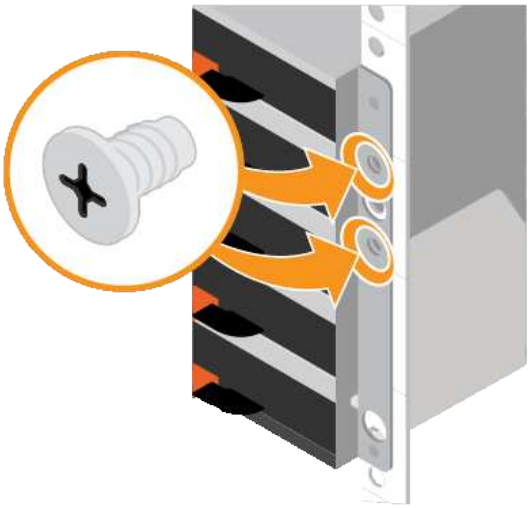
   Para quitar las asas, tire hacia atrás del pestillo de liberación, empuje hacia abajo y tire hacia fuera de la bandeja.

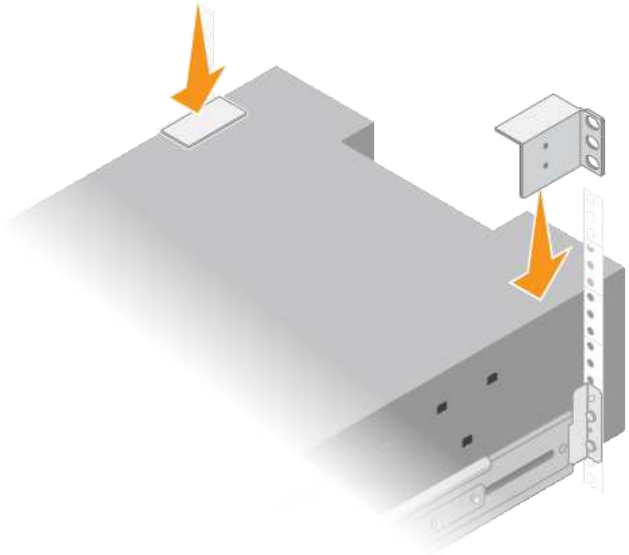
6. Fije la bandeja a la parte frontal del armario.

   Inserte los tornillos en el primer y tercer orificio de la parte superior de la bandeja en ambos lados.

7. Fije la bandeja a la parte posterior del armario.

   Coloque dos soportes traseros a cada lado de la parte superior trasera del estante. Inserte los tornillos en el primer y tercer orificio de cada soporte.





8. Repita estos pasos para todas las bandejas de ampliación.

SG6060 y SG6060X: Instalación de las unidades

Después de instalar la bandeja de 60 unidades en un armario o rack, debe instalar las 60 unidades en la bandeja. El envío para la bandeja de controladoras E2860 incluye dos unidades SSD, que debe instalarse en el cajón superior de la bandeja de controladoras. Cada bandeja de expansión opcional incluye 60 unidades de disco duro y sin unidades SSD.

Lo que necesitará

Instaló la bandeja de controladoras E2860 o bandejas de expansión opcionales (uno o dos) en el armario o rack.

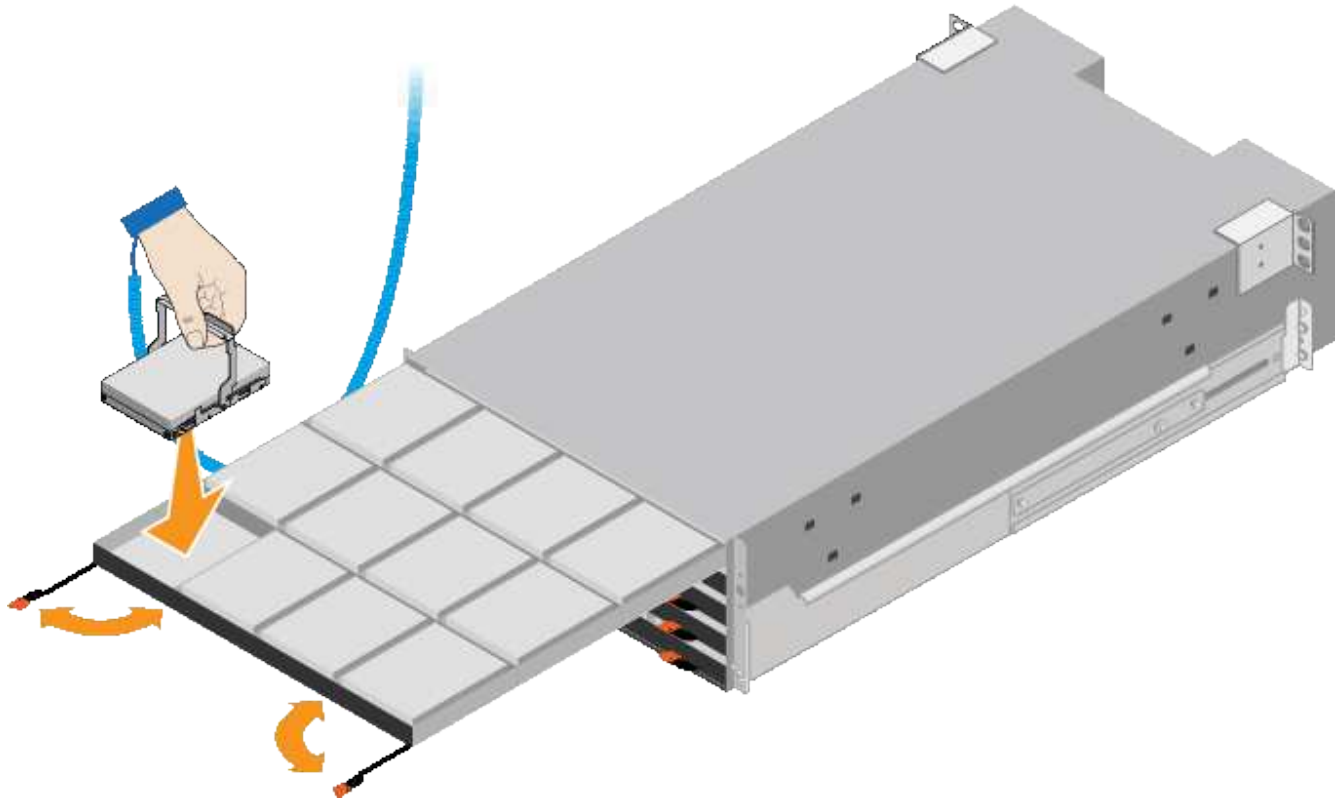
> Para evitar que se dañe el hardware, no mueva nunca la bandeja si hay unidades instaladas. Debe quitar todas las unidades antes de mover la bandeja.

Pasos

1. Envuelva el extremo de la correa de la muñequera ESD alrededor de su muñeca y fije el extremo de la pinza a una masa metálica para evitar descargas estáticas.
2. Quite las unidades de su embalaje.
3. Suelte las palancas del cajón de mando superior y deslice el cajón hacia fuera con las palancas.
4. Busque las dos unidades SSD.

   > Las bandejas de expansión no utilizan unidades SSD.

5. Levante cada palanca de mando a una posición vertical.
6. Instale las dos unidades SSD en las ranuras 0 y 1 (las primeras dos ranuras a lo largo del lado izquierdo del cajón).
7. Coloque con cuidado cada unidad en su ranura y baje el asa de la unidad levantada hasta que encaje en su lugar.



8. Instale 10 unidades de disco duro en el cajón superior.
9. Deslice el cajón hacia atrás presionando el centro y cerrando ambas palancas con cuidado.

> Deje de empujar el cajón si siente que está agarrotado. Utilice las palancas de liberación de la parte delantera del cajón para desdeslizar el cajón hacia atrás. A continuación, vuelva a insertar con cuidado el cajón en la ranura.

10. Repita estos pasos para instalar unidades de disco duro en los otros cuatro cajones.

> Debe instalar las 60 unidades para garantizar que su funcionamiento es correcto.

11. Coloque el panel frontal en la bandeja.
12. Si tiene bandejas de ampliación, repita estos pasos para instalar 12 unidades de disco duro en cada cajón de cada bandeja de ampliación.
13. Siga las instrucciones de instalación del SG6000-CN en un armario o bastidor.

SGF6024: Instale las bandejas de 24 unidades en el armario o rack

Debe instalar un conjunto de rieles para la bandeja de controladoras EF570 en su armario o rack y, a continuación, deslizar la cabina sobre los rieles.

Lo que necesitará

- Ha revisado el documento de avisos de seguridad que se incluye en la caja y comprende las precauciones para mover e instalar el hardware.
- Tiene las instrucciones incluidas en el kit de raíl.

Pasos

1. Siga con cuidado las instrucciones del kit de raíl para instalar los rieles en su armario o rack.

   En el caso de armarios con orificios cuadrados, primero debe instalar las tuercas de jaula proporcionadas para asegurar la parte delantera y trasera de la estantería con tornillos.

2. Retire la caja de embalaje exterior del aparato. A continuación, pliegue las solapas de la caja interior.
3. Coloque la parte posterior de la bandeja (el extremo con los conectores) en los rieles.

   Una balda totalmente cargada pesa aproximadamente 24 kg (52 lb). Se necesitan dos personas para mover la carcasa de forma segura.

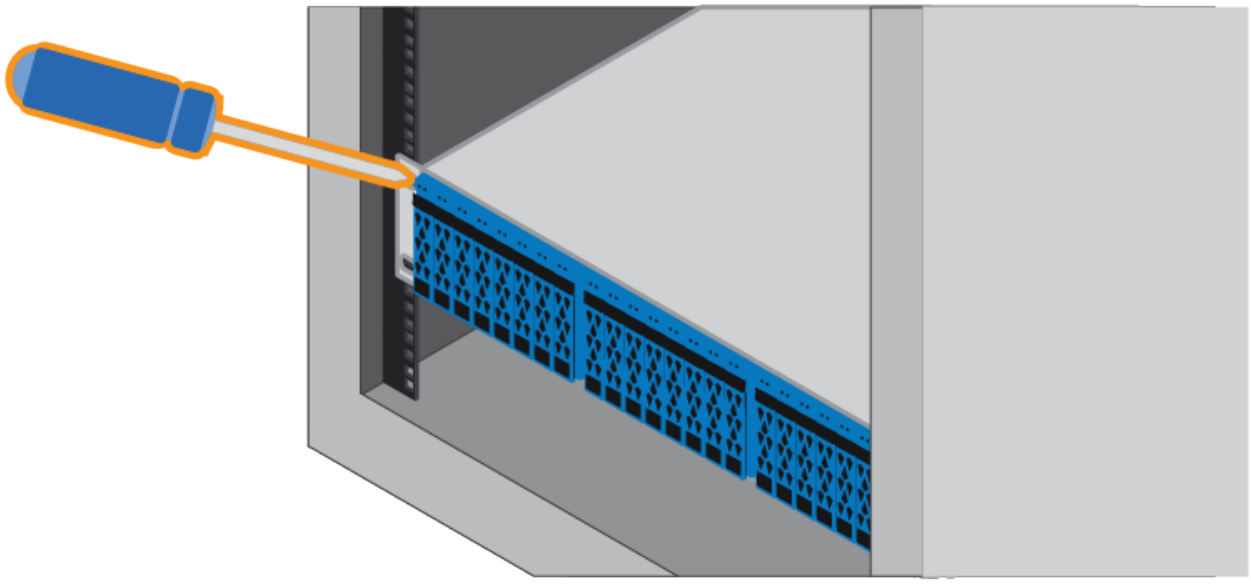
4. Deslice con cuidado la caja completamente sobre los rieles.

   Es posible que tenga que ajustar los rieles para asegurarse de que el alojamiento se desliza completamente sobre los rieles.

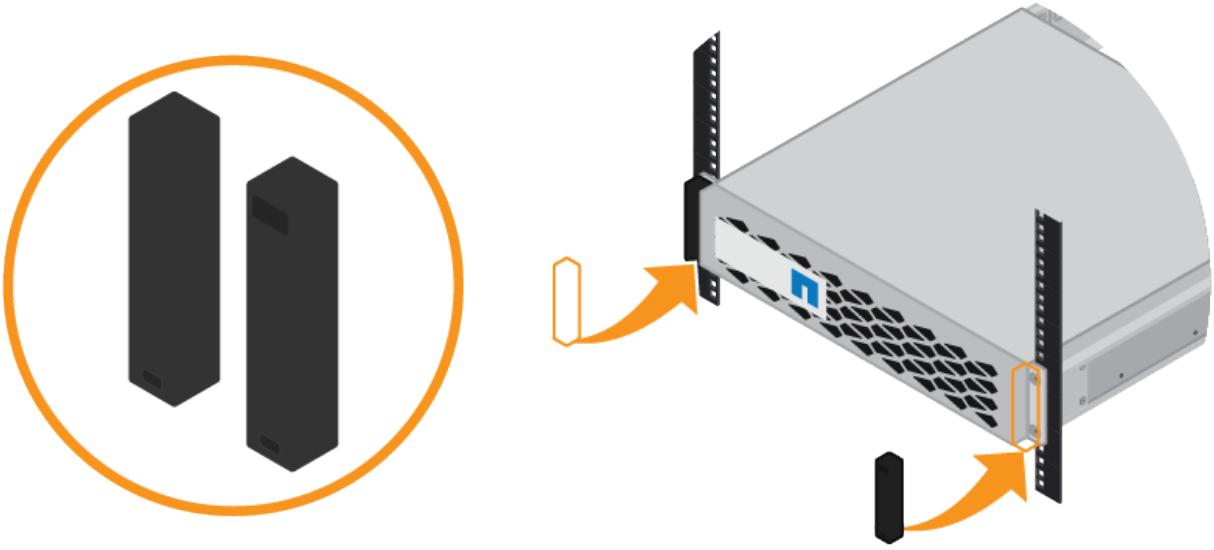
   No coloque equipo adicional sobre los rieles después de haber terminado de instalar la carcasa. Los rieles no están diseñados para soportar un peso adicional.

   Si corresponde, puede que deba retirar las tapas de extremo de la bandeja o el panel frontal del sistema para fijar el compartimento a la poste del rack; si es así, debe sustituir las tapas de extremo o el bisel cuando haya terminado.

5. Fije el compartimento a la parte frontal del armario o rack y los rieles introduciendo dos tornillos M5 a través de los soportes de montaje (preinstalados en ambos lados de la parte frontal del gabinete), los orificios en el rack o armario del sistema y los orificios en la parte frontal de los rieles.



6. Fije la carcasa a la parte posterior de los rieles insertando dos tornillos M5 por los soportes de la carcasa y el soporte del kit de rieles.
7. Si procede, sustituya las tapas del extremo de la bandeja o el embellecedor del sistema.



SG6000-CN: Instalación en armario o bastidor

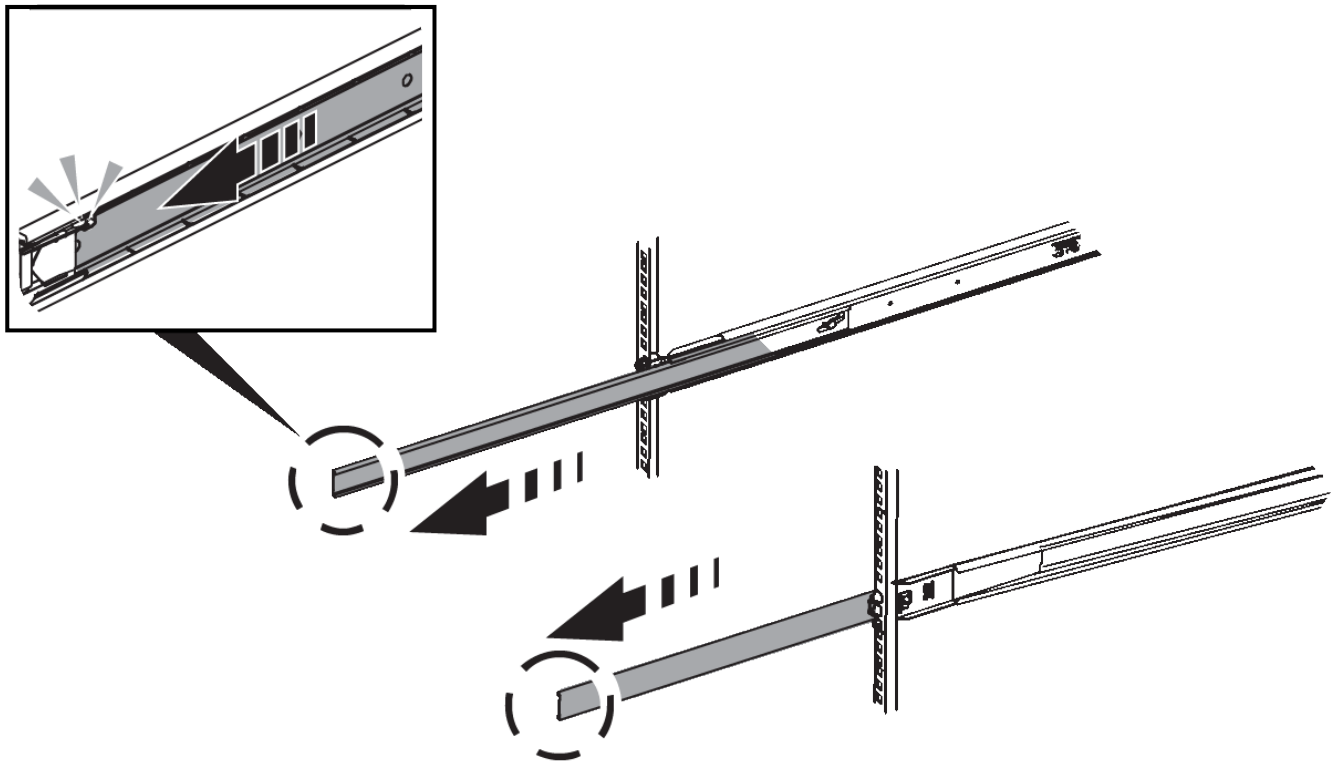
Debe instalar un conjunto de rieles para el controlador SG6000-CN en su armario o rack y, a continuación, deslizar el controlador sobre los rieles.

Lo que necesitará

- Ha revisado el documento de avisos de seguridad que se incluye en la caja y comprende las precauciones para mover e instalar el hardware.
- Tiene las instrucciones incluidas en el kit de raíl.
- Instaló la bandeja de controladoras E2860 y unidades o la bandeja de controladoras EF570.

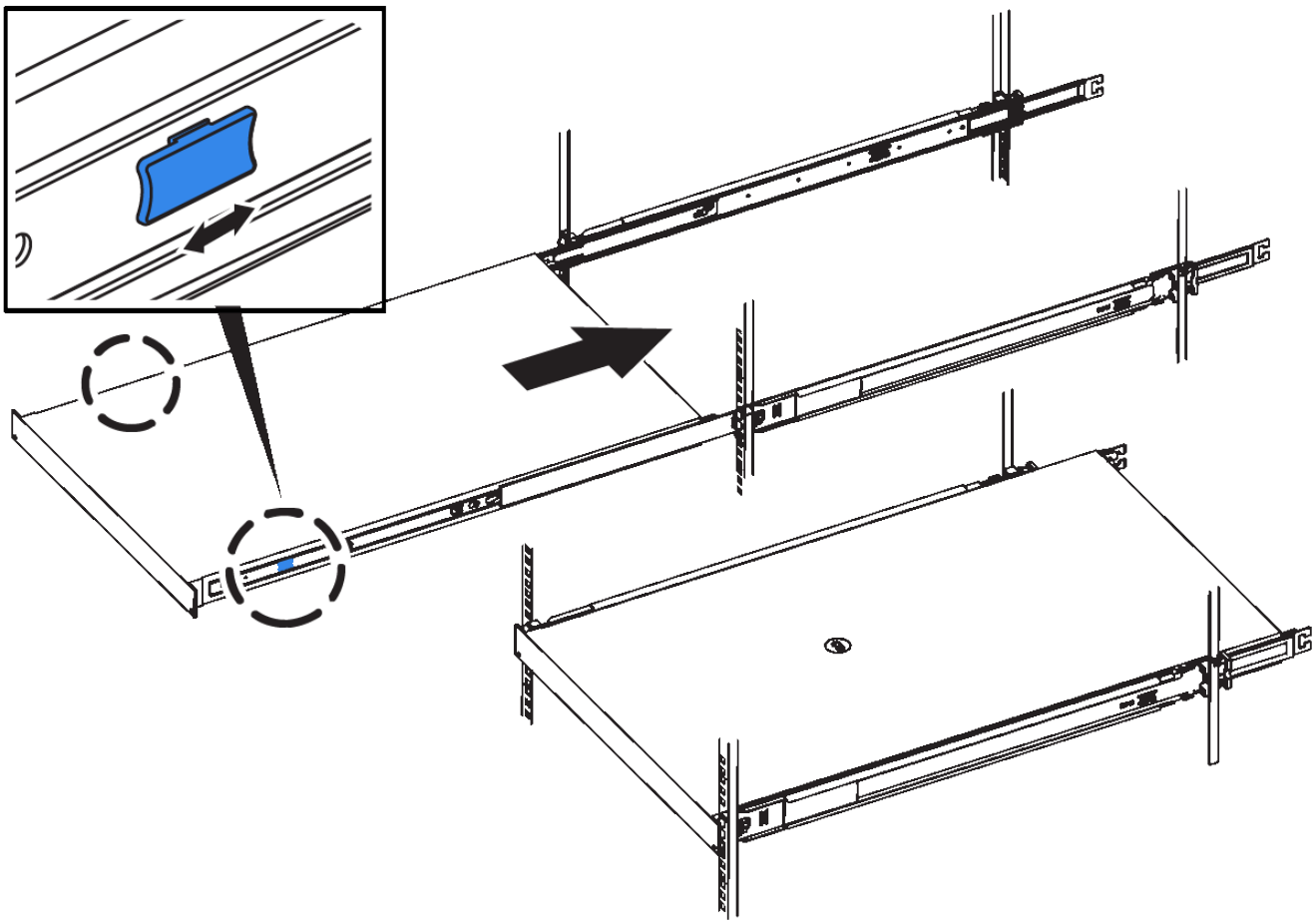
Pasos

1. Siga con cuidado las instrucciones del kit de raíl para instalar los rieles en su armario o rack.
2. En los dos rieles instalados en el armario o rack, extienda las partes móviles de los rieles hasta que oiga un clic.



3. Inserte el controlador SG6000-CN en los rieles.
4. Deslice el controlador en el armario o rack.

   Cuando no pueda mover el controlador más, tire de los pestillos azules a ambos lados del chasis para deslizar el controlador completamente.



No conecte el panel frontal hasta que haya encendido la controladora.

5. Apriete los tornillos cautivos del panel frontal del controlador para fijar el controlador en el rack.

Aparato de cable (SG6000)

Debe conectar los controladores de almacenamiento al controlador SG6000-CN, conectar los puertos de administración de los tres controladores y conectar los puertos de red del controlador SG6000-CN a la red de cuadrícula y a la red de cliente opcional para StorageGRID.

Lo que necesitará

- Dispone de los cuatro cables ópticos suministrados con el aparato para conectar los dos controladores de almacenamiento al controlador SG6000-CN.
- Tiene cables Ethernet RJ-45 (cuatro mínimos) para conectar los puertos de administración.
- Tiene una de las siguientes opciones para los puertos de red. Estos artículos no se proporcionan con el aparato.
  - De uno a cuatro cables Twinax para conectar los cuatro puertos de red.

- De uno a cuatro transceptores SFP+ o SFP28 si planea utilizar cables ópticos para los puertos.

> **Riesgo de exposición a la radiación láser** — no desmonte ni retire ninguna parte de un transceptor SFP. Puede que esté expuesto a la radiación láser.

Acerca de esta tarea

En esta sección se proporcionan instrucciones para el cableado de los siguientes dispositivos:

- SG6060 y SG6060X
- SGF6024

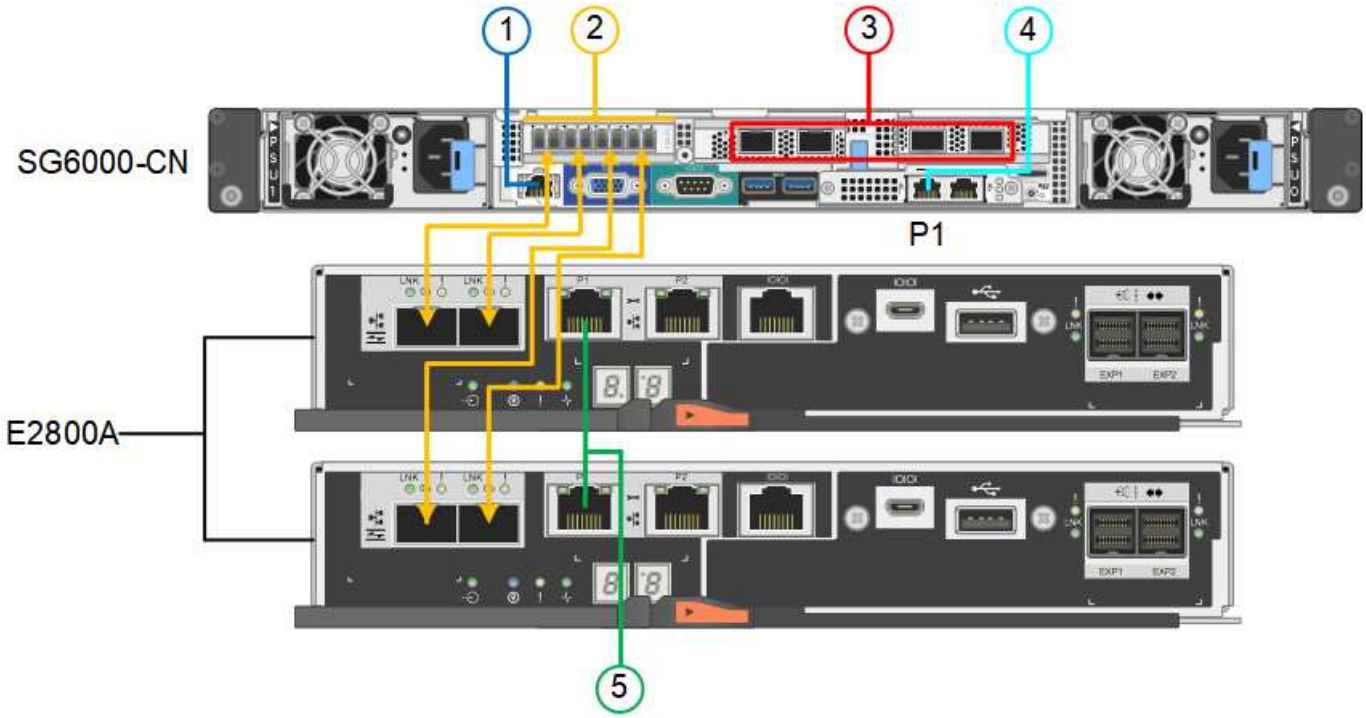
Conecte el cable SG6060 o SG6060X

Las siguientes figuras muestran las tres controladoras en los dispositivos SG6060 y SG6060X, con el controlador de computación SG6000-CN en la parte superior y las dos controladoras de almacenamiento E2800 en la parte inferior.

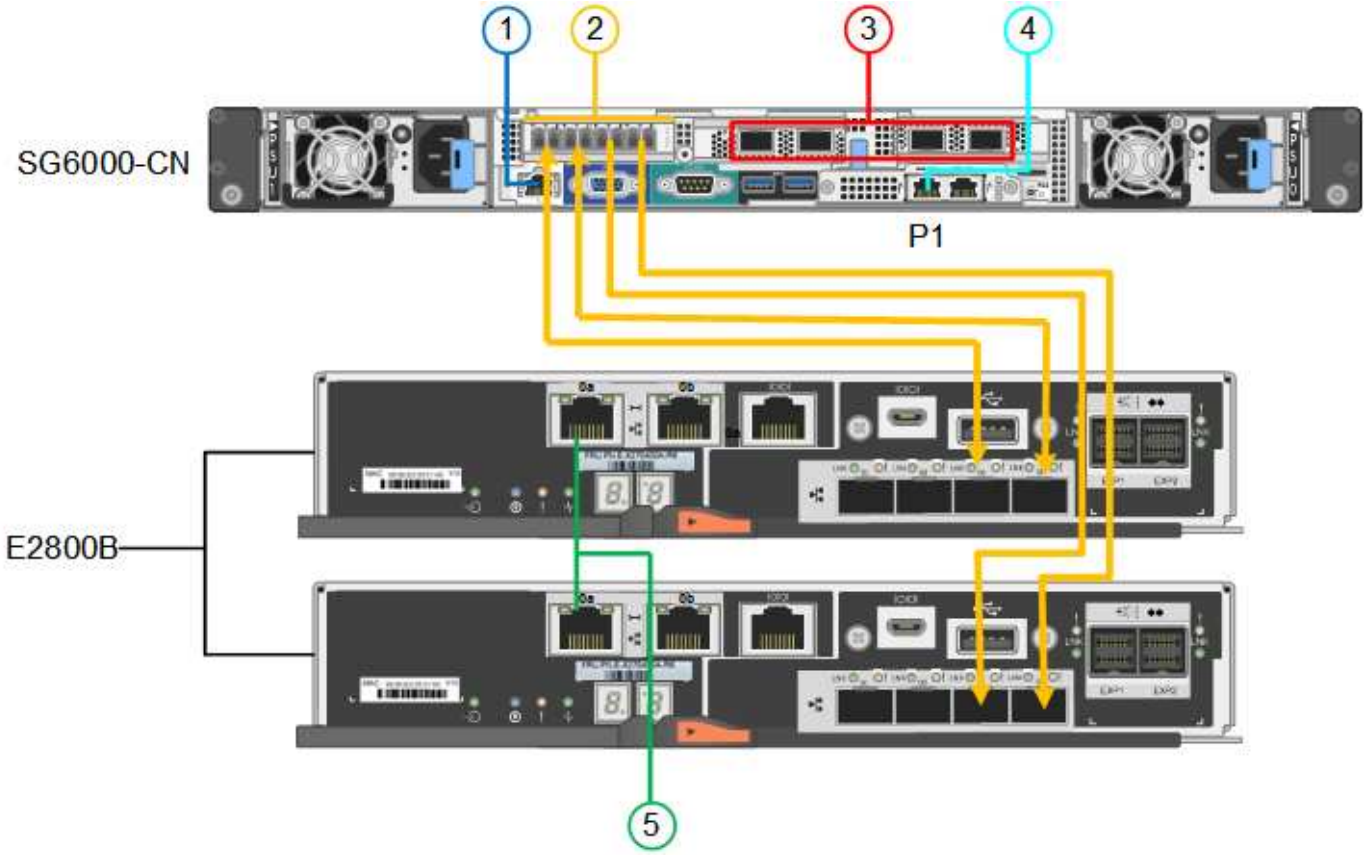
> El SG6060 tiene controladores E2800A y la SG606060X tiene controladoras E2800B. Ambas versiones de la controladora E2800 tienen especificaciones y funciones idénticas a excepción de la ubicación de los puertos de interconexión.

> No use las controladoras E2800A y E2800B en el mismo dispositivo.

SG6060 a E2800A conexiones

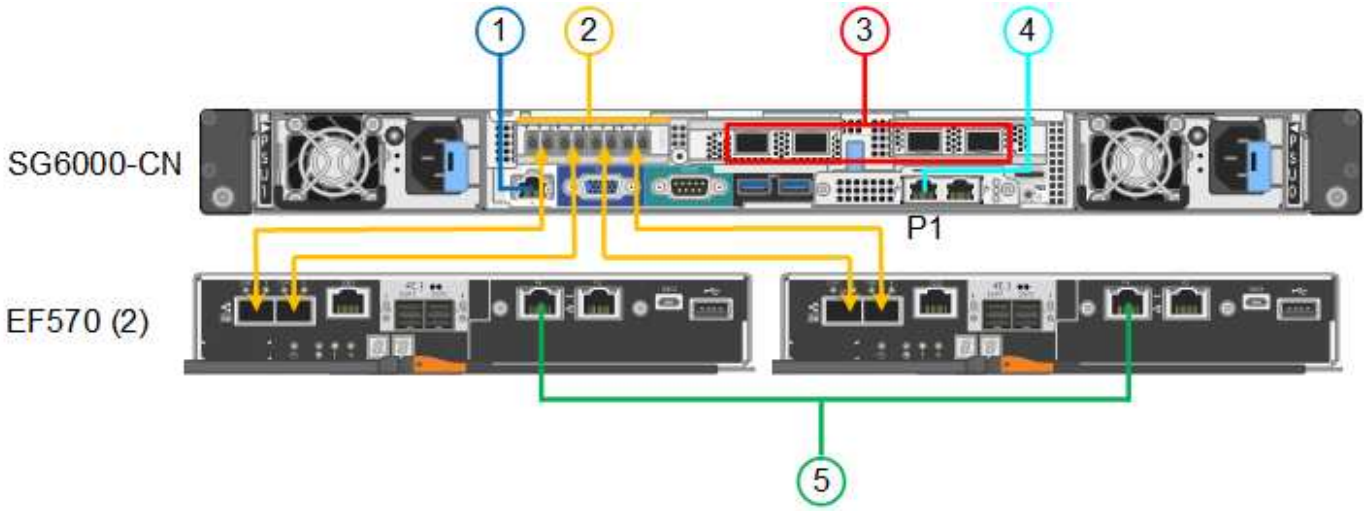


Conexiones SG606060X a E2800B



Conecte el cable SGF6024

La siguiente figura muestra las tres controladoras del dispositivo SGF6024, con el controlador de computación SG6000-CN en la parte superior y las dos controladoras de almacenamiento EF570 en paralelo debajo del controlador de computación.



	Puerto	Tipo de puerto	Función
1	Puerto de gestión de BMC en el controlador SG6000-CN	1 GbE (RJ-45).	Se conecta a la red en la que se accede a la interfaz del BMC.

	Puerto	Tipo de puerto	Función
2	Puertos de conexión FC: • 4 en el controlador SG6000-CN • 2 en cada controladora de almacenamiento	SFP+ óptico FC de 16 GB/s	Conecte cada controlador de almacenamiento al controlador SG6000-CN.
3	Cuatro puertos de red en el controlador SG6000-CN	10/25 GbE	Conéctese a la red de red y a la red de cliente para StorageGRID.
4	Puerto de red de administración en el controlador SG6000-CN (con la etiqueta P1 en la figura)	1 GbE (RJ-45). **Importante:** este puerto funciona sólo a 1000 BaseT/full y no admite velocidades de 10 o 100 megabits.	Conecta el controlador SG6000-CN a la red de administración para StorageGRID.
	Puerto RJ-45 derecho en el controlador SG6000-CN	1 GbE (RJ-45). **Importante:** este puerto funciona sólo a 1000 BaseT/full y no admite velocidades de 10 o 100 megabits.	• Se puede unir al puerto de administración 1 si desea una conexión redundante a la red de administración. • Puede dejarse sin cables y disponible para acceso local temporal (IP 169.254.0.1). • Durante la instalación, se puede utilizar para conectar el controlador SG6000-CN a un portátil de servicio si las direcciones IP asignadas por DHCP no están disponibles.
5	Puerto de gestión 1 en cada controladora de almacenamiento	1 GbE (RJ-45).	Se conecta a la red en la que se accede a System Manager de SANtricity.
	Puerto de gestión 2 en cada controladora de almacenamiento	1 GbE (RJ-45).	Reservado para soporte técnico.

Pasos

1. Conecte el puerto de administración de BMC del controlador SG6000-CN a la red de administración mediante un cable Ethernet.

   Aunque esta conexión es opcional, se recomienda facilitar el soporte.

2. Conecte los dos puertos FC de cada controlador de almacenamiento a los puertos FC de la controladora

SG6000-CN, utilizando cuatro cables ópticos y cuatro transceptores SFP+ para las controladoras de almacenamiento.

3. Conecte los puertos de red del controlador SG6000-CN a los switches de red adecuados utilizando cables Twinax o cables ópticos y transceptores SFP+ o SFP28.

> Los cuatro puertos de red deben usar la misma velocidad de enlace. Instale transceptores SFP+ si tiene pensado utilizar velocidades de enlace 10-GbE. Instale transceptores SFP28 si tiene pensado utilizar velocidades de enlace 25-GbE.

   - Si piensa utilizar el modo de enlace de puerto fijo (predeterminado), conecte los puertos a la red de StorageGRID y a las redes de cliente, como se muestra en la tabla.

Puerto	Conecta a…
Puerto 1	Red de cliente (opcional)
Puerto 2	Red Grid
Puerto 3	Red de cliente (opcional)
Puerto 4	Red Grid

   - Si planea utilizar el modo de enlace de puerto agregado, conecte uno o varios puertos de red a uno o varios switches. Debe conectar al menos dos de los cuatro puertos para evitar tener un único punto de error. Si utiliza más de un switch para un único vínculo LACP, los switches deben ser compatibles con MLAG o equivalente.

4. Si tiene previsto utilizar la Red de administración para StorageGRID, conecte el puerto Red de administración del controlador SG6000-CN a la Red de administración, mediante un cable Ethernet.
5. Si tiene pensado utilizar la red de gestión para SANtricity System Manager, conecte el puerto de gestión 1 (P1 en el E2800A y 0a en el E2800B) en cada controladora de almacenamiento (el puerto RJ-45 a la izquierda) a la red de gestión para SANtricity System Manager, utilizando un cable Ethernet.

   No utilice el puerto de gestión 2 (P2 en E2800A y 0b en E2800B) en la controladora de almacenamiento (el puerto RJ-45 a la derecha). Este puerto está reservado para el soporte técnico.

Información relacionada

Modos de enlace de puertos para el controlador SG6000-CN

Vuelva a instalar el controlador SG6000-CN en el armario o bastidor

SG6060 y SG606060X: Cableado de bandejas de expansión opcionales

Si utiliza bandejas de expansión, debe conectarlos a la bandeja de controladoras E2860. Puede tener un máximo de dos bandejas de expansión para cada dispositivo SG6060 o SG6060X.

Lo que necesitará

- Se suministran los dos cables SAS con cada bandeja de ampliación.

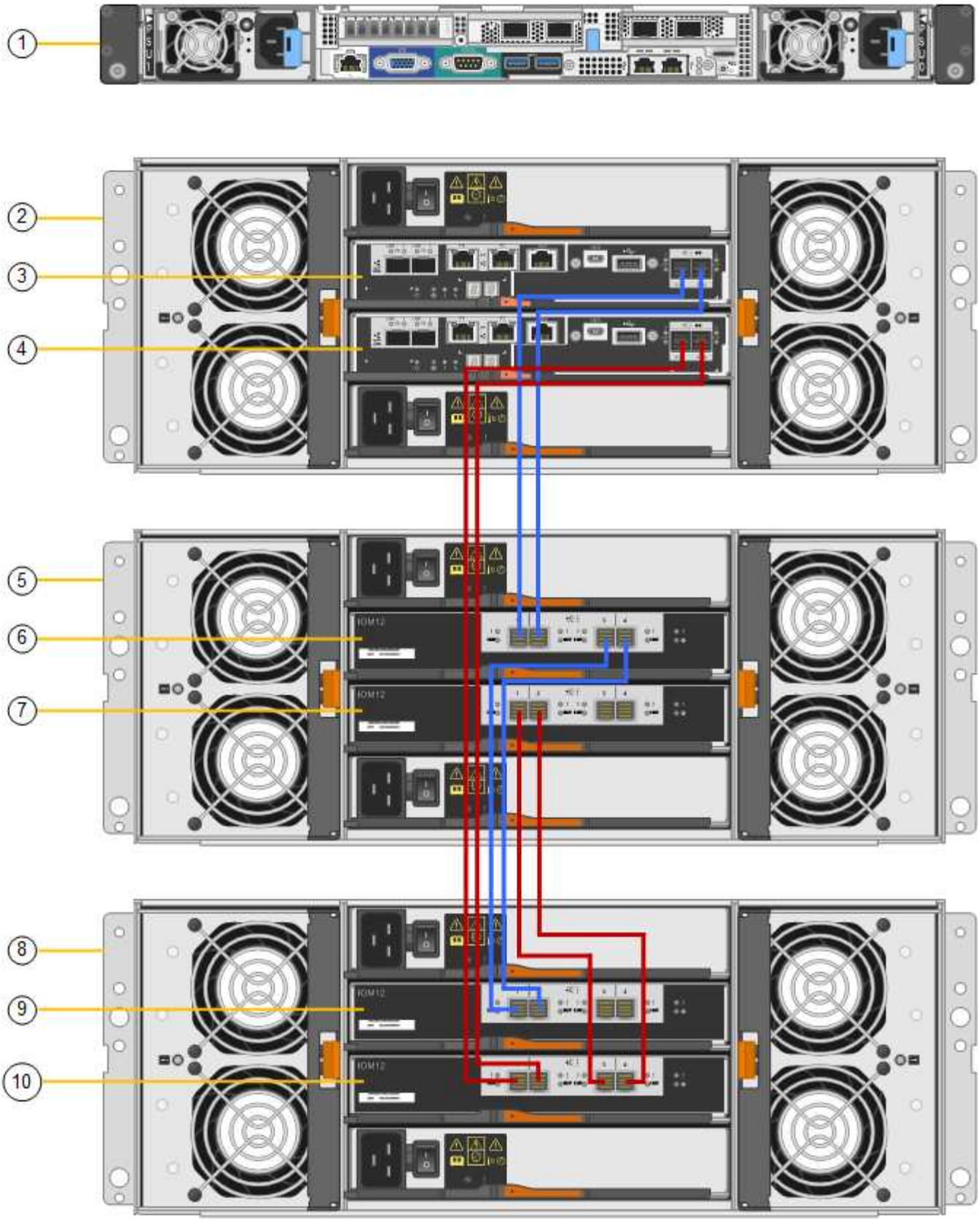
- Instaló las bandejas de expansión en el armario o rack que contiene la bandeja de controladoras E2860.

  SG6060 y SG606060X: Instale bandejas de 60 unidades en el armario o rack

Paso

Conecte cada bandeja de expansión a la bandeja de controladoras E2860 como se muestra en el diagrama.

Este dibujo muestra el cableado para dos estantes de expansión en un SG6060 (el cableado de expansión para SG6060X es el mismo). Si solo tiene una bandeja de expansión, conecte IOM A a la controladora A y conecte el IOM B a la controladora B.



Llamada	Descripción
1	SG6000-CN

Llamada	Descripción
2	Bandeja de controladoras E2860
3	Controladora a
4	Controladora B
5	Bandeja de expansión 1
6	IOM A para la bandeja de ampliación 1
7	IOM B para la bandeja de expansión 1
8	Bandeja de expansión 2
9	IOM A para bandeja de expansión 2
10	IOM B para la bandeja de expansión 2

Conexión de los cables de alimentación y alimentación (SG6000)

Después de conectar los cables de red, estará preparado para aplicar alimentación al controlador SG6000-CN y a los dos controladores de almacenamiento o a las bandejas de expansión opcionales.

Pasos

1. Confirmar que ambas controladoras de la bandeja de controladoras de almacenamiento están desactivadas.

> **Riesgo de descarga eléctrica** — antes de conectar los cables de alimentación, asegúrese de que los interruptores de alimentación de cada uno de los dos controladores de almacenamiento están apagados.

2. Si tiene bandejas de expansión, confirme que ambos switches de alimentación de IOM están apagados.

> **Riesgo de descarga eléctrica** — antes de conectar los cables de alimentación, asegúrese de que los dos interruptores de alimentación de cada uno de los estantes de expansión están apagados.

3. Conecte un cable de alimentación a cada una de las dos unidades de alimentación del controlador SG6000-CN.
4. Conecte estos dos cables de alimentación a dos unidades de distribución de alimentación (PDU) diferentes en el armario o rack.
5. Conecte un cable de alimentación a cada una de las dos unidades de alimentación de la bandeja del controlador de almacenamiento.
6. Si dispone de bandejas de expansión, conecte un cable de alimentación a cada una de las dos unidades

de alimentación de cada bandeja de expansión.

7. Conecte los dos cables de alimentación de cada bandeja de almacenamiento (incluidas las bandejas de expansión opcionales) a dos PDU diferentes en el armario o rack.
8. Si el botón de encendido de la parte frontal del controlador SG6000-CN no está iluminado en azul actualmente, pulse el botón para encender el controlador.

   No vuelva a pulsar el botón de encendido durante el proceso de encendido.

9. Encienda los dos switches de alimentación en la parte posterior de la bandeja de controladoras de almacenamiento. Si tiene bandejas de expansión, encienda los dos switches de alimentación de cada bandeja.
   - No apague los interruptores de alimentación durante el proceso de encendido.
   - Es posible que los ventiladores de la bandeja de controladoras de almacenamiento y las bandejas de expansión opcionales sean muy ruidosos cuando se inician por primera vez. El ruido fuerte durante el arranque es normal.
10. Una vez arrancados los componentes, compruebe su estado.
    - Revise la visualización de siete segmentos en la parte posterior de cada controladora de almacenamiento. Consulte el artículo sobre la visualización de los códigos de estado de inicio para obtener más información.
    - Compruebe que el botón de encendido situado en la parte frontal del controlador SG6000-CN está encendido.
11. Si se producen errores, corrija los problemas.
12. Fije el bisel frontal al controlador SG6000-CN si se ha retirado.

Información relacionada

Ver los códigos de estado de arranque para los controladores de almacenamiento SG6000

Ver los indicadores de estado y los botones del controlador SG6000-CN

Vuelva a instalar el controlador SG6000-CN en el armario o bastidor

Ver los indicadores de estado y los botones del controlador SG6000-CN

El controlador SG6000-CN incluye indicadores que ayudan a determinar el estado del controlador, incluidos los siguientes indicadores y botones.

	Mostrar	Descripción
1	Botón de encendido	• Azul: El controlador está encendido. • Apagado: La controladora está apagada.

	Mostrar	Descripción
2	Botón de reinicio	*No hay indicador* Utilice este botón para realizar un restablecimiento completo del controlador.
3	Botón identificar	• Parpadeo o azul fijo: Identifica la controladora en el armario o rack. • Desactivado: El controlador no se puede identificar visualmente en el armario o bastidor. Este botón se puede establecer en enlace, encendido (sólido) o Apagado.
4	LED de alarma	• Ámbar: Se ha producido un error. **Nota:** para ver los códigos de arranque y error, debe acceder a la interfaz del BMC. • Desactivado: No hay errores.

códigos generales de arranque

Durante el arranque o tras un restablecimiento manual del controlador SG6000-CN, se produce lo siguiente:

1. El controlador de administración de la placa base (BMC) registra los códigos de la secuencia de arranque, incluidos los errores que se produzcan.
2. El botón de encendido se ilumina.
3. Si se produce algún error durante el arranque, el LED de alarma se enciende.

   Para ver los códigos de arranque y error, debe acceder a la interfaz del BMC.

Información relacionada

Solución de problemas de instalación de hardware (SG6000)

Configurar la interfaz de BMC (SG6000)

Encienda el controlador SG6000-CN y compruebe el funcionamiento

Ver los códigos de estado de arranque para los controladores de almacenamiento SG6000

Cada controladora de almacenamiento tiene una pantalla de siete segmentos que proporciona códigos de estado cuando se enciende la controladora. Los códigos de estado son los mismos para la controladora E2800 y la controladora EF570.

Acerca de esta tarea

Para obtener descripciones de estos códigos, consulte la información de supervisión del sistema E-Series para usted sobre el tipo de controladora de almacenamiento.

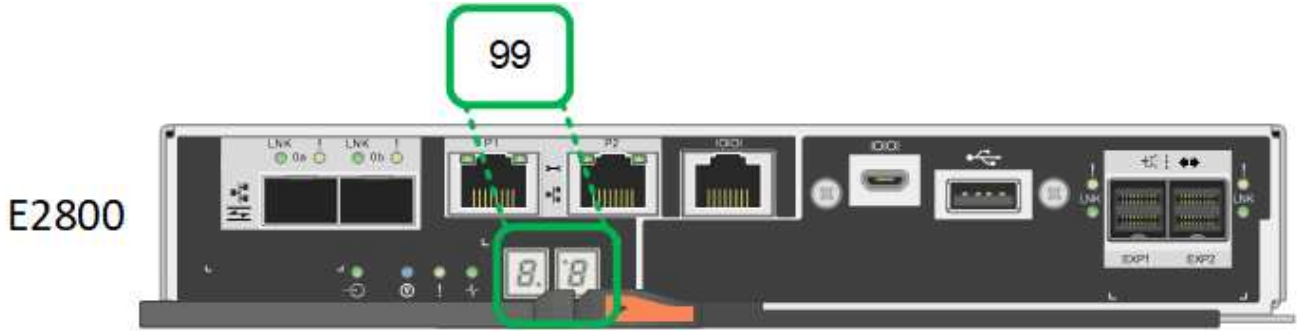
Pasos

1. Durante el arranque, supervise el progreso visualizando los códigos que se muestran en la pantalla de siete segmentos de cada controladora de almacenamiento.

   La pantalla de siete segmentos de cada controlador de almacenamiento muestra la secuencia de repetición **OS**, **SD**, ***blank*** indica que la controladora está ejecutando el procesamiento de inicio del día.

2. Una vez arrancados las controladoras, confirme que cada controladora de almacenamiento muestra 99, que es el ID predeterminado de una bandeja de controladoras E-Series.

   Asegúrese de que este valor se muestre en ambas controladoras de almacenamiento, como se muestra en este ejemplo de controladora E2800.



3. Si una o ambas controladoras muestran otros valores, consulte Solución de problemas de instalación de hardware (SG6000) y confirme que ha completado los pasos de la instalación correctamente. Si no puede resolver el problema, póngase en contacto con el soporte técnico.

Información relacionada

"Guía de supervisión del sistema E5700 y E2800"

"Soporte de NetApp"

Encienda el controlador SG6000-CN y compruebe el funcionamiento

Configuración del hardware (SG6000)

Después de aplicar la alimentación al dispositivo, debe configurar las conexiones de red que utilizará StorageGRID. Es necesario configurar SANtricity System Manager, que es el software que se utilizará para supervisar las controladoras de almacenamiento y otro hardware en la bandeja de controladoras. También debe asegurarse de que puede acceder a la interfaz de BMC para el controlador SG6000-CN.

Configurar las conexiones StorageGRID (SG6000)

Para poder implementar un dispositivo StorageGRID como nodo de almacenamiento en un sistema StorageGRID, debe configurar las conexiones entre el dispositivo y las redes que planea utilizar. Puede configurar la red en el instalador de dispositivos de StorageGRID, que está preinstalado en el controlador SG6000-CN (el controlador de computación).

Acceda al instalador de dispositivos de StorageGRID

Debe acceder al instalador de dispositivos de StorageGRID para verificar la versión del instalador y configurar las conexiones entre el dispositivo y las tres redes StorageGRID: La red de grid, la red de administración (opcional) y la red de cliente (opcional).

Lo que necesitará

- Está utilizando cualquier cliente de gestión que pueda conectarse a la red de administración de StorageGRID o que tenga un portátil de servicio.
- El cliente o el portátil de servicio tienen un navegador web compatible.
- El controlador SG6000-CN está conectado a todas las redes StorageGRID que se van a utilizar.
- Conoce la dirección IP, la puerta de enlace y la subred del controlador SG6000-CN en estas redes.
- Configuró los switches de red que planea utilizar.

Acerca de esta tarea

Para acceder inicialmente al instalador de dispositivos de StorageGRID, puede utilizar la dirección IP asignada por DHCP para el puerto de red de administración en el controlador SG6000-CN (si el controlador está conectado a la red de administración) o puede conectar un portátil de servicio directamente al controlador SG6000-CN.

Pasos

1. Si es posible, utilice la dirección DHCP del puerto de red de administración del controlador SG6000-CN para acceder al instalador de dispositivos de StorageGRID.

   a. Busque la etiqueta de dirección MAC en la parte frontal del controlador SG6000-CN y determine la dirección MAC del puerto de red de administración.

      La etiqueta de dirección MAC incluye la dirección MAC para el puerto de gestión del BMC.

      Para determinar la dirección MAC del puerto de red de administración, debe agregar **2** al número hexadecimal de la etiqueta. Por ejemplo, si la dirección MAC de la etiqueta termina en **09**, la dirección MAC del puerto de administración finalizará en **0B**. Si la dirección MAC de la etiqueta termina en **(*y*)FF**, la dirección MAC del puerto de administración finalizará en **(*y*+1)01**. Puede realizar este cálculo fácilmente abriendo Calculadora en Windows, establecerlo en modo Programador, seleccionando hex, escribiendo la dirección MAC y, a continuación, escribiendo **+ 2 =**.

   b. Proporcione la dirección MAC al administrador de red, de modo que puedan buscar la dirección DHCP del dispositivo en la red de administración.

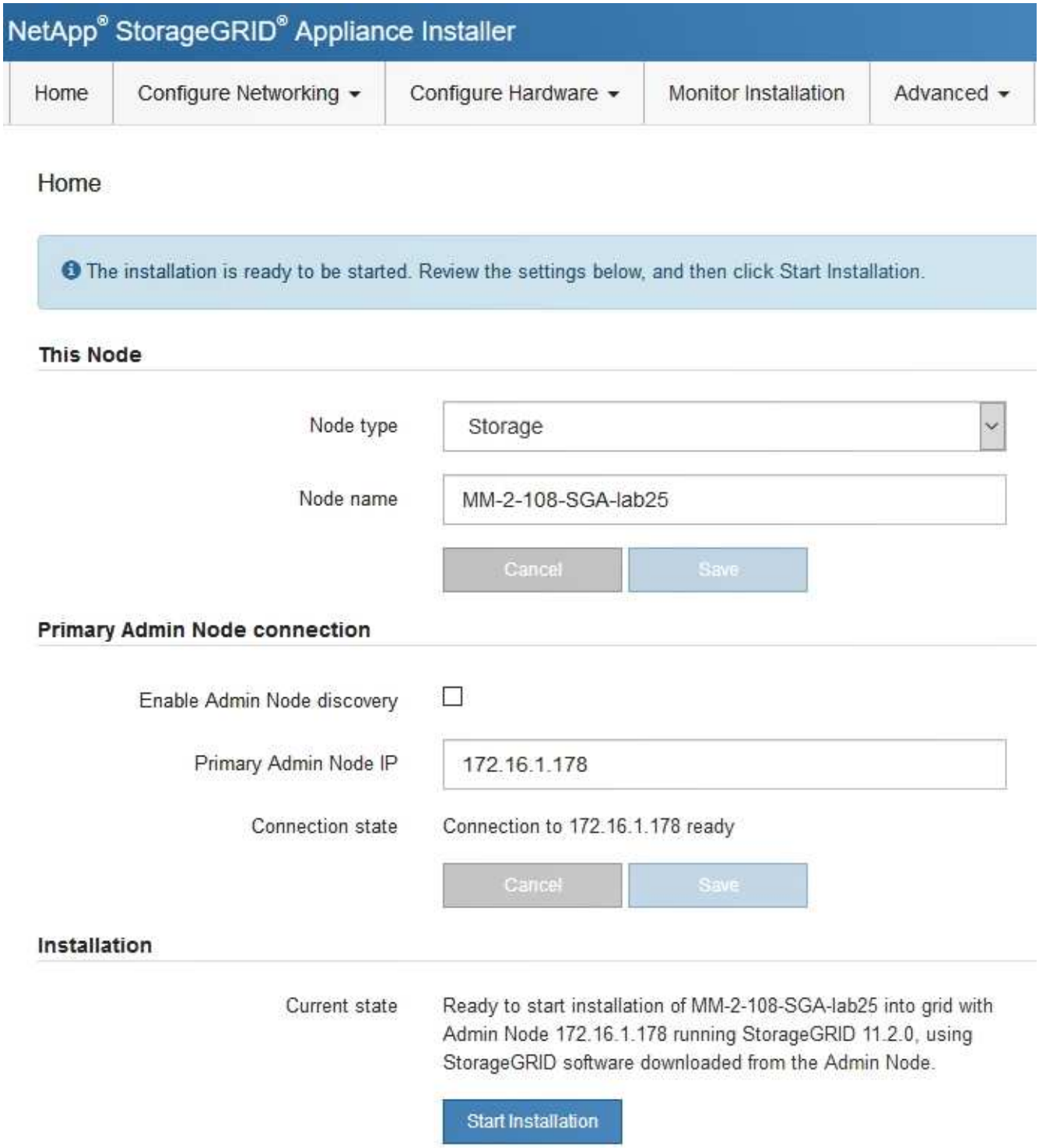
   c. Desde el cliente, introduzca esta URL para el instalador de dispositivos StorageGRID: **`https://Appliance_Controller_IP:8443`**

      Para *`SG6000-CN_Controller_IP`*, Utilice la dirección DHCP.

   d. Si se le solicita una alerta de seguridad, vea e instale el certificado con el asistente de instalación del explorador.

      La alerta no aparecerá la próxima vez que acceda a esta URL.

Aparece la página de inicio del instalador de dispositivos de StorageGRID. La información y los mensajes que se muestran cuando accede por primera vez a esta página dependen de cómo el dispositivo está conectado actualmente a redes StorageGRID. Pueden aparecer mensajes de error que se resolverán en pasos posteriores.



2. Si no puede obtener una dirección IP mediante DHCP, puede usar una conexión de enlace local.

   a. Conecte un portátil de servicio directamente al puerto RJ-45 más derecho del controlador SG6000-CN mediante un cable Ethernet.

b. Abra un explorador Web en el portátil de servicios.

c. Introduzca esta URL para el instalador del dispositivo StorageGRID:
`https://169.254.0.1:8443`

Aparece la página de inicio del instalador de dispositivos de StorageGRID. La información y los mensajes que se muestran al acceder por primera vez a esta página dependen de cómo esté conectado el dispositivo actualmente.

> Si no puede acceder a la página de inicio a través de una conexión local de enlace, configure la dirección IP del portátil de servicio como `169.254.0.2`y vuelva a intentarlo.

Después de terminar

Tras acceder al instalador de dispositivos de StorageGRID:

- Compruebe que la versión de instalador de dispositivos StorageGRID del dispositivo coincide con la versión de software instalada en el sistema StorageGRID. Si es necesario, actualice el instalador de dispositivos StorageGRID.

  Comprobar y actualizar la versión de StorageGRID Appliance Installer

- Revise los mensajes que se muestran en la página principal del instalador de dispositivos de StorageGRID y configure la configuración del enlace y la configuración IP, según sea necesario.

Información relacionada

Requisitos del navegador web

Comprobar y actualizar la versión de StorageGRID Appliance Installer

La versión de instalador del dispositivo StorageGRID en el dispositivo debe coincidir con la versión de software instalada en el sistema StorageGRID para garantizar que todas las funciones de StorageGRID sean compatibles.

Lo que necesitará

Ha accedido al instalador de dispositivos de StorageGRID.

Acerca de esta tarea

Los dispositivos StorageGRID vienen de fábrica preinstalados con el instalador de dispositivos StorageGRID. Si va a añadir un dispositivo a un sistema StorageGRID actualizado recientemente, es posible que deba actualizar manualmente el instalador de dispositivos StorageGRID antes de instalar el dispositivo como un nodo nuevo.

El instalador de dispositivos de StorageGRID se actualiza automáticamente cuando se actualiza a una nueva versión de StorageGRID. No es necesario actualizar el instalador de dispositivos StorageGRID en los nodos del dispositivo instalados. Este procedimiento sólo es necesario cuando se instala un dispositivo que contiene una versión anterior del instalador de dispositivos de StorageGRID.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Actualizar firmware**.
2. Compare la versión actual del firmware con la versión de software instalada en el sistema StorageGRID. (En la parte superior de Grid Manager, seleccione el icono de ayuda y seleccione **Acerca de**).

   El segundo dígito de las dos versiones debe coincidir. Por ejemplo, si el sistema StorageGRID está ejecutando la versión 11.**6**.*x*.*y*, la versión del instalador de dispositivos StorageGRID debe ser 3.**6**.*z*.

3. Si el dispositivo tiene una versión de nivel inferior del instalador de dispositivos de StorageGRID, vaya a. "Descargas de NetApp: Dispositivo de StorageGRID".

   Inicie sesión con el nombre de usuario y la contraseña de su cuenta de NetApp.

4. Descargue la versión adecuada del archivo **Soporte para dispositivos StorageGRID** y el archivo de suma de comprobación correspondiente.

   El archivo de soporte para dispositivos StorageGRID es un `.zip` archivo que contiene las versiones de firmware actuales y anteriores para todos los modelos de dispositivos StorageGRID, en subdirectorios para cada tipo de controlador.

   Después de descargar el archivo de soporte para dispositivos StorageGRID, extraiga el `.zip` archive y consulte el archivo README para obtener información importante sobre la instalación del instalador de dispositivos StorageGRID.

5. Siga las instrucciones de la página Actualizar firmware de Instalador de dispositivos StorageGRID para realizar estos pasos:
   a. Cargue el archivo de soporte (imagen de firmware) apropiado para el tipo de controladora y el archivo de suma de comprobación.
   b. Actualice la partición inactiva.
   c. Reiniciar e intercambiar particiones.
   d. Actualice la segunda partición (inactiva).

Configuración de enlaces de red (serie SG6000)

Puede configurar los enlaces de red para los puertos utilizados para conectar el dispositivo a la red de grid, la red de cliente y la red de administración. Puede establecer la velocidad de enlace, así como los modos de enlace de red y puerto.

Lo que necesitará

Si clona un nodo de un dispositivo, configure los enlaces de red del dispositivo de destino para todos los enlaces que use el nodo del dispositivo de origen.

Si tiene previsto utilizar una velocidad de enlace de 25 GbE:

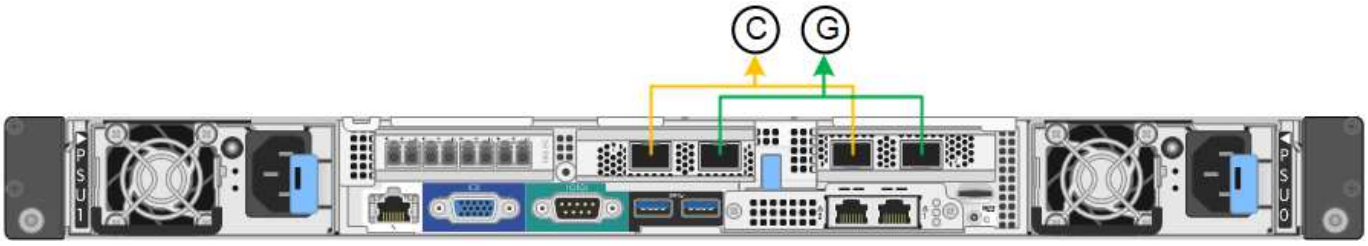
- Está utilizando cables SFP28 Twinax o ha instalado transceptores SFP28 en los puertos de red que va a utilizar.
- Ya debe haber conectado los puertos de red a los switches que puedan admitir estas funciones.
- Comprende cómo configurar los switches para que utilicen esta mayor velocidad.

Si planea utilizar el modo de enlace de puerto de agregado, el modo de enlace de red LACP o el etiquetado de VLAN:

- Conectó los puertos de red del dispositivo a los switches que admiten VLAN y LACP.
- Si varios switches participan en el enlace LACP, los switches admiten grupos de agregación de enlaces de varios chasis (MLAG) o equivalente.
- Comprende cómo configurar los switches para que utilicen VLAN, LACP y MLAG o equivalente.
- Conoce la etiqueta de VLAN única que se utilizará para cada red. Esta etiqueta VLAN se añadirá a cada paquete de red para garantizar que el tráfico de red se dirija a la red correcta.

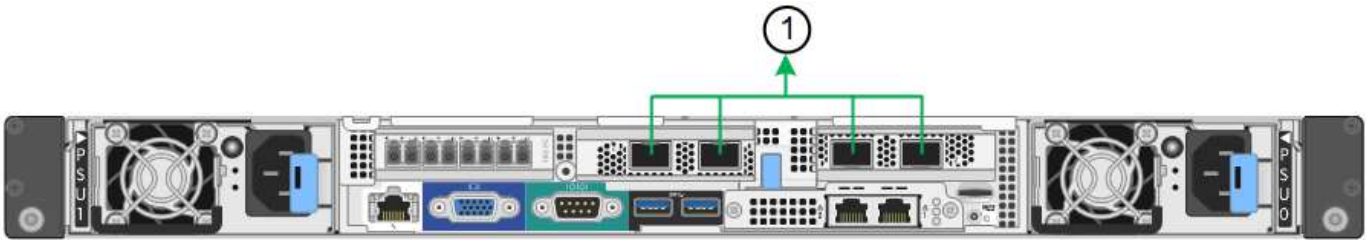
Acerca de esta tarea

En esta figura, se muestra cómo los cuatro puertos de red se vinculan en modo de enlace de puerto fijo (configuración predeterminada).



Llamada	Qué puertos están Unidos
C	Los puertos 1 y 3 se unen para la red cliente, si se utiliza esta red.
G	Los puertos 2 y 4 están Unidos para la red de cuadrícula.

En esta figura, se muestra cómo los cuatro puertos de red están Unidos en el modo de enlace de puerto agregado.



Llamada	Qué puertos están Unidos
1	Los cuatro puertos se agrupan en un enlace LACP único, lo que permite que se usen todos los puertos para el tráfico de red de grid y de red de cliente.

En las tablas, se resumen las opciones para configurar los cuatro puertos de red. La configuración predeterminada se muestra en negrita. Sólo tiene que configurar los ajustes en la página Configuración de vínculos si desea utilizar un valor no predeterminado.

- **Modo de enlace de puerto fijo (predeterminado)**

Modo de enlace de red	Red de cliente desactivada (predeterminada)	Red de cliente habilitada
Active-Backup (predeterminado)	• Los puertos 2 y 4 utilizan un vínculo de copia de seguridad activa para la red Grid. • Los puertos 1 y 3 no se usan. • Una etiqueta de VLAN es opcional.	• Los puertos 2 y 4 utilizan un vínculo de copia de seguridad activa para la red Grid. • Los puertos 1 y 3 utilizan un vínculo de backup activo para la red cliente. • Es posible especificar etiquetas de VLAN para ambas redes.
LACP (802.3ad)	• Los puertos 2 y 4 utilizan un enlace LACP para la red de grid. • Los puertos 1 y 3 no se usan. • Una etiqueta de VLAN es opcional.	• Los puertos 2 y 4 utilizan un enlace LACP para la red de grid. • Los puertos 1 y 3 utilizan un enlace LACP para la red de cliente. • Es posible especificar etiquetas de VLAN para ambas redes.

- **Modo de enlace de puerto agregado**

Modo de enlace de red	Red de cliente desactivada (predeterminada)	Red de cliente habilitada
Solo LACP (802.3ad)	• Los puertos 1-4 utilizan un enlace LACP único para la red de grid. • Una única etiqueta VLAN identifica los paquetes de red Grid.	• Los puertos 1-4 utilizan un enlace LACP único para la red de grid y la red de cliente. • Dos etiquetas VLAN permiten que los paquetes de red de cuadrícula se separen de los paquetes de red de cliente.

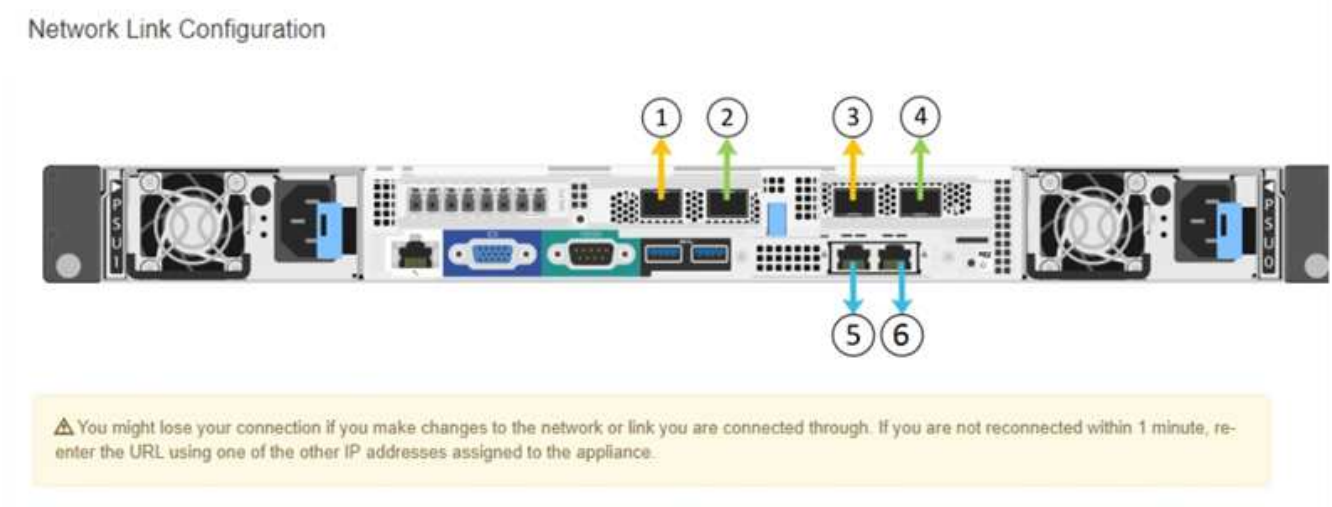
Consulte Modos de enlace de puertos para el controlador SG6000-CN para obtener más información acerca de los modos de enlace de puerto y enlace de red.

Esta figura muestra cómo los dos puertos de gestión de 1 GbE del controlador SG6000-CN están Unidos en el modo de enlace de red Active-Backup para la red Admin.

Pasos

1. En el instalador del dispositivo StorageGRID, haga clic en **Configurar la red Configuración del enlace**.

La página Network Link Configuration muestra un diagrama del dispositivo con los puertos de red y administración numerados.



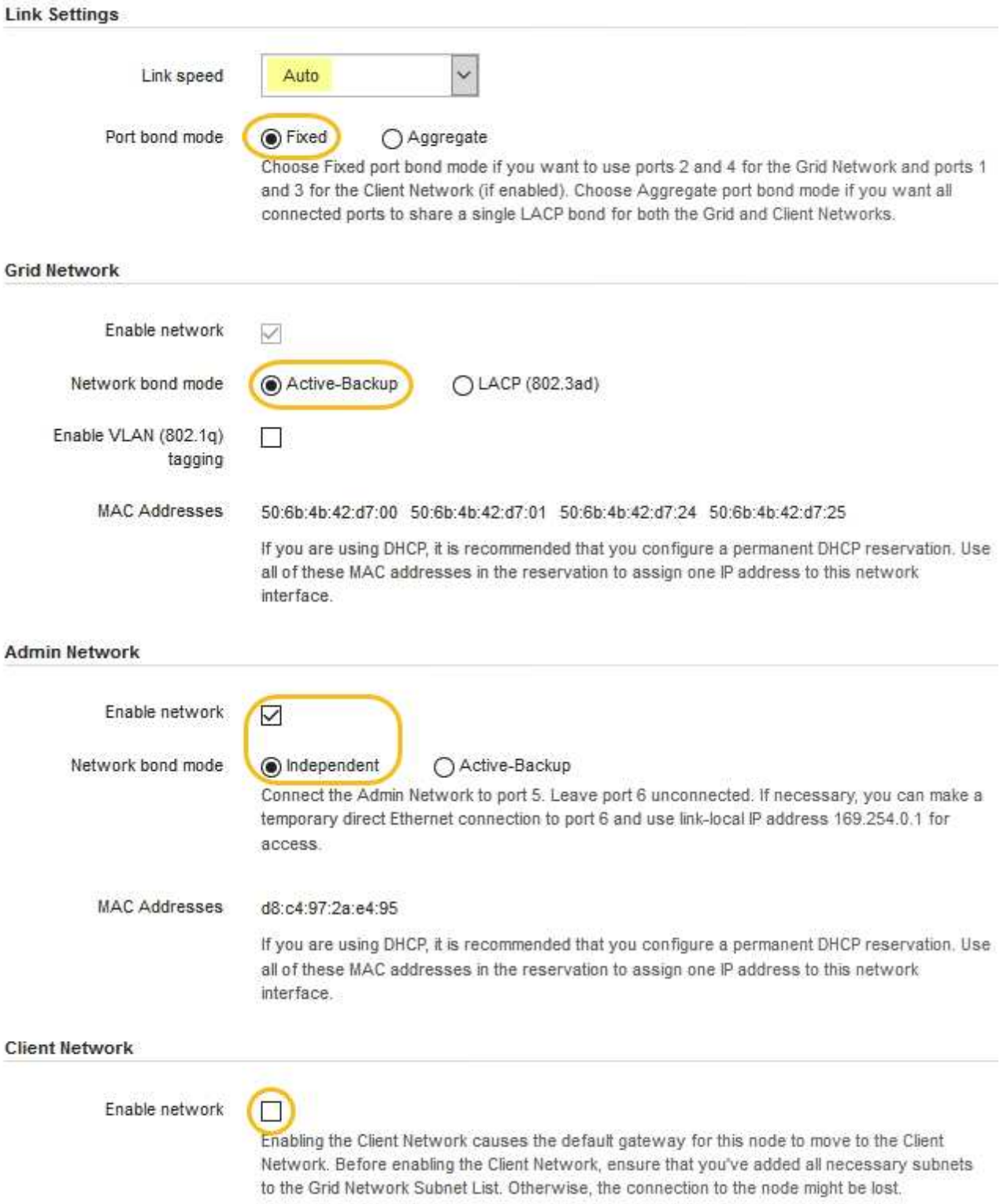
La tabla Estado del enlace muestra el estado de los vínculos (arriba/abajo) y la velocidad (1/10/25/40/100 Gbps) de los puertos numerados.

Link Status

Link	State	Speed (Gbps)
1	Up	100
2	Up	100
3	Down	N/A
4	Down	N/A
5	Up	1
6	Up	1

La primera vez que acceda a esta página:

- **Velocidad de enlace** se ajusta en **Auto**.
- **El modo de enlace de puerto** está establecido en **fijo**.
- **El modo de enlace de red** se establece en **Active-Backup** para la red de cuadrícula.
- La **Red de administración** está activada y el modo de enlace de red se establece en **independiente**.
- La **Red cliente** está desactivada.



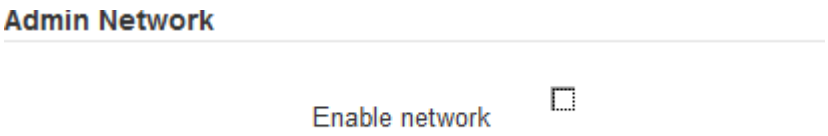
2. Si planea utilizar la velocidad de enlace de 25 GbE para los puertos de red, seleccione **Auto** en la lista desplegable velocidad de enlace.

   Los switches de red que utiliza para la red de cuadrícula y la red de cliente también deben ser compatibles y configurados para esta velocidad. Debe utilizar cables Twinax o cables ópticos de SFP28 y transceptores SFP28.

3. Habilite o deshabilite las redes StorageGRID que tiene previsto utilizar.

Se requiere la red de red. No se puede deshabilitar esta red.

a. Si el dispositivo no está conectado a la red de administración, anule la selección de la casilla de verificación **Activar red** para la red de administración.



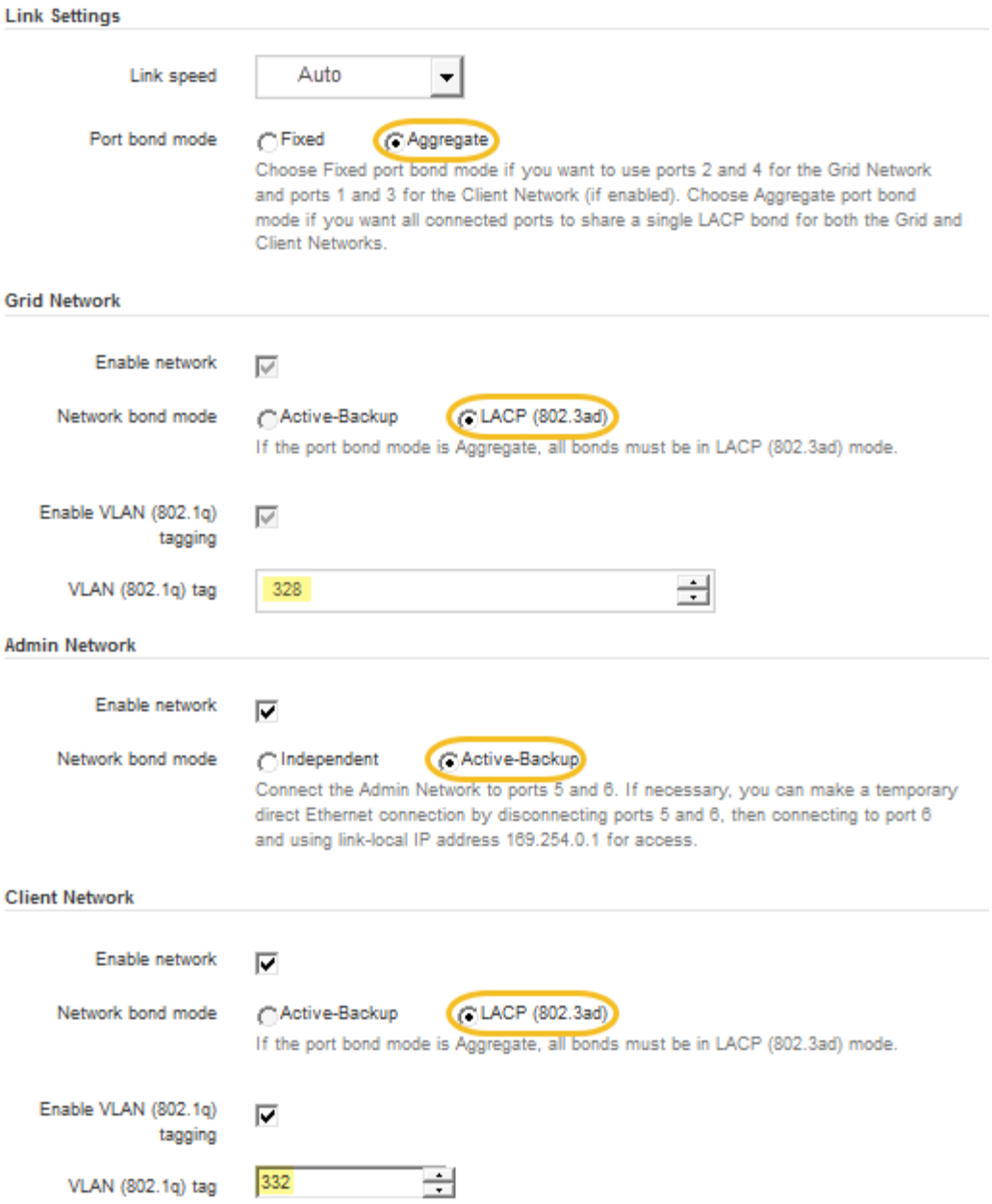
b. Si el dispositivo está conectado a la red cliente, seleccione la casilla de verificación **Activar red** de la red cliente.

   Ahora se muestran los ajustes de red de cliente para los puertos de red.

4. Consulte la tabla y configure el modo de enlace de puerto y el modo de enlace de red.

   Este ejemplo muestra:

   - **Agregado** y **LACP** seleccionados para las redes Grid y Client. Debe especificar una etiqueta de VLAN exclusiva para cada red. Puede seleccionar valores entre 0 y 4095.
   - **Active-Backup** seleccionado para la red de administración.



5. Cuando esté satisfecho con sus selecciones, haga clic en **Guardar**.

> Puede perder la conexión si ha realizado cambios en la red o el enlace que está conectado a través de. Si no vuelve a conectarse en un minuto, vuelva a introducir la URL del instalador de dispositivos de StorageGRID utilizando uno del otro Direcciones IP asignado al dispositivo: **`https://SG6000-CN_Controller_IP:8443`**

Configure las direcciones IP de StorageGRID

El instalador de dispositivos StorageGRID se utiliza para configurar las direcciones IP y la información de enrutamiento utilizadas para el nodo de almacenamiento del dispositivo en las redes de cliente, administrador y grid de StorageGRID.

Acerca de esta tarea

Debe asignar una IP estática al dispositivo en cada red conectada o asignar una concesión permanente a la dirección del servidor DHCP.

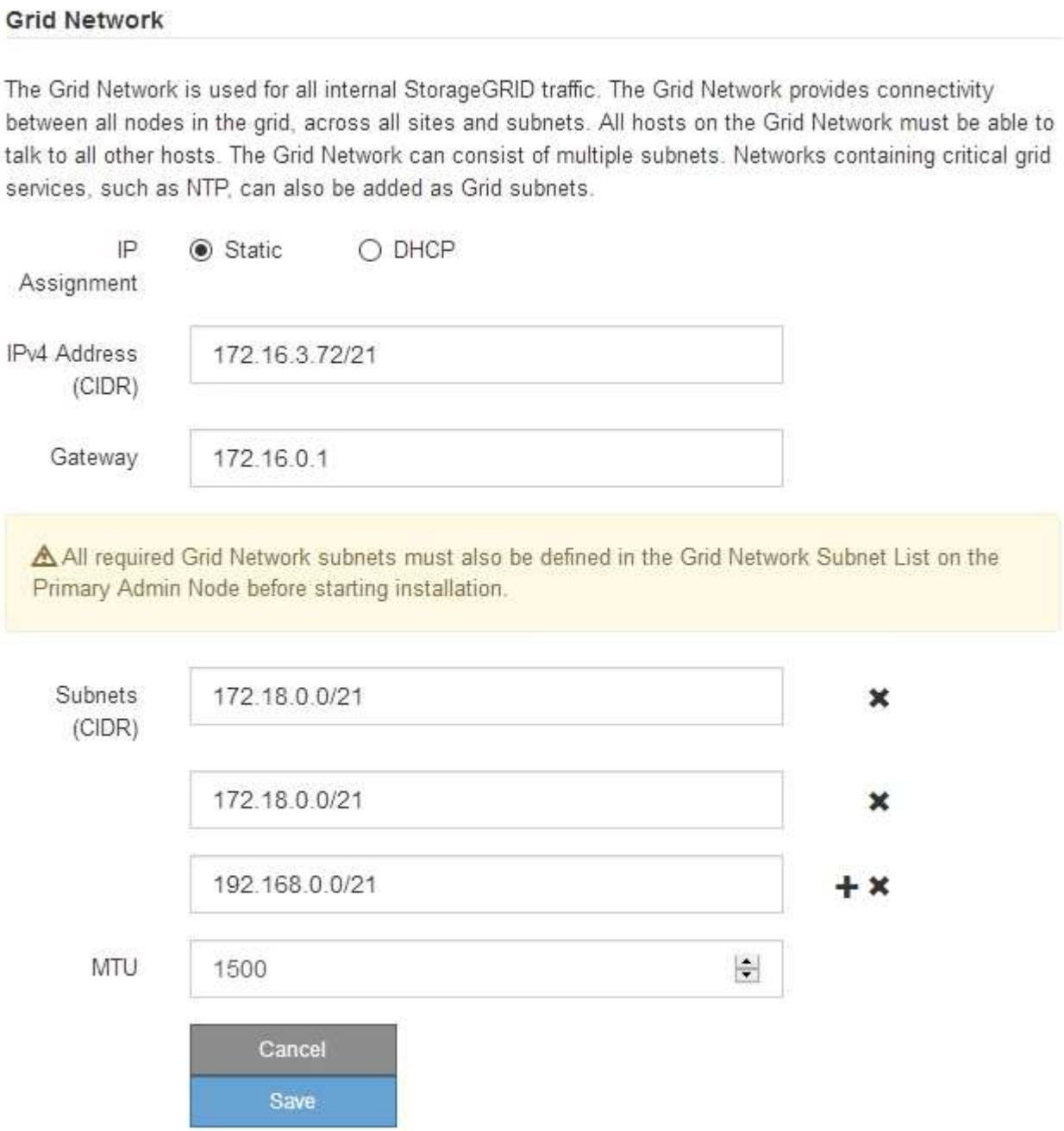
Si desea cambiar la configuración de vínculos, consulte Instrucciones para cambiar la configuración de enlace del controlador SG6000-CN.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Configurar redes** > **Configuración IP**.

   Aparece la página Configuración de IP.

2. Para configurar Grid Network, seleccione **Static** o **DHCP** en la sección **Grid Network** de la página.



3. Si ha seleccionado **estático**, siga estos pasos para configurar la red de cuadrícula:

a. Introduzca la dirección IPv4 estática utilizando la notación CIDR.

b. Introduzca la puerta de enlace.

   Si la red no tiene una puerta de enlace, vuelva a introducir la misma dirección IPv4 estática.

c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

   > 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. Los valores de MTU no tienen que ser iguales para todos los tipos de red.

d. Haga clic en **Guardar**.

   Al cambiar la dirección IP, la pasarela y la lista de subredes también pueden cambiar.

   Si pierde la conexión con el instalador de dispositivos StorageGRID, vuelva a introducir la URL con la nueva dirección IP estática que acaba de asignar. Por ejemplo, `https://services_appliance_IP:8443`

e. Confirme que la lista de subredes de red es correcta.

   Si tiene 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. Estas subredes de red de cuadrícula también deben definirse en la Lista de subredes de red de cuadrícula del nodo de administración principal al iniciar la instalación de StorageGRID.

   > La ruta predeterminada no aparece en la lista. Si la red de cliente no está activada, la ruta predeterminada utilizará la puerta de enlace de red de cuadrícula.

   - Para agregar una subred, haga clic en el icono de inserción + a la derecha de la última entrada.
   - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

f. Haga clic en **Guardar**.

4. Si ha seleccionado **DHCP**, siga estos pasos para configurar Grid Network:

   a. Después de seleccionar el botón de opción **DHCP**, haga clic en **Guardar**.

      Los campos **Dirección IPv4**, **Puerta de enlace** y **subredes** se rellenan automáticamente. Si el servidor DHCP está configurado para asignar un valor MTU, el campo **MTU** se rellena con ese valor y el campo pasa a ser de sólo lectura.

      El navegador web se redirige automáticamente a la nueva dirección IP para el instalador de dispositivos StorageGRID.

   b. Confirme que la lista de subredes de red es correcta.

Si tiene 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. Estas subredes de red de cuadrícula también deben definirse en la Lista de subredes de red de cuadrícula del nodo de administración principal al iniciar la instalación de StorageGRID.

> La ruta predeterminada no aparece en la lista. Si la red de cliente no está activada, la ruta predeterminada utilizará la puerta de enlace de red de cuadrícula.

- Para agregar una subred, haga clic en el icono de inserción + a la derecha de la última entrada.
- Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

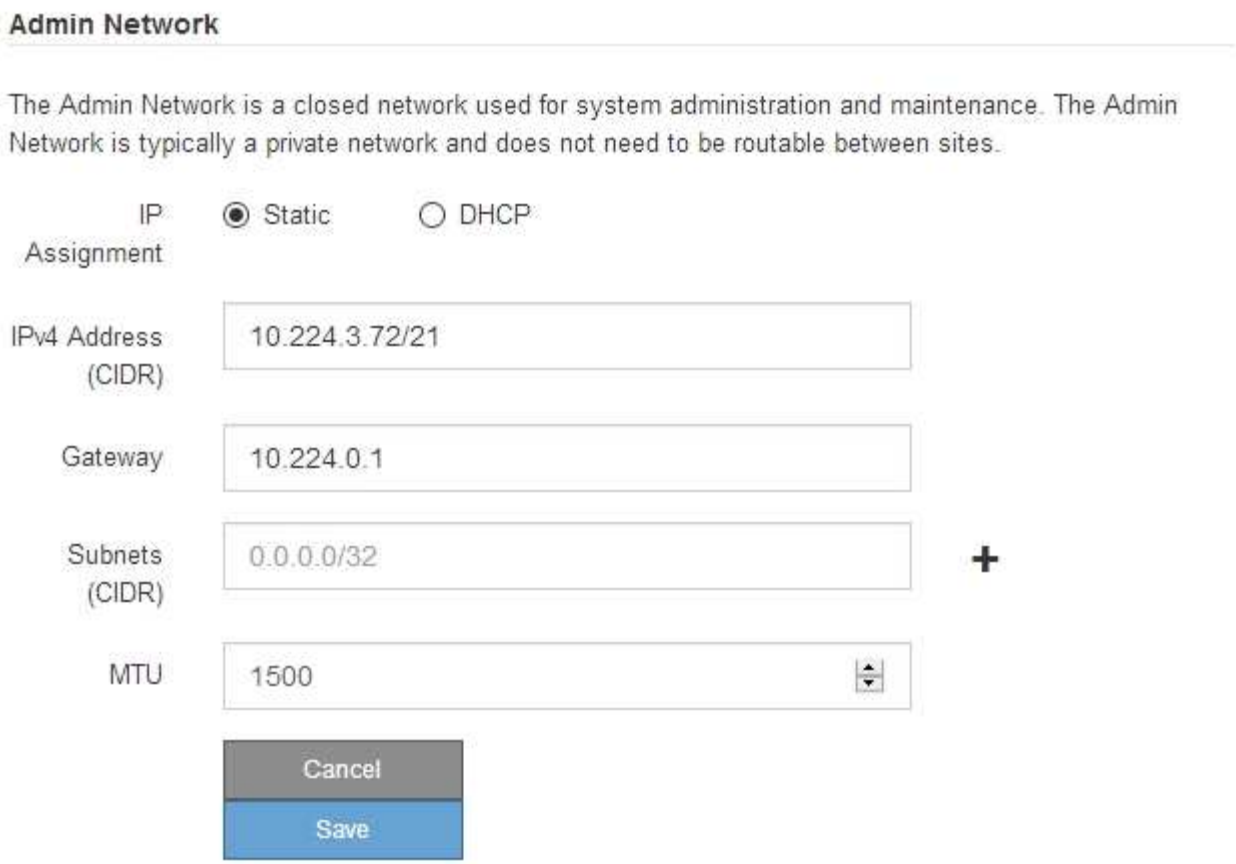
> El valor de MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, pueden ocurrir problemas de rendimiento de red o pérdida de paquetes.

> 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. Los valores de MTU no tienen que ser iguales para todos los tipos de red.

a. Haga clic en **Guardar**.

5. Para configurar la red administrativa, seleccione **Static** o **DHCP** en la sección **Admin Network** de la página.

> Para configurar la Red de administración, debe activar la Red de administración en la página Configuración de vínculos.



6. Si ha seleccionado **estático**, siga estos pasos para configurar la red de administración:
   a. Introduzca la dirección IPv4 estática, mediante la notación CIDR, para el puerto de gestión 1 del dispositivo.

      El puerto de gestión 1 está a la izquierda de los dos puertos RJ45 de 1-GbE del extremo derecho del dispositivo.

   b. Introduzca la puerta de enlace.

      Si la red no tiene una puerta de enlace, vuelva a introducir la misma dirección IPv4 estática.

   c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

      > 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.

   d. Haga clic en **Guardar**.

      Al cambiar la dirección IP, la pasarela y la lista de subredes también pueden cambiar.

      Si pierde la conexión con el instalador de dispositivos StorageGRID, vuelva a introducir la URL con la nueva dirección IP estática que acaba de asignar. Por ejemplo, `https://services_appliance:8443`

e. Confirme que la lista de subredes de la red administrativa es correcta.

   Debe verificar que se pueda acceder a todas las subredes mediante la puerta de enlace que ha proporcionado.

   > No se puede realizar la ruta predeterminada para utilizar la puerta de enlace de red de administración.

   - Para agregar una subred, haga clic en el icono de inserción ➕ a la derecha de la última entrada.
   - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

f. Haga clic en **Guardar**.

7. Si ha seleccionado **DHCP**, siga estos pasos para configurar la red de administración:

   a. Después de seleccionar el botón de opción **DHCP**, haga clic en **Guardar**.

      Los campos **Dirección IPv4**, **Puerta de enlace** y **subredes** se rellenan automáticamente. Si el servidor DHCP está configurado para asignar un valor MTU, el campo **MTU** se rellena con ese valor y el campo pasa a ser de sólo lectura.

      El navegador web se redirige automáticamente a la nueva dirección IP para el instalador de dispositivos StorageGRID.

   b. Confirme que la lista de subredes de la red administrativa es correcta.

      Debe verificar que se pueda acceder a todas las subredes mediante la puerta de enlace que ha proporcionado.

      > No se puede realizar la ruta predeterminada para utilizar la puerta de enlace de red de administración.

      - Para agregar una subred, haga clic en el icono de inserción ➕ a la derecha de la última entrada.
      - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

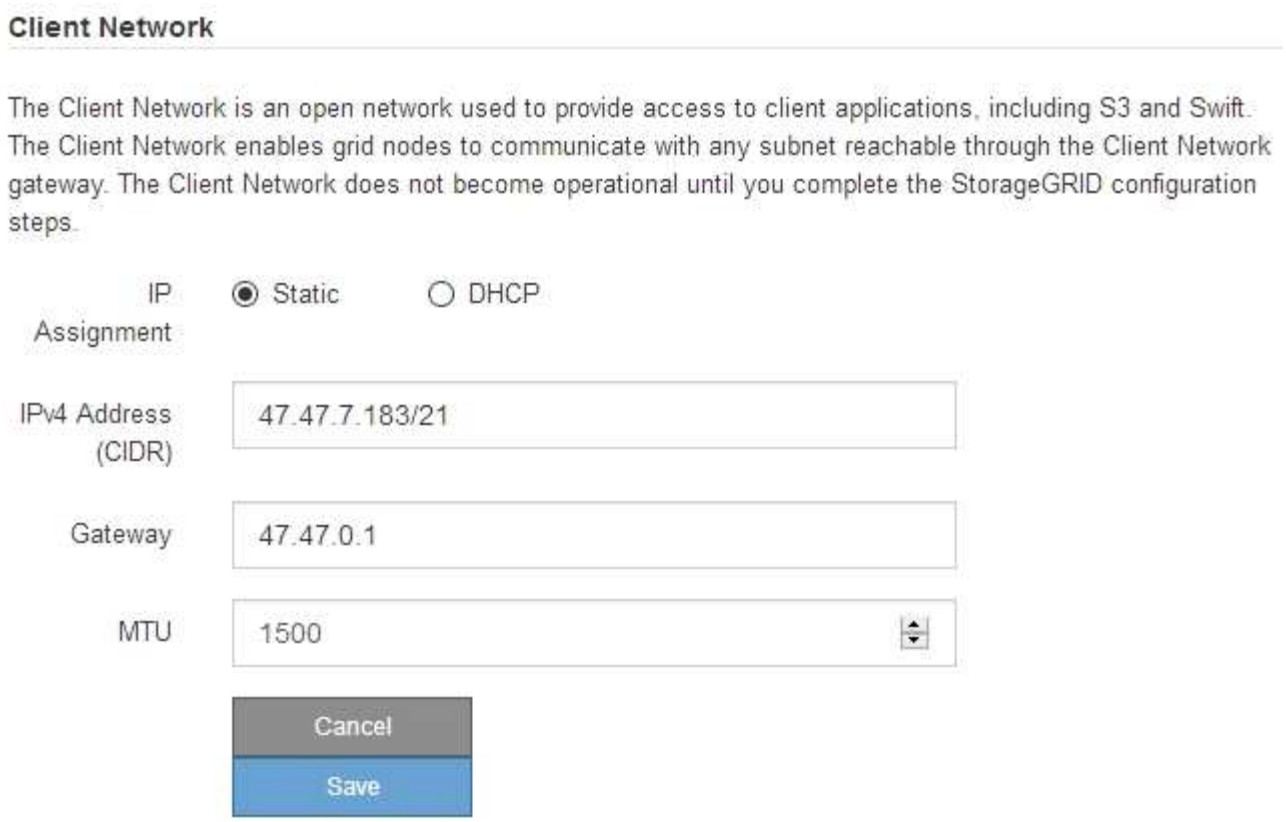
   c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

      > 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.

   d. Haga clic en **Guardar**.

8. Para configurar la red de cliente, seleccione **Static** o **DHCP** en la sección **Client Network** de la página.

   > Para configurar la red de cliente, debe activar la red de cliente en la página Configuración de vínculos.



9. Si ha seleccionado **estático**, siga estos pasos para configurar la red de cliente:
   a. Introduzca la dirección IPv4 estática utilizando la notación CIDR.
   b. Haga clic en **Guardar**.
   c. Confirme que la dirección IP de la puerta de enlace de red de cliente es correcta.

   > Si la red de cliente está activada, se muestra la ruta predeterminada. La ruta predeterminada utiliza la puerta de enlace de red de cliente y no se puede mover a otra interfaz mientras la red de cliente está activada.

   d. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

   > 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.

   e. Haga clic en **Guardar**.
10. Si ha seleccionado **DHCP**, siga estos pasos para configurar la red de cliente:
   a. Después de seleccionar el botón de opción **DHCP**, haga clic en **Guardar**.

   Los campos **Dirección IPv4** y **Puerta de enlace** se rellenan automáticamente. Si el servidor DHCP está configurado para asignar un valor MTU, el campo **MTU** se rellena con ese valor y el campo pasa a ser de sólo lectura.

El navegador web se redirige automáticamente a la nueva dirección IP para el instalador de dispositivos

StorageGRID.

a. Confirme que la puerta de enlace es correcta.

> Si la red de cliente está activada, se muestra la ruta predeterminada. La ruta predeterminada utiliza la puerta de enlace de red de cliente y no se puede mover a otra interfaz mientras la red de cliente está activada.

b. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

> 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.

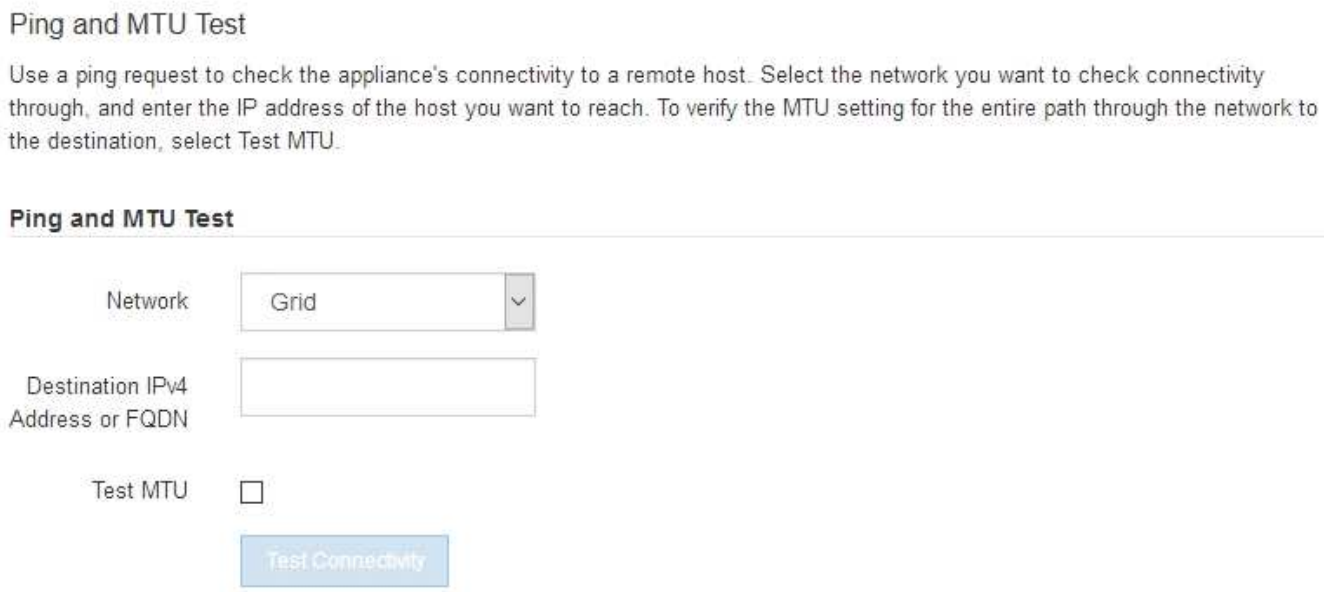
Compruebe las conexiones de red

Debe confirmar que puede acceder a las redes StorageGRID que está utilizando desde el dispositivo. Para validar el enrutamiento mediante puertas de enlace de red, debe probar la conectividad entre el instalador de dispositivos de StorageGRID y las direcciones IP en subredes diferentes. También puede verificar la configuración de MTU.

Pasos

1. En la barra de menús del instalador del dispositivo StorageGRID, haga clic en **Configurar redes** > **Ping y prueba de MTU**.

   Aparece la página pruebas de ping y MTU.



2. En el cuadro desplegable **Red**, seleccione la red que desea probar: Grid, Admin o Client.
3. Introduzca la dirección IPv4 o el nombre de dominio completo (FQDN) correspondiente a un host en esa red.

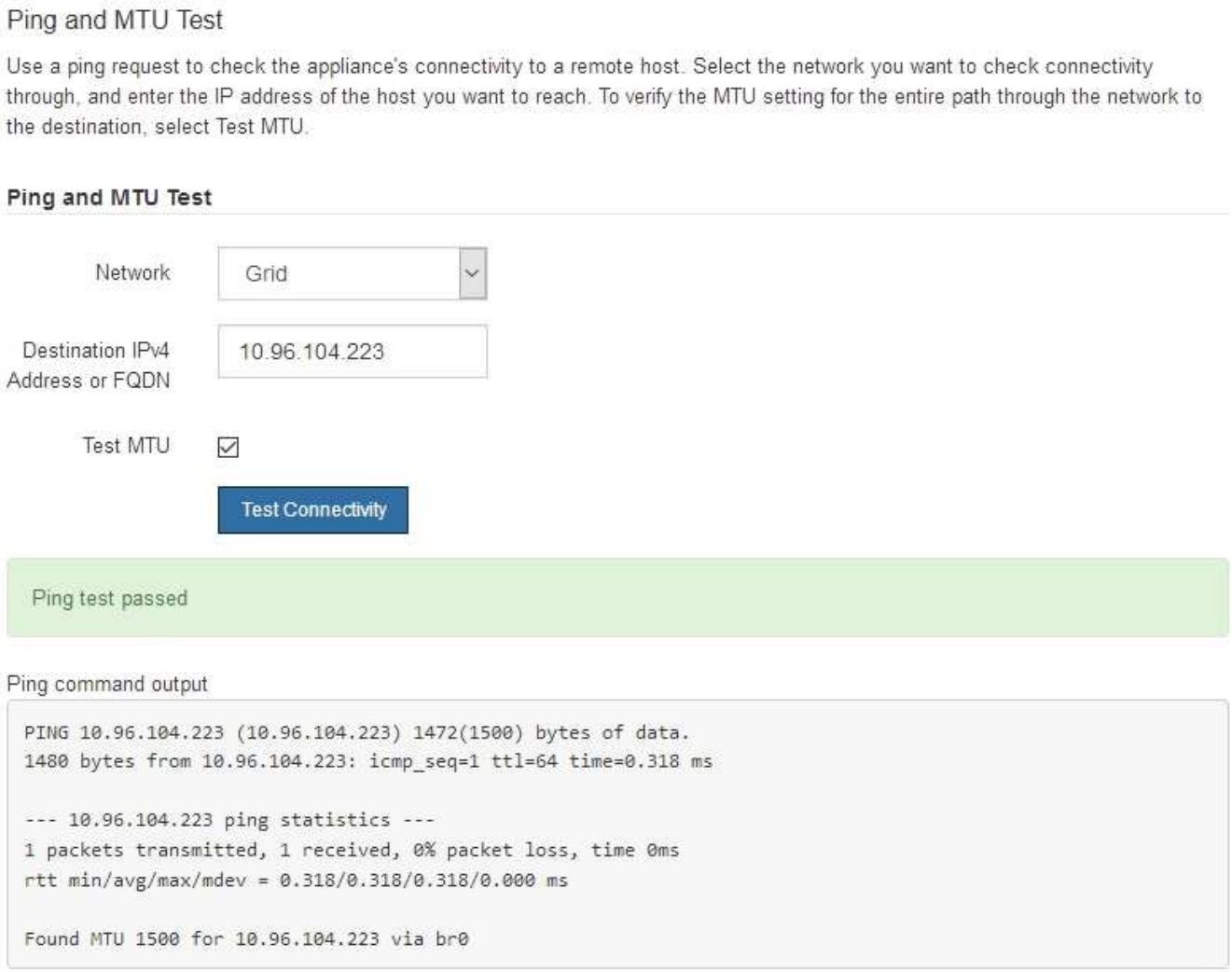
   Por ejemplo, puede hacer ping a la puerta de enlace de la red o al nodo de administración principal.

4. Opcionalmente, active la casilla de verificación **probar MTU** para comprobar la configuración de MTU para toda la ruta de acceso a través de la red hasta el destino.

   Por ejemplo, puede probar la ruta entre el nodo del dispositivo y un nodo en un sitio diferente.

5. Haga clic en **probar conectividad**.

   Si la conexión de red es válida, aparece el mensaje "Ping test pased", con la salida del comando ping en la lista.



Información relacionada

Configuración de enlaces de red (SG6000)

Cambie la configuración de MTU

Verifique las conexiones de red a nivel de puerto

Para garantizar que los firewalls no obstruyan el acceso entre el instalador del dispositivo StorageGRID y otros nodos, confirme que el instalador del dispositivo StorageGRID puede conectarse a un puerto TCP o a un conjunto de puertos en la dirección IP o el rango de direcciones especificados.

Acerca de esta tarea

Con la lista de puertos que se incluye en el instalador de dispositivos de StorageGRID, puede probar la conectividad entre el dispositivo y los demás nodos de la red de grid.

Además, puede probar la conectividad en las redes de administración y cliente y en los puertos UDP, como los que se utilizan para servidores NFS o DNS externos. Para obtener una lista de estos puertos, consulte la referencia de puertos en las directrices de red de StorageGRID.

> Los puertos de red de red enumerados en la tabla de conectividad de puertos sólo son válidos para StorageGRID versión 11.6.0. Para verificar qué puertos son correctos para cada tipo de nodo, siempre debe consultar las directrices de red para su versión de StorageGRID.

Pasos

1. En el instalador del dispositivo StorageGRID, haga clic en **Configurar red** > **Prueba de conectividad de puerto (nmap)**.

   Aparece la página Prueba de conectividad de puerto.

   La tabla de conectividad de puertos enumera los tipos de nodos que requieren conectividad TCP en la red de cuadrícula. Para cada tipo de nodo, la tabla enumera los puertos de red de cuadrícula a los que el dispositivo debe acceder.

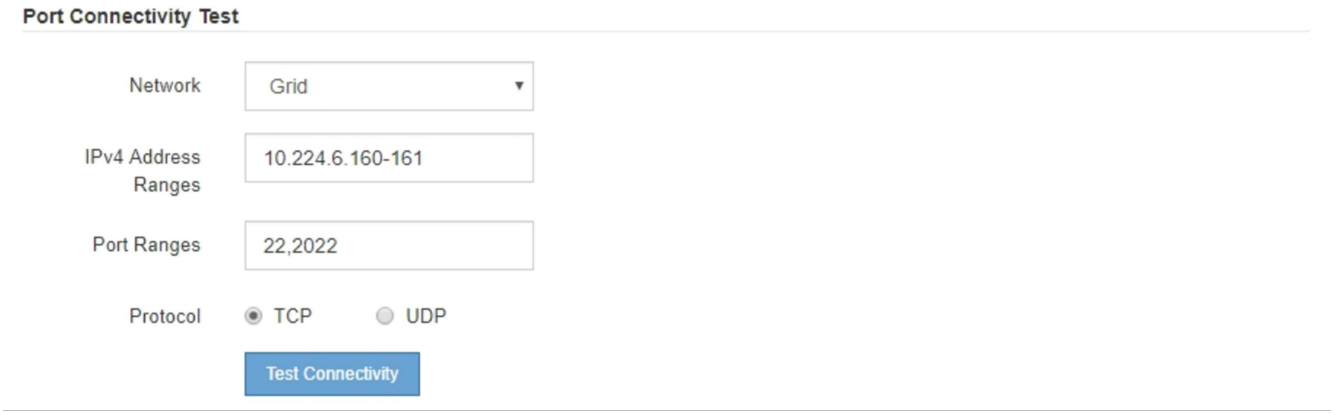
   Puede probar la conectividad entre los puertos del dispositivo que aparecen en la tabla y los demás nodos de la red de grid.

2. En el menú desplegable **Red**, seleccione la red que desea probar: **Grid**, **Admin** o **Cliente**.
3. Especifique un rango de direcciones IPv4 para los hosts en esa red.

   Por ejemplo, es posible que desee sondear la puerta de enlace en la red o en el nodo de administración principal.

   Especifique un rango utilizando un guión, como se muestra en el ejemplo.

4. Introduzca un número de puerto TCP, una lista de puertos separados por comas o un intervalo de puertos.



5. Haga clic en **probar conectividad**.

   - Si las conexiones de red a nivel de puerto seleccionadas son válidas, el mensaje "'Prueba de conectividad de puerto superada'" aparece en un banner verde. El resultado del comando nmap se muestra debajo del banner.

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- Si se realiza una conexión de red a nivel de puerto al host remoto, pero el host no escucha en uno o más de los puertos seleccionados, el mensaje "'error de prueba de conectividad de puerto'" aparece en un banner amarillo. El resultado del comando nmap se muestra debajo del banner.

  Cualquier puerto remoto al que no esté escuchando el host tiene un estado de "'cerrado'". Por ejemplo, puede ver este banner amarillo cuando el nodo al que intenta conectarse está en estado preinstalado y el servicio NMS de StorageGRID aún no se está ejecutando en ese nodo.

Port connectivity test failed
Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
1504/tcp closed evb-elm
1505/tcp open   funkproxy
1506/tcp open   utcd
1508/tcp open   diagmond
7443/tcp open   oracleas-https
9999/tcp open   abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- Si no se puede establecer una conexión de red a nivel de puerto para uno o más puertos seleccionados, el mensaje "'Port Connectivity test failed'" aparece en un banner rojo. El resultado del comando nmap se muestra debajo del banner.

  El banner rojo indica que se ha realizado un intento de conexión TCP a un puerto en el host remoto, pero no se ha devuelto nada al remitente. Cuando no se devuelve ninguna respuesta, el puerto tiene un estado de "filtrado" y es probable que sea bloqueado por un firewall.

  ⓘ También se enumeran los puertos con «'cerrado'».

Port connectivity test failed
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT     STATE    SERVICE
22/tcp   open     ssh
79/tcp   filtered finger
80/tcp   open     http
443/tcp  open     https
1504/tcp closed   evb-elm
1505/tcp open     funkproxy
1506/tcp open     utcd
1508/tcp open     diagmond
7443/tcp open     oracleas-https
9999/tcp open     abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

Información relacionada

Directrices sobre redes

Acceder y configurar SANtricity System Manager (SG6000)

Puede usar System Manager de SANtricity para supervisar el estado de las controladoras de almacenamiento, los discos de almacenamiento y otros componentes de hardware en la bandeja de controladoras de almacenamiento. También puede configurar un proxy para AutoSupport E-Series que permite enviar mensajes de AutoSupport desde el dispositivo sin utilizar el puerto de gestión.

Configuración y acceso a System Manager de SANtricity

Es posible que tenga que acceder a System Manager de SANtricity en la controladora de almacenamiento para supervisar el hardware de la bandeja de controladoras de almacenamiento o configurar AutoSupport de E-Series.

Lo que necesitará

- Está utilizando un navegador web compatible.
- Para acceder a SANtricity System Manager a través de Grid Manager, debe tener instalado StorageGRID, y debe tener el permiso de administrador de dispositivo de almacenamiento o de acceso raíz.
- Para acceder a System Manager de SANtricity mediante el instalador de dispositivos de StorageGRID, debe tener el nombre de usuario y la contraseña de administrador de SANtricity System Manager.
- Para acceder a SANtricity System Manager directamente mediante un explorador web, debe tener el nombre de usuario y la contraseña de administrador de SANtricity System Manager.

> Debe tener el firmware 8.70 (11.70) de SANtricity o superior para acceder a System Manager de SANtricity mediante Grid Manager o el instalador de dispositivos de StorageGRID. Puede comprobar su versión de firmware mediante el instalador del dispositivo StorageGRID y seleccionando **Ayuda** > **Acerca de**.

> Acceder a SANtricity System Manager desde Grid Manager o desde el instalador de dispositivos generalmente se realiza solo para supervisar el hardware y configurar E-Series AutoSupport. Muchas funciones y operaciones en SANtricity System Manager, como la actualización de firmware, no se aplican a la supervisión del dispositivo StorageGRID. Para evitar problemas, siga siempre las instrucciones de instalación y mantenimiento del hardware del dispositivo.

Acerca de esta tarea

Existen tres formas de acceder a System Manager de SANtricity, en función de la fase del proceso de instalación y configuración en la que se encuentre:

- Si el dispositivo aún no se ha puesto en marcha como nodo en su sistema StorageGRID, debe usar la pestaña Avanzada del instalador de dispositivos de StorageGRID.

  > Una vez que el nodo se pone en marcha, ya no podrá utilizar el instalador de dispositivos de StorageGRID para acceder a System Manager de SANtricity.

- Si el dispositivo se ha implementado como nodo en el sistema StorageGRID, use la pestaña SANtricity System Manager de la página Nodes de Grid Manager.
- Si no puede utilizar el instalador de dispositivos de StorageGRID o Grid Manager, puede acceder a SANtricity System Manager directamente mediante un explorador web conectado al puerto de gestión.

Este procedimiento incluye los pasos para su acceso inicial a System Manager de SANtricity. Si ya ha configurado SANtricity System Manager, vaya a la configure el paso de alertas de hardware.

> Utilizar Grid Manager o el instalador de dispositivos de StorageGRID le permite acceder a SANtricity System Manager sin necesidad de configurar ni conectar el puerto de gestión del dispositivo.

Utilice System Manager de SANtricity para supervisar lo siguiente:

- Datos de rendimiento como el rendimiento en cabinas de almacenamiento, la latencia de I/o, el uso de CPU y el rendimiento
- Estado de los componentes de hardware
- Entre las funciones de soporte se incluyen la visualización de datos de diagnóstico

Puede usar System Manager de SANtricity para configurar las siguientes opciones:

- Alertas por correo electrónico, alertas SNMP o alertas de syslog para los componentes de la bandeja de controladoras de almacenamiento
- Configuración de AutoSupport de E-Series para los componentes de la bandeja de la controladora de almacenamiento.

  Si quiere más información sobre E-Series AutoSupport, consulte "Sitio de documentación para sistemas E-Series y EF-Series de NetApp".

- Claves Drive Security, que se necesitan para desbloquear unidades seguras (este paso es necesario si la función Drive Security está habilitada)
- Contraseña de administrador para acceder a System Manager de SANtricity

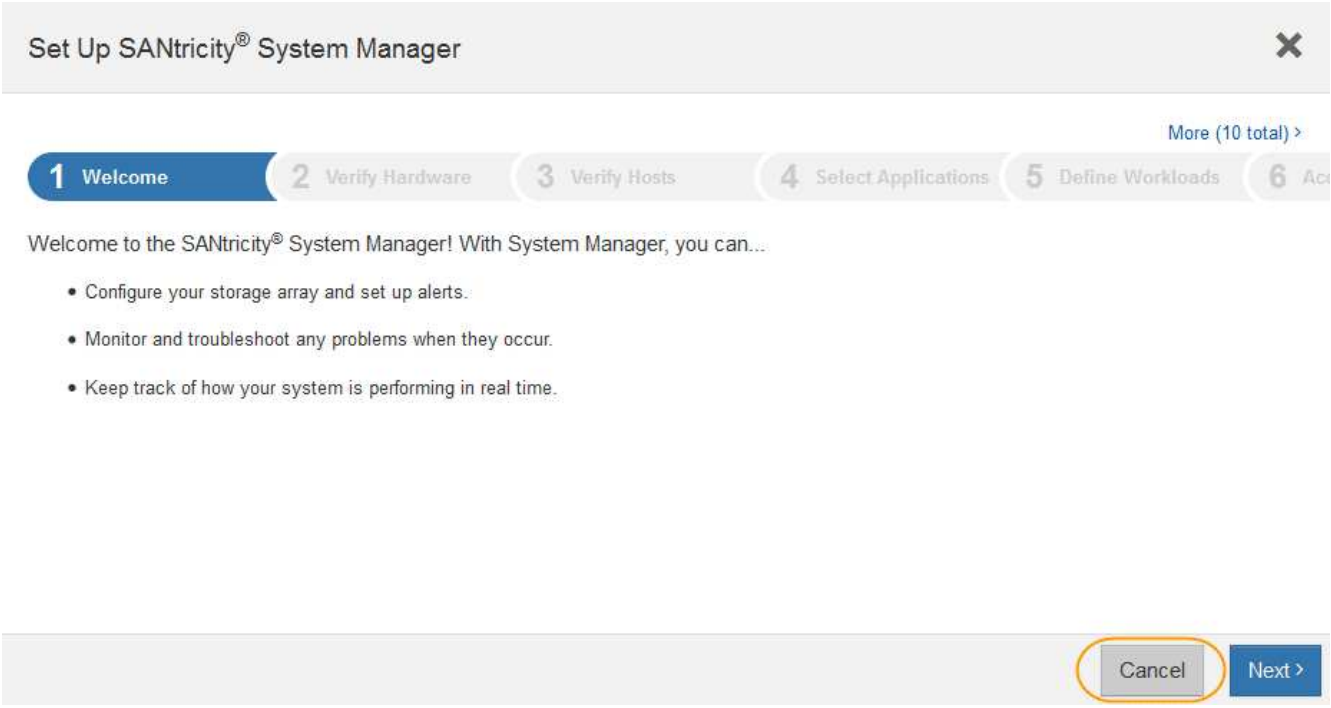
Pasos

1. Utilice el instalador del dispositivo StorageGRID y seleccione **Avanzado** > **Administrador del sistema SANtricity**

> Si el instalador de dispositivos StorageGRID no está disponible o no aparece la página de inicio de sesión, debe utilizar el Las direcciones IP para las controladoras de almacenamiento. Para acceder a SANtricity System Manager, vaya a la IP de la controladora de almacenamiento.

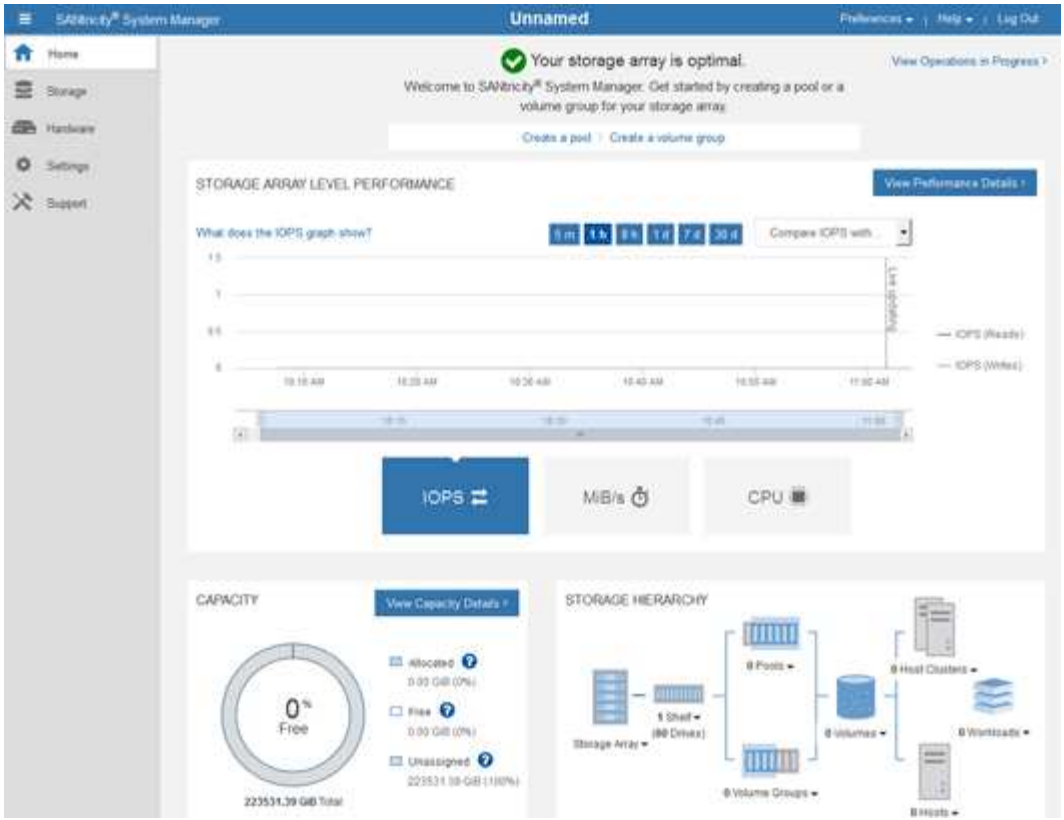
2. Defina o introduzca la contraseña del administrador.

   SANtricity System Manager utiliza una única contraseña de administrador que comparten todos los usuarios.



3. Seleccione **Cancelar** para cerrar el asistente.

> No complete el asistente de configuración de un dispositivo StorageGRID.



4. Configurar las alertas de hardware.
   a. Seleccione **Ayuda** para acceder a la ayuda en línea del Administrador del sistema de SANtricity.
   b. Utilice la sección **Configuración** > **Alertas** de la ayuda en línea para obtener información sobre las alertas.
   c. Siga las instrucciones de configuración para configurar alertas por correo electrónico, alertas SNMP o alertas syslog.
5. Gestione AutoSupport para los componentes de la bandeja de controladoras de almacenamiento.
   a. Seleccione **Ayuda** para acceder a la ayuda en línea del Administrador del sistema de SANtricity.
   b. Utilice la sección **SUPPORT** > **Support Center** de la ayuda en línea para obtener más información sobre la función AutoSupport.
   c. Siga las instrucciones «¿Cómo?» para gestionar AutoSupport.

      Para obtener instrucciones específicas sobre la configuración de un proxy StorageGRID para enviar mensajes de AutoSupport E-Series sin utilizar el puerto de gestión, vaya al instrucciones para configurar la configuración del proxy de almacenamiento.
6. Si la función Drive Security está habilitada para el dispositivo, cree y gestione la clave de seguridad.
   a. Seleccione **Ayuda** para acceder a la ayuda en línea del Administrador del sistema de SANtricity.
   b. Utilice la sección **Configuración** > **sistema** > **Gestión de claves de seguridad** de la ayuda en línea para obtener información sobre Drive Security.
   c. Siga las instrucciones de «Cómo» para crear y gestionar la clave de seguridad.
7. Si lo desea, puede cambiar la contraseña del administrador.
   a. Seleccione **Ayuda** para acceder a la ayuda en línea del Administrador del sistema de SANtricity.
   b. Utilice la sección **Inicio** > **Administración de matrices de almacenamiento** de la ayuda en línea

para obtener información sobre la contraseña de administrador.

c. Siga las instrucciones de "'Cómo'" para cambiar la contraseña.

Revisar el estado del hardware en System Manager de SANtricity

Puede usar System Manager de SANtricity para supervisar y gestionar componentes de hardware individuales de la bandeja de controladoras de almacenamiento y para revisar la información medioambiental y los diagnósticos de hardware, como la temperatura de los componentes, así como los problemas relacionados con las unidades.

Lo que necesitará

- Está utilizando un navegador web compatible.
- Para acceder a System Manager de SANtricity a través de Grid Manager, debe contar con permisos de administrador de dispositivos de almacenamiento o de acceso raíz.
- Para acceder a System Manager de SANtricity mediante el instalador de dispositivos de StorageGRID, debe tener el nombre de usuario y la contraseña de administrador de SANtricity System Manager.
- Para acceder a SANtricity System Manager directamente mediante un explorador web, debe tener el nombre de usuario y la contraseña de administrador de SANtricity System Manager.

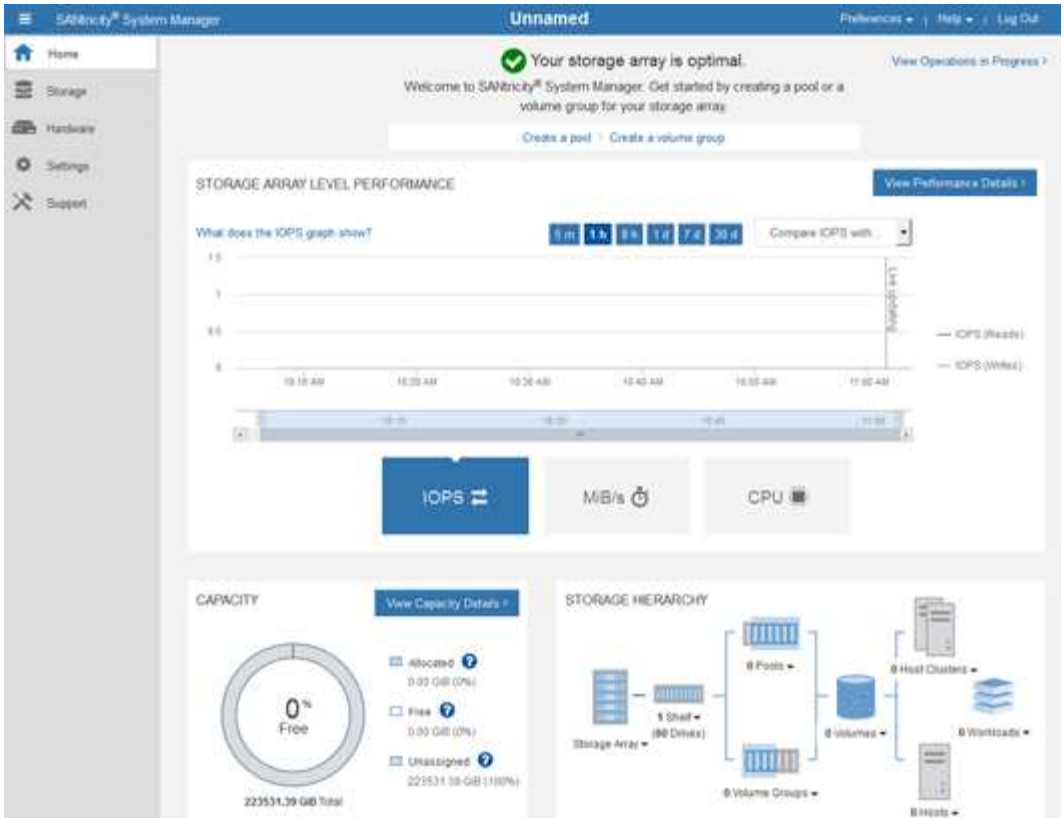
Debe tener el firmware 8.70 (11.70) de SANtricity o superior para acceder a System Manager de SANtricity mediante Grid Manager o el instalador de dispositivos de StorageGRID.

Acceder a SANtricity System Manager desde Grid Manager o desde el instalador de dispositivos generalmente se realiza solo para supervisar el hardware y configurar E-Series AutoSupport. Muchas funciones y operaciones en SANtricity System Manager, como la actualización de firmware, no se aplican a la supervisión del dispositivo StorageGRID. Para evitar problemas, siga siempre las instrucciones de instalación y mantenimiento del hardware del dispositivo.

Pasos

1. Acceda a SANtricity System Manager.
2. Introduzca el nombre de usuario y la contraseña del administrador si es necesario.
3. Haga clic en **Cancelar** para cerrar el asistente de configuración y mostrar la página de inicio del Administrador del sistema de SANtricity.

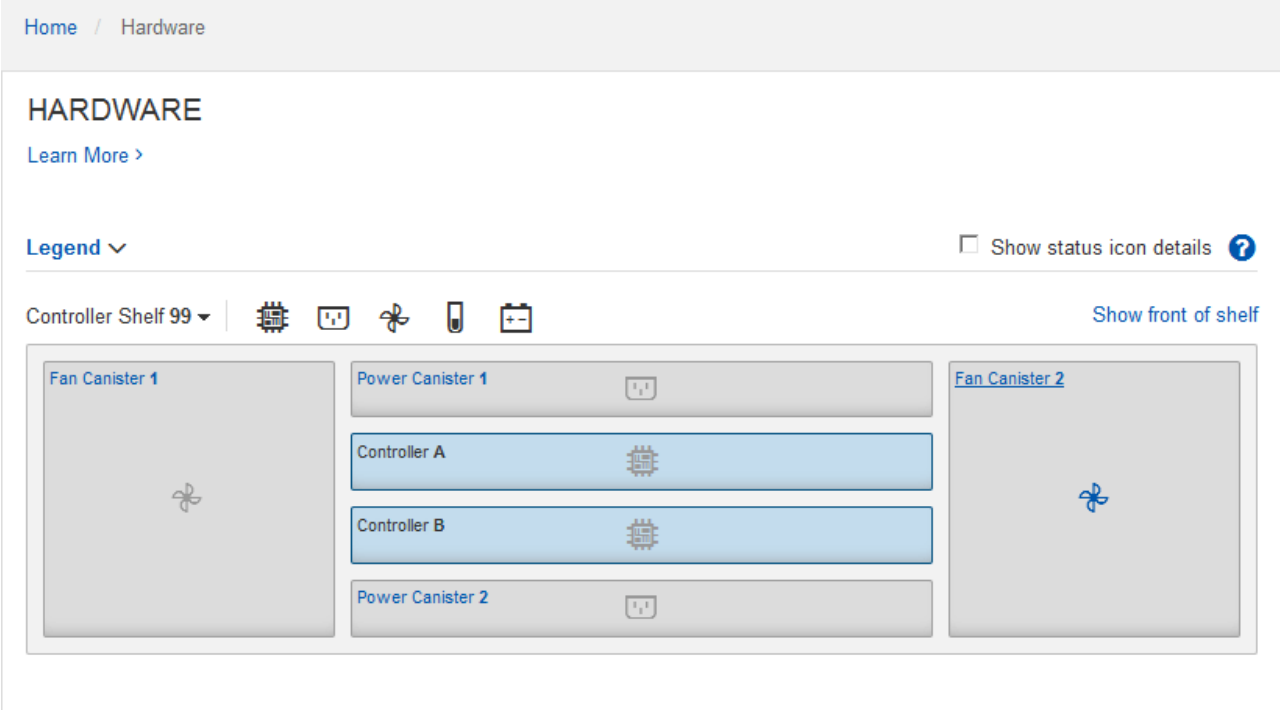
   Se mostrará la página de inicio de SANtricity System Manager. En SANtricity System Manager, la bandeja de controladoras se denomina cabina de almacenamiento.



4. Revise la información mostrada para el hardware del dispositivo y confirme que todos los componentes de hardware tienen un estado óptimo.

   a. Haga clic en la ficha **hardware**.

   b. Haga clic en **Mostrar parte posterior de la bandeja**.



Desde la parte posterior de la bandeja, puede ver ambas controladoras de almacenamiento, la batería de cada controladora de almacenamiento, los dos contenedores de alimentación, los dos compartimentos de

ventiladores y las bandejas de expansión (si los hubiera). También puede ver las temperaturas de los componentes.

a. Para ver los ajustes de cada controlador de almacenamiento, seleccione el controlador y seleccione **Ver ajustes** en el menú contextual.
b. Para ver la configuración de otros componentes de la parte posterior de la bandeja, seleccione el componente que desea ver.
c. Haga clic en **Mostrar frente de la bandeja** y seleccione el componente que desea ver.

   Desde el frente de la bandeja, es posible ver las unidades y los cajones de unidades de la bandeja de controladoras de almacenamiento o las bandejas de expansión (si las hubiera).

Si el estado de cualquier componente es necesita atención, siga los pasos de Recovery Guru para resolver el problema o póngase en contacto con el soporte técnico.

Establezca las direcciones IP para las controladoras de almacenamiento mediante el instalador de dispositivos de StorageGRID

El puerto de gestión 1 de cada controladora de almacenamiento conecta el dispositivo a la red de gestión para SANtricity System Manager. Si no puede acceder a System Manager de SANtricity desde el instalador de dispositivos StorageGRID, debe configurar una dirección IP estática para cada controladora de almacenamiento a fin de garantizar que no se pierda la conexión de gestión con el hardware y el firmware de la controladora en la bandeja de controladoras.

Lo que necesitará

- Está utilizando cualquier cliente de gestión que pueda conectarse a la red de administración de StorageGRID o que tenga un portátil de servicio.
- El cliente o el portátil de servicio tienen un navegador web compatible.

Acerca de esta tarea

Las direcciones asignadas por DHCP pueden cambiar en cualquier momento. Asigne direcciones IP estáticas a las controladoras para garantizar una accesibilidad constante.

> Siga este procedimiento sólo si no tiene acceso al Administrador del sistema SANtricity desde el instalador del dispositivo StorageGRID (**Avanzado** > **Administrador del sistema SANtricity**) o el Administrador de grid (**NODOS** > **Administrador del sistema SANtricity**).

Pasos

1. Desde el cliente, introduzca la URL del instalador de dispositivos de StorageGRID:
   `https://`*`Appliance_Controller_IP`*`:8443`

   Para *`Appliance_Controller_IP`*, Utilice la dirección IP del dispositivo en cualquier red StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Configurar hardware** > **Configuración de red del controlador de almacenamiento**.

   Aparece la página Storage Controller Network Configuration.

3. En función de la configuración de la red, seleccione **habilitado** para IPv4, IPv6 o ambos.
4. Anote la dirección IPv4 que se muestra automáticamente.

   DHCP es el método predeterminado para asignar una dirección IP al puerto de gestión de la controladora de almacenamiento.

   > Puede que los valores de DHCP deban tardar varios minutos en aparecer.

5. De manera opcional, configurar una dirección IP estática para el puerto de gestión de la controladora de almacenamiento.

   > Debe asignar una IP estática al puerto de gestión o una concesión permanente para la dirección en el servidor DHCP.

   a. Seleccione **estático**.
   b. Introduzca la dirección IPv4 mediante la notación CIDR.
   c. Introduzca la pasarela predeterminada.

   d. Haga clic en **Guardar**.

      Puede que los cambios se apliquen en unos minutos.

   Cuando se conecta a SANtricity System Manager, utilizará la nueva dirección IP estática como la URL: `https://Storage_Controller_IP`

Configurar la interfaz de BMC (SG6000)

La interfaz de usuario del controlador de administración de la placa base (BMC) del controlador SG6000-CN proporciona información de estado sobre el hardware y permite configurar los ajustes SNMP y otras opciones para el controlador SG6000-CN.

Cambie la contraseña raíz de la interfaz de BMC

Por motivos de seguridad, debe cambiar la contraseña del usuario raíz del BMC.

Lo que necesitará

- El cliente de gestión está usando un navegador web compatible.

Acerca de esta tarea

Al instalar el dispositivo por primera vez, el BMC utiliza una contraseña predeterminada para el usuario raíz (`root/calvin`). Debe cambiar la contraseña del usuario raíz para proteger el sistema.

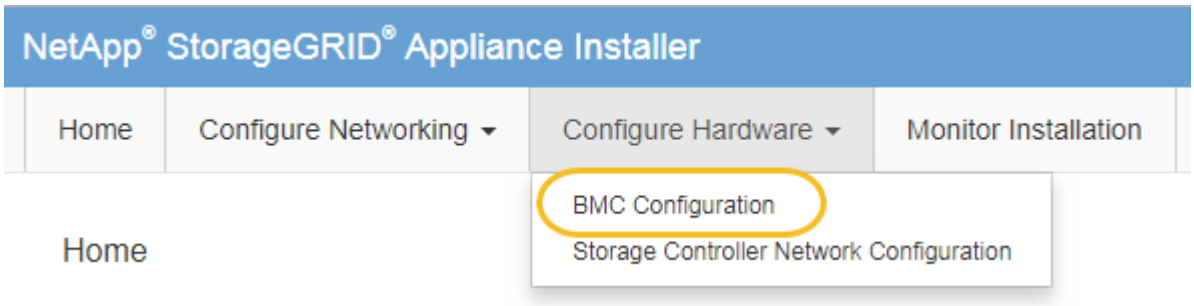
Pasos

1. Desde el cliente, introduzca la URL del instalador de dispositivos de StorageGRID: **`https://Appliance_Controller_IP:8443`**

   Para *`Appliance_Controller_IP`*, Utilice la dirección IP del dispositivo en cualquier red StorageGRID.

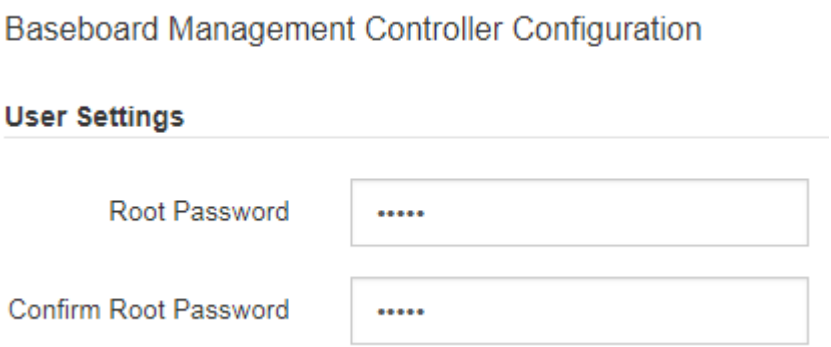
   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Configurar hardware Configuración de BMC**.



   Aparece la página Configuración de la controladora de gestión de placa base.

3. Introduzca una nueva contraseña para la cuenta raíz en los dos campos proporcionados.



4. Haga clic en **Guardar**.

Establezca la dirección IP para el puerto de administración de BMC

Para poder acceder a la interfaz del BMC, debe configurar la dirección IP del puerto de administración del BMC en el controlador SG6000-CN.

Lo que necesitará

- El cliente de gestión está usando un navegador web compatible.
- Está usando cualquier cliente de gestión que pueda conectarse a una red StorageGRID.
- El puerto de gestión del BMC está conectado a la red de gestión que tiene previsto utilizar.

Acerca de esta tarea

Para fines de soporte, el puerto de gestión del BMC permite un acceso bajo al hardware.

> Solo debe conectar este puerto a una red de gestión interna segura y de confianza. Si no hay ninguna red disponible, deje el puerto BMC desconectado o bloqueado, a menos que el soporte técnico solicite una conexión a BMC.

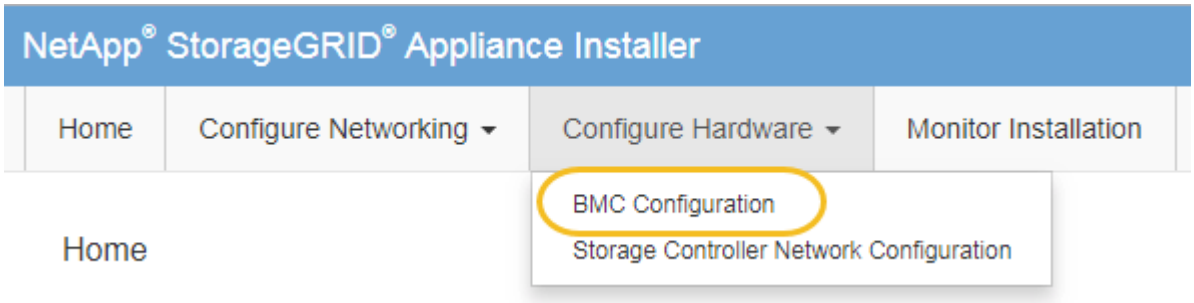
Pasos

1. Desde el cliente, introduzca la URL del instalador de dispositivos de StorageGRID:
   `https://`*`SG6000-CN_Controller_IP`*`:8443`

   Para `SG6000-CN_Controller_IP`, Utilice la dirección IP del dispositivo en cualquier red StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Configurar hardware Configuración de BMC**.

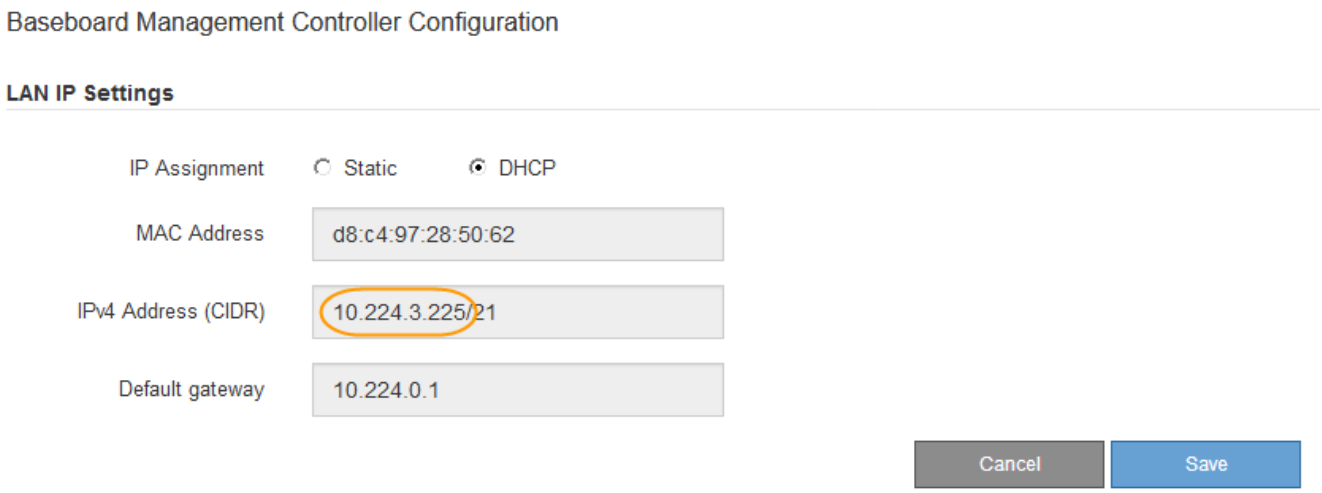


   Aparece la página Configuración de la controladora de gestión de placa base.

3. Anote la dirección IPv4 que se muestra automáticamente.

   DHCP es el método predeterminado para asignar una dirección IP a este puerto.

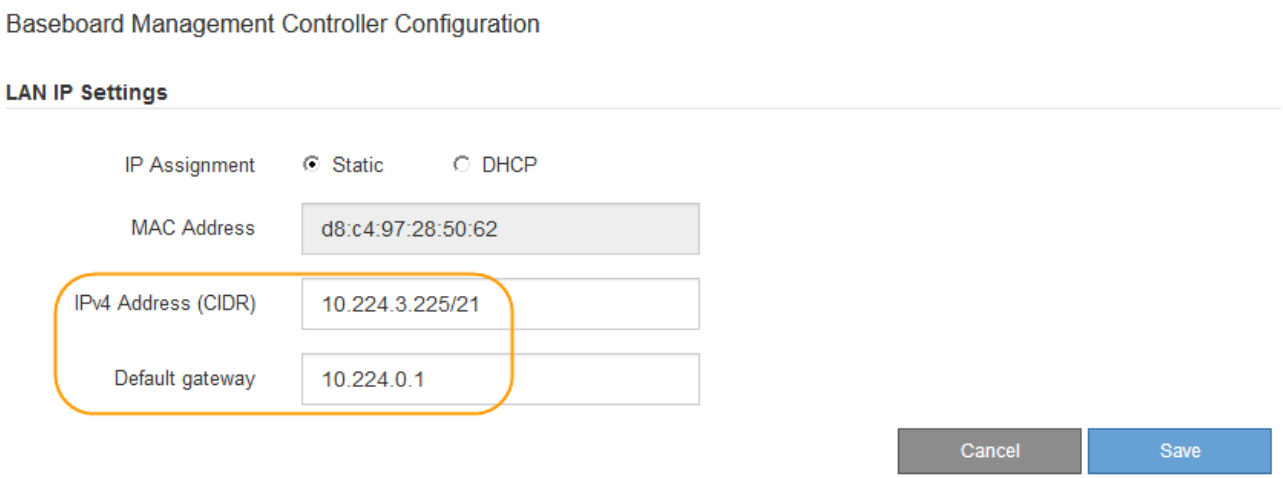
   > Puede que los valores de DHCP deban tardar varios minutos en aparecer.



4. De manera opcional, establezca una dirección IP estática para el puerto de gestión del BMC.

> Debe asignar una IP estática al puerto de gestión de BMC o una concesión permanente para la dirección en el servidor DHCP.

a. Seleccione **estático**.
b. Introduzca la dirección IPv4 mediante la notación CIDR.
c. Introduzca la pasarela predeterminada.



d. Haga clic en **Guardar**.

   Puede que los cambios se apliquen en unos minutos.

Acceda a la interfaz de BMC

Puede acceder a la interfaz del BMC en el controlador SG6000-CN utilizando la dirección DHCP o IP estática para el puerto de administración del BMC.

Lo que necesitará

- El puerto de administración de BMC del controlador SG6000-CN está conectado a la red de administración que se va a utilizar.

- El cliente de gestión está usando un navegador web compatible.

Pasos

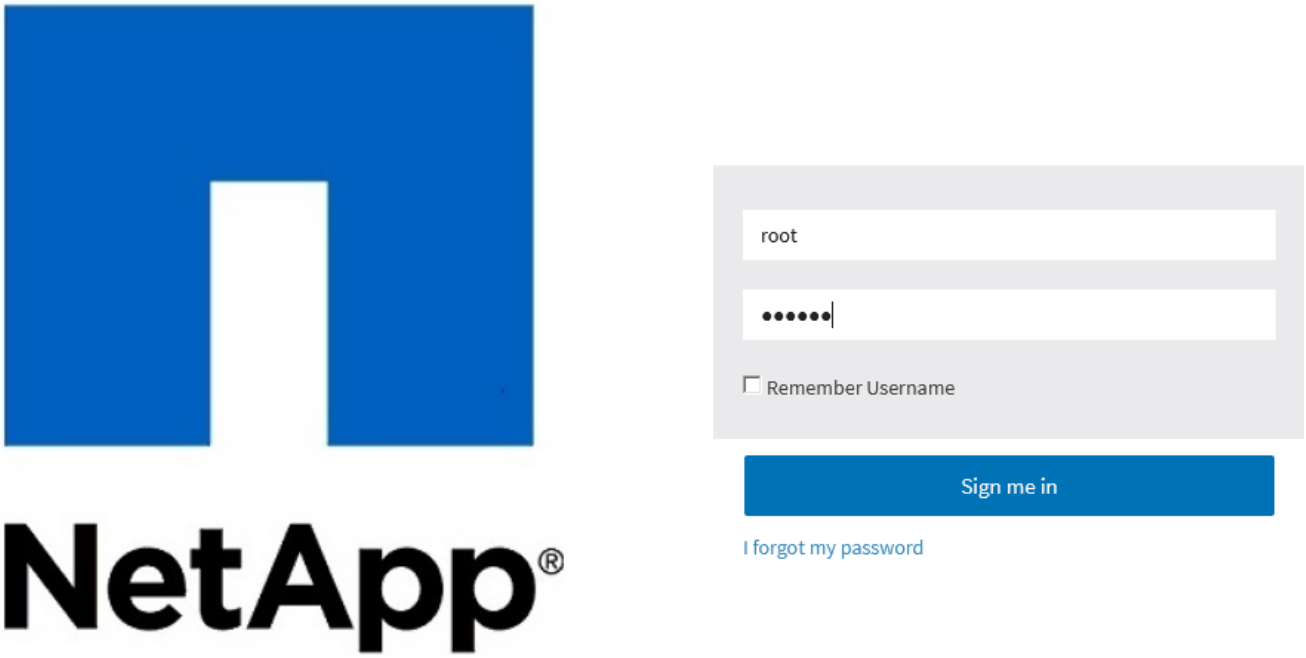
1. Introduzca la dirección URL de la interfaz del BMC:
   `https://BMC_Port_IP`

   Para *`BMC_Port_IP`*, Utilice la dirección IP estática o DHCP para el puerto de administración del BMC.

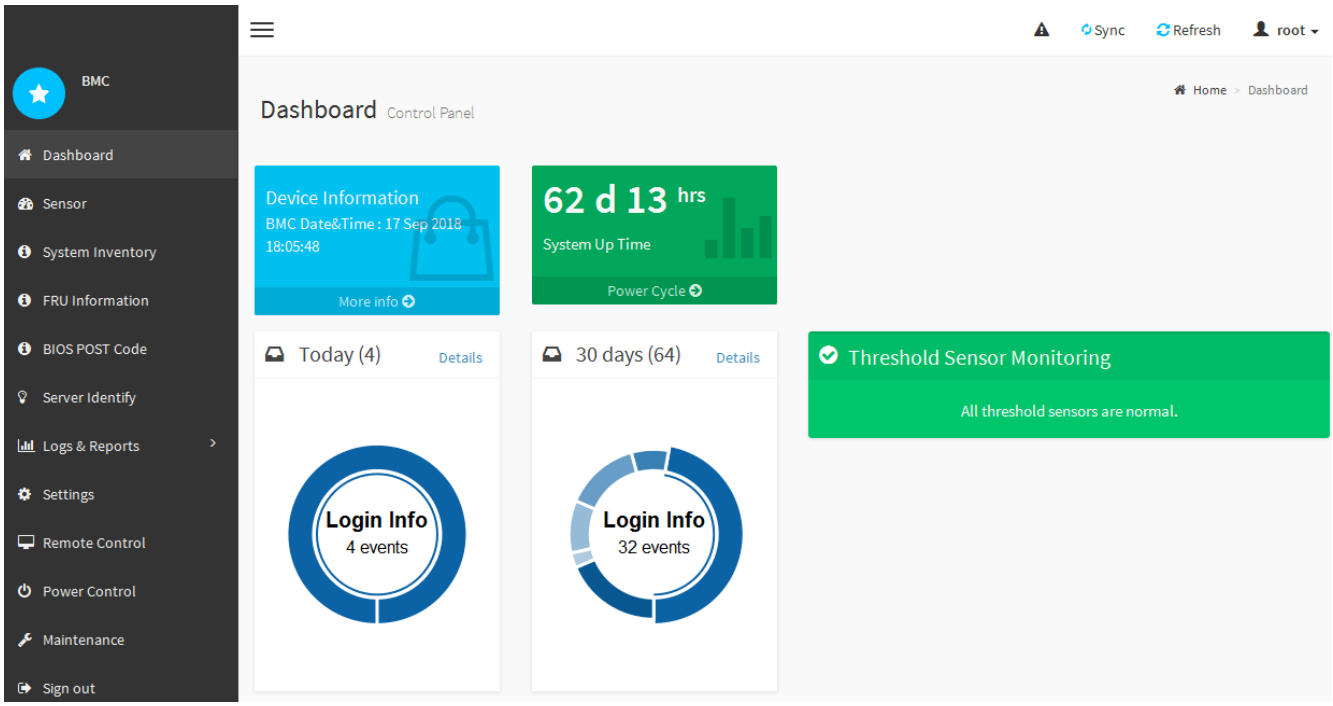
   Aparece la página de inicio de sesión de BMC.

   > Si aún no ha configurado `BMC_Port_IP`, siga las instrucciones de Configurar la interfaz de BMC (SG6000). Si no puede seguir este procedimiento debido a un problema de hardware y aún no ha configurado una dirección IP de BMC, es posible que aún pueda acceder al BMC. De forma predeterminada, el BMC obtiene una dirección IP mediante DHCP. Si DHCP está activado en la red BMC, el administrador de red puede proporcionar la dirección IP asignada al BMC MAC, que se imprime en la etiqueta situada en la parte frontal del controlador SG6000-CN. Si DHCP no está habilitado en la red BMC, el BMC no responderá después de unos minutos y se asignará la IP estática predeterminada `192.168.0.120`. Es posible que necesite conectar su portátil directamente al puerto BMC y cambiar la configuración de red para asignar una IP a su portátil `192.168.0.200/24`, para navegar a. `192.168.0.120`.

2. Introduzca el nombre de usuario y la contraseña de raíz con la contraseña que estableció al usuario se ha cambiado la contraseña raíz predeterminada:



3. Seleccione **Iniciar sesión**.



4. Opcionalmente, cree usuarios adicionales seleccionando **Ajustes Gestión de usuarios** y haciendo clic en cualquier usuario "desactivado".

> Cuando los usuarios inician sesión por primera vez, es posible que se les pida que cambien su contraseña para aumentar la seguridad.

Configurar los ajustes SNMP para el controlador SG6000-CN

Si está familiarizado con la configuración de SNMP para el hardware, puede utilizar la interfaz BMC para configurar los ajustes SNMP para el controlador SG6000-CN. Puede proporcionar cadenas de comunidad seguras, habilitar capturas SNMP y especificar hasta cinco destinos SNMP.

Lo que necesitará

- Sabe cómo acceder al panel de BMC.
- Tiene experiencia en la configuración de la configuración de SNMP para el equipo SNMPv1-v2c.

> Es posible que los ajustes de BMC realizados por este procedimiento no se conserven si el SG6000-CN falla y se tiene que sustituir. Asegúrese de que tiene un registro de todos los ajustes que ha aplicado, para que se puedan volver a aplicar fácilmente después de reemplazar el hardware si es necesario.

Pasos

1. En el panel del BMC, seleccione **Ajustes Ajustes SNMP**.
2. En la página SNMP Settings (Configuración SNMP), seleccione **Enable SNMP V1/V2** (Activar SNMP V1/V2*) y, a continuación, proporcione una cadena de comunidad de sólo lectura y una cadena de comunidad de lectura y escritura.

   La cadena de comunidad de sólo lectura es como un ID de usuario o una contraseña. Debe cambiar este valor para evitar que los intrusos obtengan información acerca de la configuración de la red. La cadena de

comunidad de lectura y escritura protege el dispositivo contra cambios no autorizados.

3. Opcionalmente, seleccione **Activar solapamiento** e introduzca la información necesaria.

> Introduzca la IP de destino para cada captura SNMP mediante una dirección IP. No se admiten los nombres de dominio completos.

Habilite las capturas si desea que el controlador SG6000-CN envíe notificaciones inmediatas a una consola SNMP cuando se encuentre en un estado inusual. Los traps pueden indicar que se han superado los fallos de hardware de varios componentes o umbrales de temperatura.

4. Opcionalmente, haga clic en **Enviar captura de prueba** para probar la configuración.
5. Si la configuración es correcta, haga clic en **Guardar**.

Configure notificaciones por correo electrónico para las alertas

Si desea que las notificaciones de correo electrónico se envíen cuando se produzcan alertas, debe utilizar la interfaz de BMC para configurar las opciones SMTP, los usuarios, los destinos LAN, las directivas de alerta y los filtros de eventos.

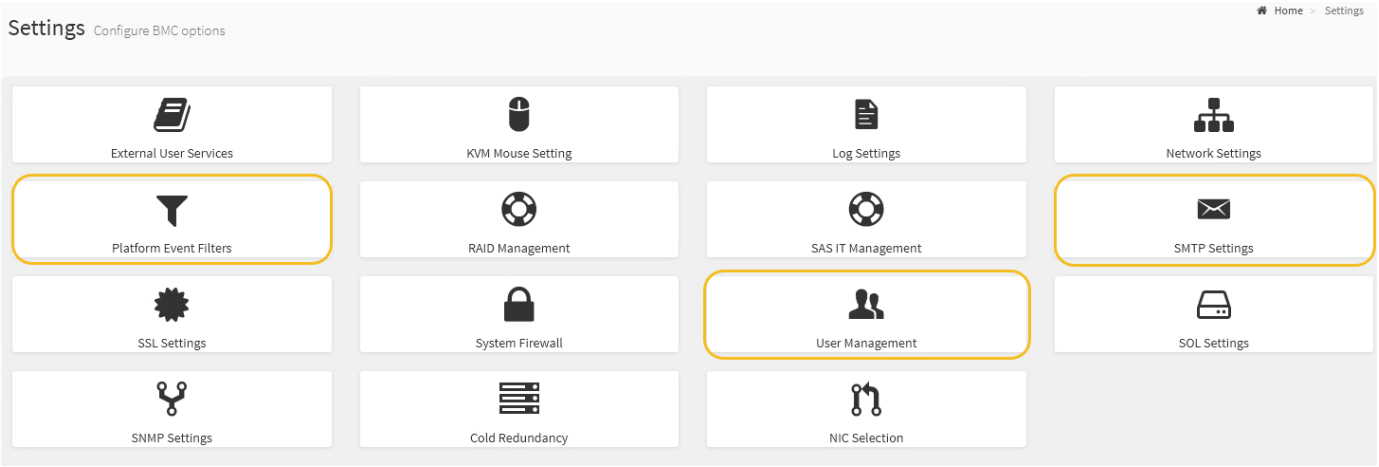
> Es posible que los ajustes de BMC realizados por este procedimiento no se conserven si el SG6000-CN falla y se tiene que sustituir. Asegúrese de que tiene un registro de todos los ajustes que ha aplicado, para que se puedan volver a aplicar fácilmente después de reemplazar el hardware si es necesario.

Lo que necesitará

Sabe cómo acceder al panel de BMC.

Acerca de esta tarea

En la interfaz del BMC, utilice las opciones **Configuración SMTP**, **Administración de usuarios** y **Filtros de sucesos de plataforma** de la página Configuración para configurar notificaciones por correo electrónico.



Pasos

1. Configure los ajustes de SMTP.
   a. Seleccione **Ajustes Ajustes SMTP**.
   b. Para el ID de correo electrónico del remitente, introduzca una dirección de correo electrónico válida.

Esta dirección de correo electrónico se proporciona como dirección de origen cuando el BMC envía correo electrónico.

2. Configurar los usuarios para que reciban alertas.
   a. En el panel de control del BMC, seleccione **Configuración Administración de usuarios**.
   b. Añada al menos un usuario para recibir notificaciones de alerta.

      La dirección de correo electrónico que configure para un usuario es la dirección a la que el BMC envía notificaciones de alerta. Por ejemplo, puede agregar un usuario genérico, como «'usuario de notificación'» y utilizar la dirección de correo electrónico de una lista de distribución de correo electrónico del equipo de soporte técnico.

3. Configure el destino de LAN para las alertas.
   a. Seleccione **Ajustes Filtros de sucesos de plataforma Destinos LAN**.
   b. Configure al menos un destino de LAN.
      - Seleccione **correo electrónico** como tipo de destino.
      - En Nombre de usuario de BMC, seleccione un nombre de usuario que haya añadido anteriormente.
      - Si agregó varios usuarios y desea que todos reciban mensajes de correo electrónico de notificación, debe agregar un destino LAN para cada usuario.
   c. Envía una alerta de prueba.
4. Configurar directivas de alerta para poder definir cuándo y dónde envía alertas el BMC.
   a. Seleccione **Configuración Filtros de sucesos de plataforma Directivas de alerta**.
   b. Configure al menos una directiva de alerta para cada destino de LAN.
      - Para número de grupo de directivas, seleccione **1**.
      - Para Acción de directiva, seleccione **siempre enviar alerta a este destino**.
      - Para el canal LAN, seleccione **1**.
      - En el Selector de destinos, seleccione el destino LAN de la directiva.
5. Configurar filtros de eventos para dirigir las alertas de diferentes tipos de eventos a los usuarios correspondientes.
   a. Seleccione **Ajustes Filtros de sucesos de plataforma Filtros de sucesos**.
   b. Para el número de grupo de políticas de alerta, introduzca **1**.
   c. Cree filtros para cada evento del que desee que se notifique al grupo de directivas de alerta.
      - Puede crear filtros de eventos para acciones de alimentación, eventos de sensor específicos o todos los eventos.
      - Si no está seguro de qué eventos debe supervisar, seleccione **todos los sensores** para el tipo de sensor y **todos los eventos** para las opciones de evento. Si recibe notificaciones no deseadas, puede cambiar sus selecciones más adelante.

Opcional: Habilite el cifrado de nodos

Si habilita el cifrado de nodos, los discos del dispositivo pueden protegerse mediante el cifrado del servidor de gestión de claves seguro (KMS) contra la pérdida física o la eliminación del sitio. Debe seleccionar y habilitar el cifrado de nodos durante la

instalación del dispositivo y no puede anular la selección del cifrado de nodos una vez que se inicia el proceso de cifrado KMS.

Lo que necesitará

Revise la información sobre KMS en las instrucciones para administrar StorageGRID.

Acerca de esta tarea

Un dispositivo con el cifrado de nodos habilitado se conecta al servidor de gestión de claves (KMS) externo que está configurado para el sitio StorageGRID. Cada KMS (o clúster KMS) administra las claves de cifrado de todos los nodos de dispositivos del sitio. Estas claves cifran y descifran los datos de cada disco de un dispositivo que tiene habilitado el cifrado de nodos.

Se puede configurar un KMS en Grid Manager antes o después de instalar el dispositivo en StorageGRID. Consulte la información sobre la configuración de KMS y del dispositivo en las instrucciones para administrar StorageGRID para obtener más detalles.

- Si se configura un KMS antes de instalar el dispositivo, el cifrado controlado por KMS comienza cuando se habilita el cifrado de nodos en el dispositivo y se lo agrega a un sitio StorageGRID donde se configura KMS.
- Si no se configura un KMS antes de instalar el dispositivo, el cifrado controlado por KMS se lleva a cabo en cada dispositivo que tenga activado el cifrado de nodos en cuanto se configure un KMS y esté disponible para el sitio que contiene el nodo del dispositivo.

> Los datos que existen antes de conectarse al KMS en un dispositivo con el cifrado de nodos habilitado se cifran con una clave temporal que no es segura. El dispositivo no está protegido de la retirada o robo hasta que la clave se configure en un valor proporcionado por el KMS.

Sin la clave KMS necesaria para descifrar el disco, los datos del dispositivo no se pueden recuperar y se pierden de forma efectiva. Este es el caso siempre que la clave de descifrado no se pueda recuperar del KMS. La clave se vuelve inaccesible si elimina la configuración de KMS, caduca una clave KMS, se pierde la conexión con el KMS o se elimina el dispositivo del sistema StorageGRID donde están instaladas sus claves KMS.

Pasos

1. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.

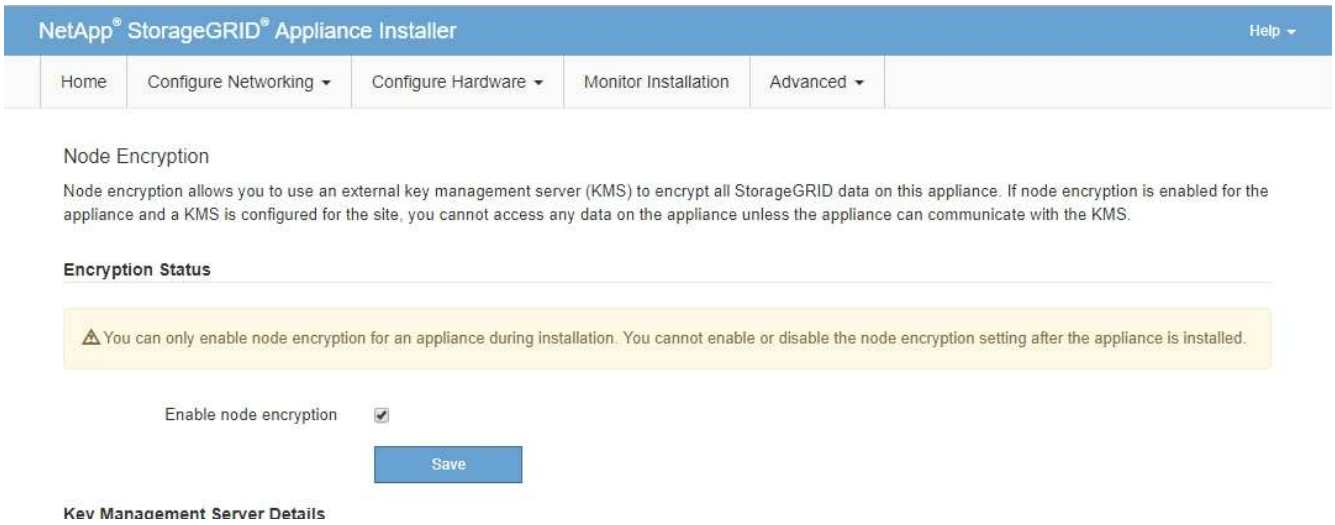
   `https://`*`Controller_IP`*`:8443`

   `Controller_IP` Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

   > Una vez que el dispositivo se ha cifrado con una clave KMS, los discos del dispositivo no se pueden descifrar sin utilizar la misma clave KMS.

2. Seleccione **Configurar hardware** > **cifrado de nodos**.



3. Seleccione **Activar cifrado de nodo**.

   Antes de instalar el dispositivo, puede anular la selección **Activar cifrado de nodo** sin riesgo de pérdida de datos. Cuando se inicia la instalación el nodo del dispositivo, accede a las claves de cifrado de KMS en el sistema StorageGRID y comienza el cifrado de disco. No se puede deshabilitar el cifrado de nodos después de haber instalado el dispositivo.

   > Después de agregar un dispositivo que tiene habilitado el cifrado de nodos a un sitio StorageGRID que tiene un KMS, no puede detener el uso del cifrado KMS para el nodo.

4. Seleccione **Guardar**.
5. Ponga en marcha el dispositivo como nodo en su sistema StorageGRID.

   El cifrado controlado POR KMS se inicia cuando el dispositivo accede a las claves KMS configuradas para el sitio StorageGRID. El instalador muestra mensajes de progreso durante el proceso de cifrado KMS, que puede tardar unos minutos en función del número de volúmenes de disco del dispositivo.

   > Los dispositivos se configuran inicialmente con una clave de cifrado no KMS aleatoria asignada a cada volumen de disco. Los discos se cifran con esta clave de cifrado temporal, que no es segura, hasta que el dispositivo con cifrado de nodos habilitado acceda a las claves KMS configuradas para el sitio StorageGRID.

Después de terminar

Puede ver el estado de cifrado de nodo, los detalles de KMS y los certificados en uso cuando el nodo del dispositivo está en modo de mantenimiento.

Información relacionada

Administre StorageGRID

Supervisar el cifrado de nodos en modo de mantenimiento (SG6000)

Opcional: Cambiar el modo RAID (sólo SG6000)

Es posible cambiar a un modo RAID diferente en el dispositivo para responder a sus requisitos de almacenamiento y recuperación. Solo puede cambiar el modo antes de implementar el nodo de almacenamiento del dispositivo.

Lo que necesitará

- Está utilizando cualquier cliente que pueda conectarse a StorageGRID.
- El cliente tiene un navegador web compatible.

Acerca de esta tarea

Antes de implementar el dispositivo como un nodo de almacenamiento, puede seleccionar una de las siguientes opciones de configuración de volumen:

- **DDP**: Este modo utiliza dos unidades de paridad por cada ocho unidades de datos. Éste es el modo predeterminado y recomendado para todos los dispositivos. En comparación con RAID6, los DDP ofrecen mejor rendimiento del sistema, reducen los tiempos de recompilación después de fallos de unidad y facilitan la gestión.

  > DDP no proporciona protección contra pérdida de cajón en dispositivos SG6060 debido a los dos SSD. La protección contra pérdida de cajón resulta efectiva en cualquier bandeja de expansión que se añada a un SG6060.

- **DDP16**: Este modo utiliza dos unidades de paridad por cada 16 unidades de datos, lo que da como resultado una mayor eficiencia de almacenamiento en comparación con DDP. En comparación con RAID6, DDP16 ofrece un mejor rendimiento del sistema, menores tiempos de recompilación después de fallos de unidad, facilidad de gestión y una eficiencia de almacenamiento similar. Para utilizar el modo DDP16, la configuración debe contener al menos 20 unidades. DDP16 no ofrece protección contra pérdida de cajón.
- **RAID6**: Este modo utiliza dos unidades de paridad por cada 16 o más unidades de datos. Para utilizar el modo RAID 6, la configuración debe contener al menos 20 unidades. Aunque RAID6 puede aumentar la eficiencia de almacenamiento del dispositivo en comparación con DDP, no es recomendable para la mayoría de entornos StorageGRID.

  > Si alguno de los volúmenes ya está configurado o si StorageGRID se instaló anteriormente, al cambiar el modo RAID se quitan y se reemplazan los volúmenes. Se perderán todos los datos de estos volúmenes.

Pasos

1. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.

   ```
   https://Controller_IP:8443
   ```

   `Controller_IP` Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Avanzado** > **modo RAID**.
3. En la página **Configurar el modo RAID**, seleccione el modo RAID deseado en la lista desplegable modo.
4. Haga clic en **Guardar**.

Información relacionada

"Sitio de documentación para sistemas E-Series y EF-Series de NetApp"

Opcional: Reasignar puertos de red para el dispositivo

Es posible que deba reasignar los puertos internos del nodo de almacenamiento del dispositivo a diferentes puertos externos. Por ejemplo, es posible que tenga que reasignar puertos debido a un problema de firewall.

Lo que necesitará

- Ya ha accedido anteriormente al instalador de dispositivos de StorageGRID.
- No ha configurado y no planea configurar los extremos del equilibrador de carga.

> Si se reasigna algún puerto, no se pueden utilizar los mismos puertos para configurar los puntos finales del equilibrador de carga. Si desea configurar puntos finales del equilibrador de carga y ya tiene puertos reasignados, siga los pasos de Eliminar reasignaciones de puertos.

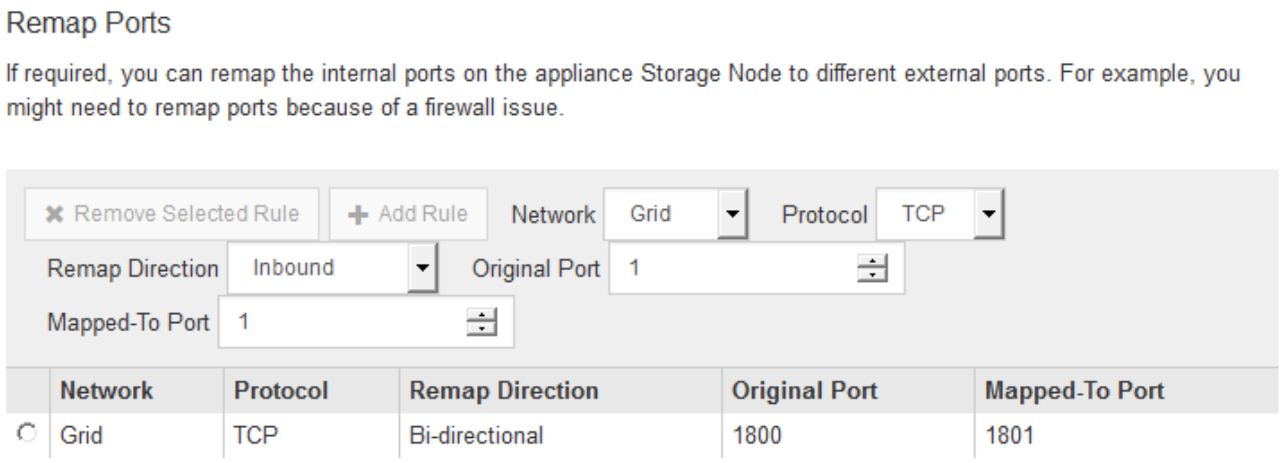
Pasos

1. En el instalador del dispositivo StorageGRID, haga clic en **Configurar redes puertos de memoria**.

   Aparecerá la página Remap Port.

2. En el cuadro desplegable **Red**, seleccione la red para el puerto que desea reasignar: Grid, Admin o Client.
3. En el cuadro desplegable **Protocolo**, seleccione el protocolo IP: TCP o UDP.
4. En el cuadro desplegable **Dirección de salida**, seleccione la dirección de tráfico que desea reasignar para este puerto: Entrante, saliente o bidireccional.
5. Para **Puerto original**, introduzca el número del puerto que desea reasignar.
6. En **Puerto asignado a**, introduzca el número del puerto que desea utilizar en su lugar.
7. Haga clic en **Agregar regla**.

   La nueva asignación de puertos se agrega a la tabla y la reasignación tiene efecto inmediatamente.



8. Para eliminar una asignación de puertos, seleccione el botón de opción de la regla que desea quitar y haga clic en **Eliminar regla seleccionada**.

Ponga en marcha el nodo de almacenamiento del dispositivo

Después de instalar y configurar el dispositivo de almacenamiento, puede ponerlo en marcha como un nodo de almacenamiento en un sistema StorageGRID. Al poner en marcha un dispositivo como nodo de almacenamiento, utiliza el instalador de dispositivos de StorageGRID que se incluye en el dispositivo.

Lo que necesitará

- Si va a clonar un nodo de dispositivo, continúe durante el proceso de recuperación y mantenimiento.

  Recuperación y mantenimiento

- El dispositivo se ha instalado en un rack o armario, conectado a las redes y encendido.
- Se han configurado los enlaces de red, las direcciones IP y la reasignación de puertos (si fuera necesario) para el dispositivo con el instalador de dispositivos de StorageGRID.
- Conoce una de las direcciones IP asignadas a la controladora de computación del dispositivo. Puede usar la dirección IP para cualquier red StorageGRID conectada.
- Se puso en marcha el nodo de administración principal del sistema 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.
- Tiene un portátil de servicio con un navegador web compatible.

Acerca de esta tarea

Cada dispositivo de almacenamiento funciona como un único nodo de almacenamiento. Cualquier dispositivo puede conectarse a la red de grid, a la red de administración y a la red de cliente

Para implementar un nodo de almacenamiento de dispositivos en un sistema StorageGRID, debe acceder al instalador de dispositivos StorageGRID y realizar los siguientes pasos:

- Debe especificar o confirmar la dirección IP del nodo de administrador principal y el nombre del nodo de almacenamiento.
- Se inicia la puesta en marcha y se espera a medida que se hayan configurado los volúmenes y se haya instalado el software.
- Cuando la instalación se detiene paso a paso a través de las tareas de instalación del dispositivo, se reanuda la instalación iniciando sesión en el Administrador de grid, aprobando todos los nodos de cuadrícula y completando los procesos de instalación e implementación de StorageGRID.

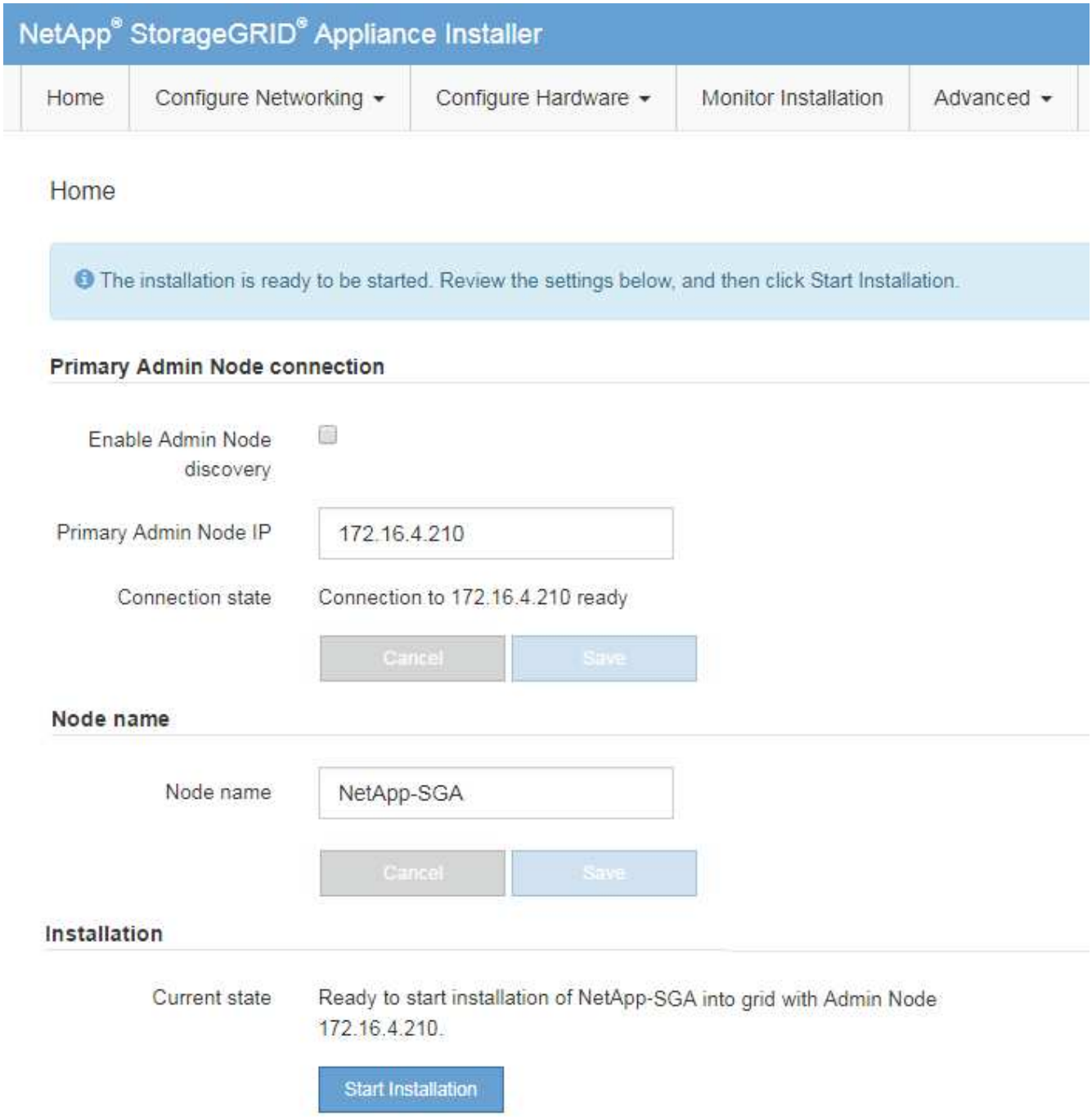
> Si necesita implementar varios nodos de dispositivos a la vez, puede automatizar el proceso de instalación mediante el `configure-sga.py` Script de instalación del dispositivo.

- Si va a realizar una operación de expansión o recuperación, siga las instrucciones correspondientes:
  - Para añadir un nodo de almacenamiento del dispositivo a un sistema StorageGRID existente, consulte las instrucciones para ampliar un sistema StorageGRID.
  - Para poner en marcha un nodo de almacenamiento del dispositivo como parte de una operación de recuperación, consulte las instrucciones de recuperación y mantenimiento.

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 **Conexión del 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. Anule la selección de la casilla de verificación **Activar descubrimiento de nodo de administración**. 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.
Detección automática de todos los nodos principales de administración conectados	a. Active la casilla de verificación **Activar descubrimiento de nodos de administración**. 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 haga clic en **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 **instalación**, confirme que el estado actual es "Listo para iniciar la instalación de `node name` En el grid con el nodo de administrador principal `admin_ip` " Y que el botón **Iniciar instalación** 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 instalación y mantenimiento del aparato.

   > Si va a poner en marcha el dispositivo Storage Node como destino de clonado de nodos, detenga el proceso de puesta en marcha aquí y continúe con el procedimiento de clonado de nodos en recuperación y mantenimiento. +Recuperación y mantenimiento

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**.

7. Si el grid incluye varios nodos de almacenamiento de dispositivos, repita estos pasos para cada dispositivo.

> Si necesita implementar varios nodos de almacenamiento para dispositivos a la vez, puede automatizar el proceso de instalación mediante el `configure-sga.py` Script de instalación del dispositivo.

Información relacionada

Amplíe su grid

Recuperación y mantenimiento

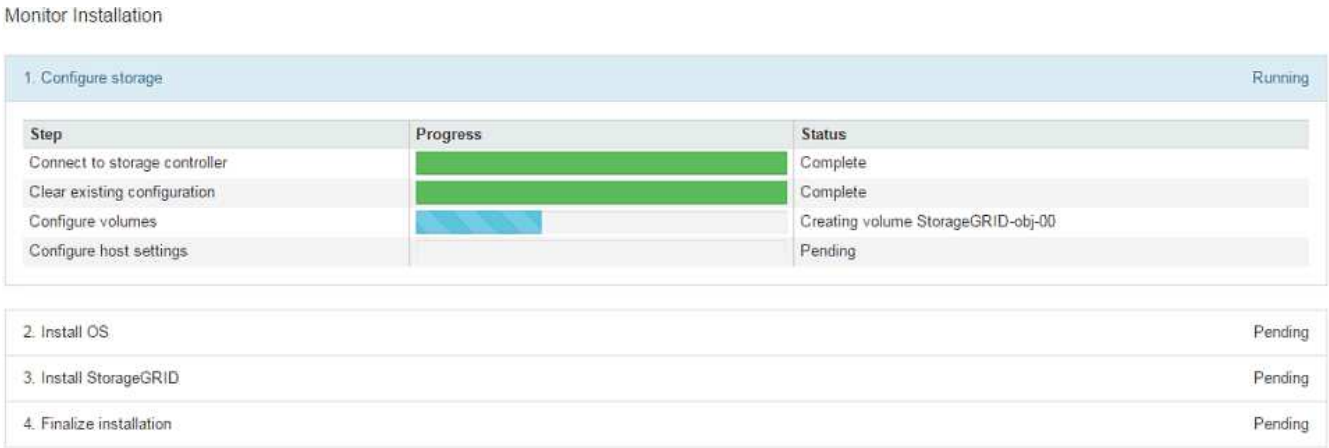
Supervise la instalación de dispositivos de almacenamiento

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**.

   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.

> El instalador garantiza que no se vuelvan a ejecutar las tareas completadas en una instalación anterior. 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 de "Shided."

2. Revise el progreso de las dos primeras etapas de instalación.

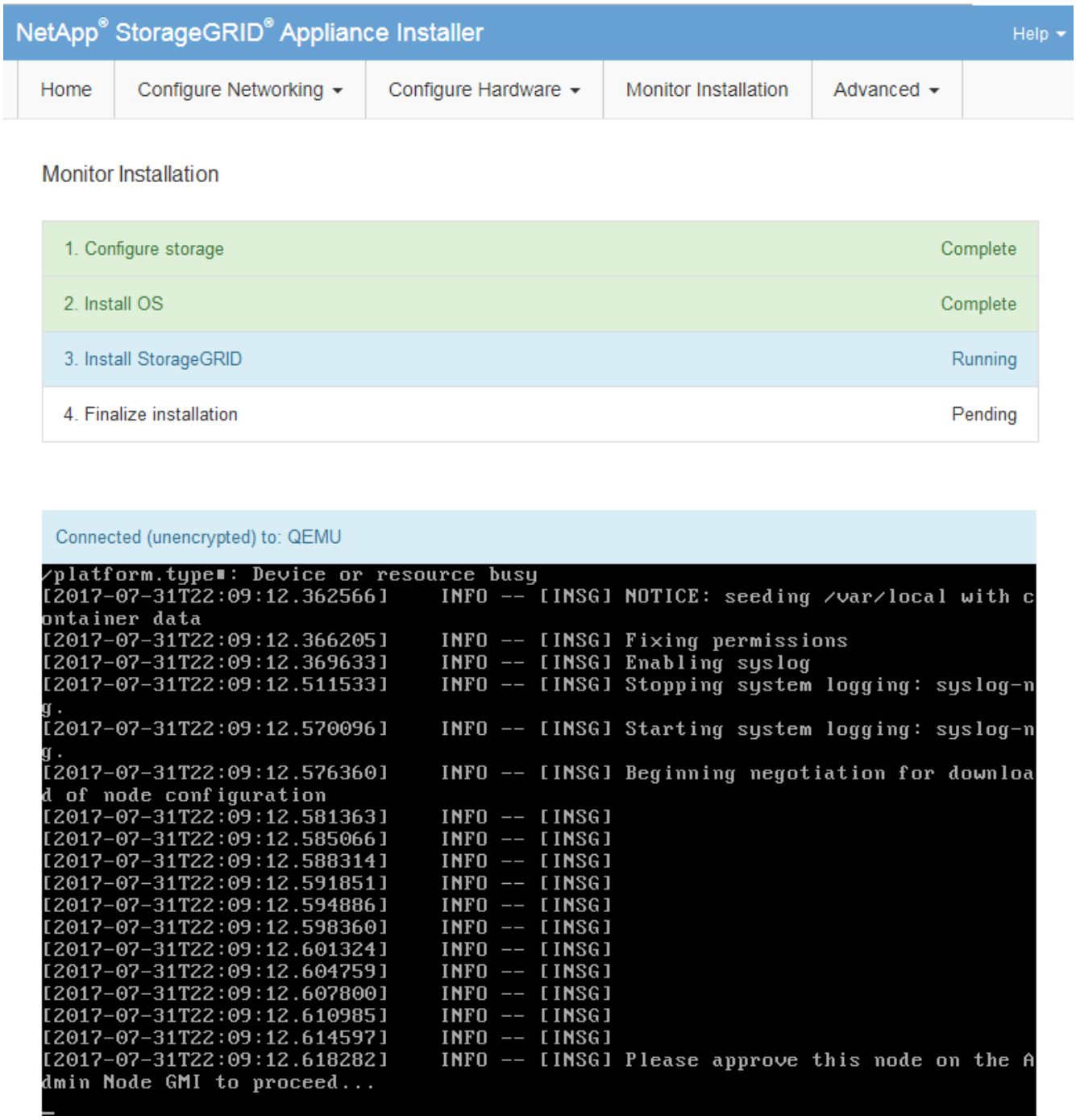
   1. Configurar almacenamiento

   Durante esta fase, el instalador se conecta al controlador de almacenamiento, borra cualquier configuración existente, se comunica con el software 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, solicitándole que apruebe este nodo en el nodo de administración mediante el Administrador de grid. Vaya al paso siguiente.



4. Vaya a Grid Manager del nodo Primary Admin, apruebe el nodo de almacenamiento pendiente y complete el proceso de instalación de StorageGRID.

   Al hacer clic en **instalar** desde Grid Manager, se completa la fase 3 y comienza la fase 4, **Finalizar instalación**. Cuando finaliza la etapa 4, se reinicia la controladora.

Instalación y configuración automatizadas del dispositivo (SG6000)

Puede automatizar la instalación y configuración de sus dispositivos y la configuración de todo el sistema StorageGRID.

Acerca de esta tarea

Automatizar la instalación y la configuración puede ser útil para poner en marcha varias instancias de StorageGRID o una instancia de StorageGRID grande y compleja.

Para automatizar la instalación y configuración, utilice una o varias de las siguientes opciones:

- Cree un archivo JSON que especifique las opciones de configuración para los dispositivos. Cargue el archivo JSON con el instalador de dispositivos StorageGRID.

  Puede usar el mismo archivo para configurar más de un dispositivo.

- Utilice la StorageGRID`configure-sga.py` Script Python para automatizar la configuración de sus dispositivos.
- Utilice scripts Python adicionales para configurar otros componentes de todo el sistema StorageGRID (la "cuadrícula").

Puede utilizar directamente los scripts Python de automatización de StorageGRID o bien puede usarlos como ejemplos de cómo utilizar la API DE REST de instalación de StorageGRID en las herramientas de puesta en marcha de grid y de configuración que desarrolla usted mismo. Consulte la información acerca de Descarga y extracción de los archivos de instalación de StorageGRID.

Automatice la configuración del dispositivo con StorageGRID Appliance Installer

Puede automatizar la configuración de un dispositivo mediante un archivo JSON que contiene la información de configuración. El archivo se carga con el instalador de dispositivos de StorageGRID.

Lo que necesitará

- El dispositivo debe tener el firmware más reciente compatible con StorageGRID 11.5 o superior.
- Debe estar conectado al instalador de dispositivos de StorageGRID en el dispositivo que esté configurando mediante un navegador web compatible.

Acerca de esta tarea

Puede automatizar las tareas de configuración de los dispositivos, como la configuración de las siguientes opciones:

- Redes de grid, red de administración y direcciones IP de red de cliente
- Interfaz BMC
- Enlaces de red
  - Modo de enlace de puerto
  - Modo de enlace de red
  - Velocidad de enlace

La configuración del dispositivo con un archivo JSON cargado suele ser más eficaz que realizar la configuración manualmente mediante múltiples páginas en el instalador del dispositivo StorageGRID, especialmente si tiene que configurar muchos nodos. Debe aplicar el archivo de configuración para cada nodo de uno en uno.

> Los usuarios con experiencia que deseen automatizar tanto la instalación como la configuración de sus dispositivos pueden utilizar el `configure-sga.py` guión. +Automatice la instalación y configuración de los nodos de los dispositivos con un script configure-sga.py

Pasos

1. Genere el archivo JSON mediante uno de los siguientes métodos:
   - Aplicación ConfigBuilder

     "ConfigBuilder.netapp.com"

   - La `configure-sga.py` script de configuración del dispositivo. Puede descargar la secuencia de comandos desde el instalador del dispositivo StorageGRID (**Ayuda** > **secuencia de comandos de configuración del dispositivo**). Consulte las instrucciones sobre cómo automatizar la configuración mediante el script configure-sga.py.

     Automatice la instalación y configuración de los nodos de los dispositivos con un script configure-sga.py

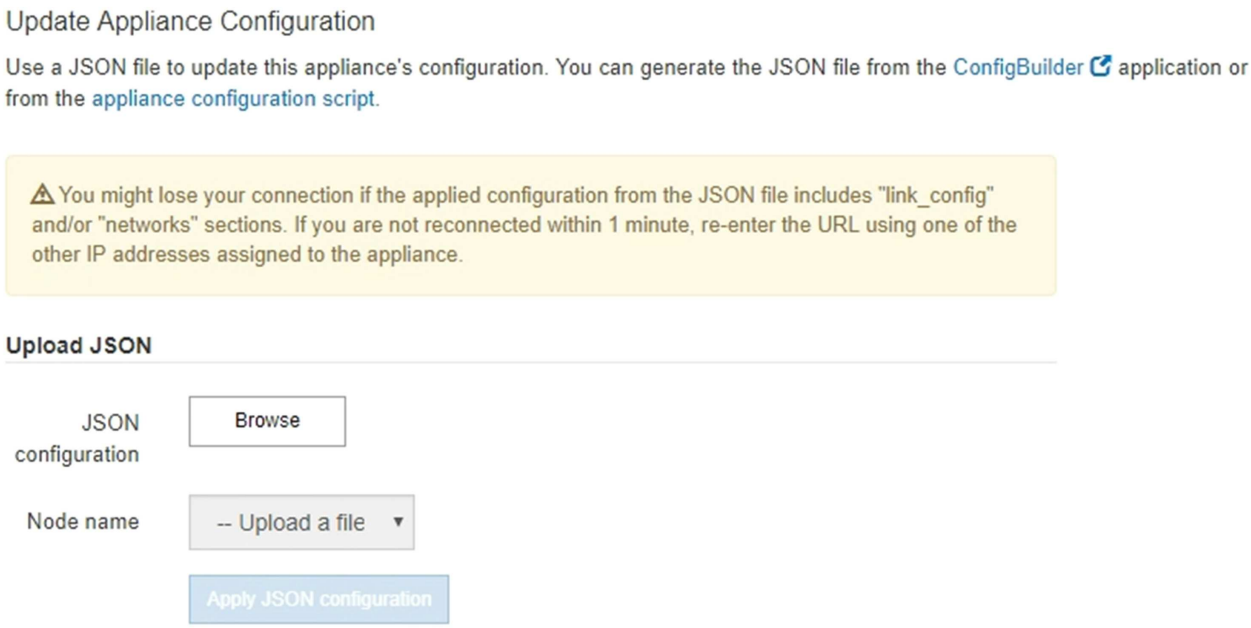
     Los nombres de nodos en el archivo JSON deben seguir estos requisitos:

   - Debe ser un nombre de host válido que contenga al menos 1 y no más de 32 caracteres
   - Puede usar letras, números y guiones
   - No se puede iniciar o finalizar con un guión
   - No puede contener solo números

     > Asegúrese de que los nombres de nodo (los nombres de nivel superior) del archivo JSON son únicos o de que no pueda configurar más de un nodo mediante el archivo JSON.

2. Seleccione **Avanzado** > **Actualizar configuración del dispositivo**.

   Aparece la página Actualizar configuración del dispositivo.



3. Seleccione el archivo JSON con la configuración que desea cargar.

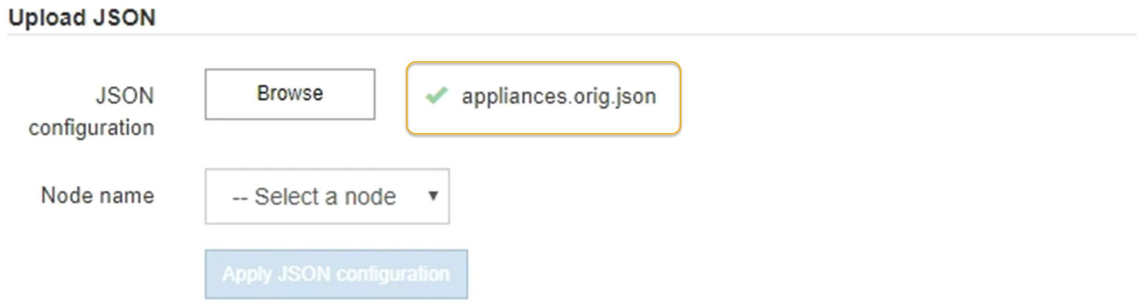
   a. Seleccione **examinar**.

   b. Localice y seleccione el archivo.

   c. Seleccione **Abrir**.

   El archivo se carga y se valida. Una vez completado el proceso de validación, se muestra el nombre del archivo junto a una Marca de verificación verde.

   > Es posible que pierda la conexión con el dispositivo si la configuración del archivo JSON incluye secciones de "link_config", "Networks" o ambas. Si no vuelve a conectarse en 1 minuto, vuelva a introducir la URL del dispositivo utilizando una de las otras direcciones IP asignadas al dispositivo.

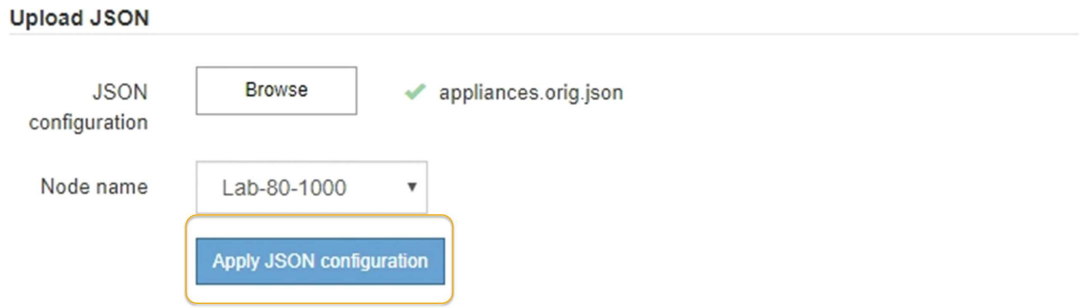


   La lista desplegable **Nombre de nodo** se rellena con los nombres de nodo de nivel superior definidos en el archivo JSON.

Si el archivo no es válido, el nombre del archivo se muestra en rojo y se muestra un mensaje de error en un banner amarillo. El archivo no válido no se ha aplicado al dispositivo. Puede utilizar ConfigBuilder para asegurarse de tener un archivo JSON válido.

4. Seleccione un nodo de la lista de la lista desplegable **Nombre de nodo**.

   El botón **aplicar configuración JSON** está activado.



5. Seleccione **aplicar configuración JSON**.

   La configuración se aplica al nodo seleccionado.

Automatice la instalación y configuración de los nodos de los dispositivos con un script configure-sga.py

Puede utilizar el `configure-sga.py` Script para automatizar muchas de las tareas de instalación y configuración para los nodos del dispositivo StorageGRID, incluida la instalación y configuración de un nodo de administración principal. Esta secuencia de comandos puede ser útil si tiene un gran número de dispositivos que configurar. También puede usar el script para generar un archivo JSON que contenga información de configuración del dispositivo.

Lo que necesitará

- 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 nodo de administración principal mediante el instalador de dispositivos de StorageGRID.
- Si está instalando el nodo de administrador principal, conoce su dirección IP.
- Si va a instalar y configurar otros nodos, el nodo de administrador principal se ha implementado y conoce su dirección IP.
- Para todos los nodos que no sean el nodo de administración principal, todas las subredes de red de cuadrícula que aparecen en la página Configuración de IP del instalador de dispositivos StorageGRID se han definido en la lista de subredes de redes de cuadrícula del nodo de administración principal.
- Ha descargado el `configure-sga.py` archivo. El archivo se incluye en el archivo de instalación o puede acceder a él haciendo clic en **Ayuda** > **secuencia de comandos de instalación del dispositivo** en el instalador del dispositivo StorageGRID.

Este procedimiento es para usuarios avanzados con cierta experiencia usando interfaces de línea de comandos. También puede usar el instalador de dispositivos de StorageGRID para automatizar la configuración. +Automatice la configuración del dispositivo con StorageGRID Appliance Installer

Pasos

1. Inicie sesión en el equipo Linux que está utilizando para ejecutar el script Python.
2. Para obtener ayuda general sobre la sintaxis de la secuencia de comandos y ver una lista de los parámetros disponibles, introduzca lo siguiente:

   ```
   configure-sga.py --help
   ```

   La `configure-sga.py` el script utiliza cinco subcomandos:

   - `advanced` Para interacciones avanzadas con dispositivos StorageGRID, incluida la configuración del BMC y la creación de un archivo JSON con la configuración actual del dispositivo
   - `configure` Para configurar los parámetros de modo RAID, nombre del nodo y red
   - `install` Para iniciar una instalación de StorageGRID
   - `monitor` Para supervisar una instalación de StorageGRID
   - `reboot` para reiniciar el dispositivo

   Si introduce un argumento de subcomando (avanzado, configure, instale, monitor o reboot) seguido del `--help` opción usted obtendrá un texto de ayuda diferente que proporciona más detalles sobre las opciones disponibles dentro de ese subcomando:
   `configure-sga.py` *`subcommand`* `--help`

3. Para confirmar la configuración actual del nodo del dispositivo, introduzca lo siguiente donde *`SGA-install-ip`* Es cualquiera de las direcciones IP del nodo del dispositivo:
   `configure-sga.py configure` *`SGA-INSTALL-IP`*

   Los resultados muestran información de IP actual del dispositivo, incluida la dirección IP del nodo de administración principal e información sobre las redes de administración, grid y cliente.

   ```
   Connecting to +https://10.224.2.30:8443+ (Checking version and
   connectivity.)
   2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
   2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
   200
   2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
   Received 200
   2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
   200
   2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
   2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
   200
   ```

```
StorageGRID Appliance
  Name:        LAB-SGA-2-30
  Node type:   storage

StorageGRID primary Admin Node
  IP:        172.16.1.170
  State:     unknown
  Message:   Initializing...
  Version:   Unknown

Network Link Configuration
  Link Status
        Link      State      Speed (Gbps)
        ----      -----      -----
        1         Up         10
        2         Up         10
        3         Up         10
        4         Up         10
        5         Up         1
        6         Down       N/A

  Link Settings
      Port bond mode:      FIXED
      Link speed:          10GBE

      Grid Network:        ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

      Admin Network:       ENABLED
          Bonding mode:    no-bond
          MAC Addresses:   00:80:e5:29:70:f4

      Client Network:      ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

Grid Network
  CIDR:      172.16.2.30/21 (Static)
  MAC:       00:A0:98:59:8E:8A
  Gateway:   172.16.0.1
  Subnets:   172.17.0.0/21
             172.18.0.0/21
             192.168.0.0/21
```

```
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

#################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#################################################################
```

4. Si necesita cambiar alguno de los valores de la configuración actual, utilice `configure` subcomando para actualizarlos. Por ejemplo, si desea cambiar la dirección IP que utiliza el dispositivo para conectarse al nodo de administración principal `172.16.2.99`, introduzca lo siguiente:
   `configure-sga.py configure --admin-ip 172.16.2.99` *`SGA-INSTALL-IP`*
5. Si desea realizar un backup de la configuración del dispositivo en un archivo JSON, utilice `advanced` y.. `backup-file` subcomandos. Por ejemplo, si desea realizar una copia de seguridad de la configuración de un dispositivo con dirección IP *`SGA-INSTALL-IP`* a un archivo llamado `appliance-SG1000.json`, introduzca lo siguiente:
   `configure-sga.py advanced --backup-file appliance-SG1000.json` *`SGA-INSTALL-IP`*

   El archivo JSON que contiene la información de configuración se escribe en el mismo directorio desde el que se ejecutó la secuencia de comandos.

   > Compruebe que el nombre del nodo de nivel superior del archivo JSON generado coincida con el nombre del dispositivo. No haga ningún cambio en este archivo a menos que sea un usuario con experiencia y que tenga una profunda comprensión de las API de StorageGRID.

6. Cuando esté satisfecho con la configuración del dispositivo, utilice `install` y.. `monitor` subcomandos para instalar el dispositivo:
   `configure-sga.py install --monitor` *`SGA-INSTALL-IP`*
7. Si desea reiniciar el dispositivo, introduzca lo siguiente:
   `configure-sga.py reboot` *`SGA-INSTALL-IP`*

Automatice la configuración de StorageGRID

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

Lo que necesitará

- 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
```

Después de terminar

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 ha especificado que se deben generar contraseñas aleatorias, debe extraer 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 general sobre la instalación de API de REST

StorageGRID proporciona dos API REST para realizar tareas de instalación: La API de instalación de StorageGRID y la API del instalador de dispositivos de StorageGRID.

Ambas API utilizan 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 (notación de objetos JavaScript).

> 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 configura inicialmente el sistema StorageGRID y en el caso de que deba realizar una recuperación de nodo de administrador principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de API, vaya a la página web de instalación del nodo de administración principal y seleccione **Ayuda** > **Documentación de 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.
- **Sites** — Operaciones de configuración a nivel de sitio. Puede crear, ver, eliminar y modificar un sitio.

API del instalador de dispositivos de StorageGRID

Se puede acceder a la API del instalador de dispositivos de StorageGRID a través de HTTPS desde `Controller_IP:8443`.

Para acceder a la documentación de la API, vaya al instalador del dispositivo StorageGRID en el dispositivo y seleccione **Ayuda** > **Documentación de la API** en la barra de menús.

La API del instalador de dispositivos de StorageGRID incluye las siguientes secciones:

- **Clone** — Operaciones para configurar y controlar la clonación de nodos.
- **Cifrado** — Operaciones para administrar el cifrado y ver el estado del cifrado.
- **Configuración del hardware** — Operaciones para configurar los ajustes del sistema en el hardware conectado.
- **Instalación** — Operaciones para iniciar la instalación del aparato y para supervisar el estado de instalación.
- **Redes** — Operaciones relacionadas con la configuración de red de Grid, Admin y Cliente para un dispositivo StorageGRID y los ajustes de puerto de dispositivo.
- **Setup** — Operaciones para ayudar con la instalación inicial del dispositivo incluyendo solicitudes para obtener información sobre el sistema y actualizar el IP principal del nodo de administración.
- **SOPORTE** — Operaciones para reiniciar el controlador y obtener registros.
- **Upgrade** — Operaciones relacionadas con la actualización del firmware del dispositivo.
- **Uploadsg** — Operaciones para cargar archivos de instalación de StorageGRID.

Solución de problemas de instalación de hardware (SG6000)

Si encuentra problemas durante la instalación, es posible que le sea útil revisar información sobre la solución de problemas relacionados con la configuración del hardware y los problemas de conectividad.

Ver los códigos de arranque del controlador SG6000-CN

Cuando se enciende el aparato, el BMC registra una serie de códigos de inicio para el controlador SG6000-CN. Puede ver estos códigos de varias maneras.

Lo que necesitará

- Sabe cómo acceder al panel de BMC.
- Si desea utilizar Serial-Over-LAN (sol), tendrá experiencia utilizando las aplicaciones de la consola sol de IPMI.

Pasos

1. Seleccione uno de los siguientes métodos para ver los códigos de arranque del controlador del dispositivo y recopilar el equipo necesario.

Método	Equipo necesario
Consola VGA	• Monitor compatible con VGA • Cable VGA
KVM	• Cable RJ-45
Puerto serie	• Cable serie DB-9 • Terminal serie virtual
SOL	• Terminal serie virtual

2. Si está utilizando una consola VGA, siga estos pasos:
   a. Conecte un monitor compatible con VGA al puerto VGA de la parte posterior del dispositivo.
   b. Ver los códigos mostrados en el monitor.
3. Si está utilizando BMC KVM, realice estos pasos:
   a. Conéctese al puerto de administración de BMC e inicie sesión en la interfaz web de BMC.
   b. Seleccione **Control remoto**.
   c. Inicie el KVM.
   d. Ver los códigos en el monitor virtual.
4. Si utiliza un puerto serie y un terminal, realice los siguientes pasos:
   a. Conecte el puerto serie DB-9 de la parte posterior del dispositivo.
   b. Utilice la configuración `115200 8-N-1`.
   c. Ver los códigos impresos en el terminal de serie.
5. Si va a utilizar sol, realice los siguientes pasos:
   a. Conéctese a IPMI sol mediante la dirección IP del BMC y las credenciales de inicio de sesión.

> Si no ha cambiado la contraseña de la cuenta raíz de BMC, el valor predeterminado de fábrica puede ser "calvin".

```
ipmitool -I lanplus -H BMC_Port_IP -U root -P Password sol activate
```

b. Ver los códigos en el terminal de serie virtual.

6. Utilice la tabla para buscar los códigos del aparato.

Codificación	Lo que indica
HOLA	Se ha iniciado la secuencia de comandos de inicio maestra.
HP	El sistema comprueba si es necesario actualizar el firmware de la tarjeta de interfaz de red (NIC).
RB	El sistema se reinicia después de aplicar las actualizaciones de firmware.
P F	Se completaron las comprobaciones de actualización del firmware del subsistema de hardware. Se están iniciando los servicios de comunicación entre controladoras.
ÉL	Solo para un nodo de almacenamiento del dispositivo: El sistema está esperando conectividad con las controladoras de almacenamiento y sincronizarse con el sistema operativo SANtricity. **Nota:** Si el procedimiento de arranque no avanza más allá de esta fase, lleve a cabo los siguientes pasos: a. Confirmar que los cuatro cables de interconexión entre el controlador SG6000-CN y los dos controladores de almacenamiento están conectados de forma segura. b. Según sea necesario, sustituya uno o más cables y vuelva a intentarlo. c. Si esto no se resuelve el problema, póngase en contacto con el soporte técnico.
HC	El sistema comprueba si hay datos de instalación de StorageGRID existentes.
HO	El instalador de dispositivos de StorageGRID se está ejecutando.
HA	StorageGRID está ejecutando.

Ver códigos de error para el controlador SG6000-CN

Si se produce un error de hardware cuando se inicia el controlador SG6000-CN, el BMC registra un código de error. Según sea necesario, puede ver estos códigos de error mediante la interfaz del BMC y, a continuación, trabajar con el soporte técnico para resolver el problema.

Lo que necesitará

- Sabe cómo acceder al panel de BMC.

Pasos

1. En el panel de control del BMC, seleccione **Código POST del BIOS**.
2. Revise la información que se muestra para el código actual y el código anterior.

   Si se muestra alguno de los siguientes códigos de error, trabaje con el soporte técnico para resolver el problema.

Codificación	Lo que indica
0x0e	No se ha encontrado el microcódigo
0x0F	No se ha cargado el microcódigo
0x50	Error de inicialización de la memoria. Tipo de memoria no válido o velocidad de memoria incompatible.
0x51	Error de inicialización de la memoria. Error en la lectura del SPD.
0x52	Error de inicialización de la memoria. El tamaño de la memoria no es válido o los módulos de memoria no coinciden.
0x53	Error de inicialización de la memoria. No se detectó memoria utilizable.
0x54	Error de inicialización de memoria no especificada
0x55	Memoria no instalada
0x56	Tipo o velocidad de CPU no válida
0x57	Discordancia de CPU
0x58	Fallo de la autoprueba de CPU o posible error de caché de CPU

Codificación	Lo que indica
0x59	No se ha encontrado el micro-código de la CPU, o la actualización del micro-código ha fallado
0x5A	Error interno de CPU
0x5b	Restablecer PPI no está disponible
0x5c	Fallo de autocomprobación PEI Phase BMC
0xD0	Error de inicialización de la CPU
0xD1	Error de inicialización del puente norte
0xD2	Error de inicialización del puente sur
0xd3	Algunos protocolos de arquitectura no están disponibles
0xD4	Error de asignación de recursos PCI. De recursos.
0xD5	No hay espacio para la ROM de opción heredada
0xD6	No se han encontrado dispositivos de salida de consola
0xD7	No se han encontrado dispositivos de entrada de consola
0xD8	Contraseña no válida
0xD9	Error al cargar la opción de arranque (LoadImage devolvió un error)
0xDA	Error en la opción de inicio (error de Startimage devuelto)
0xDB	Error en la actualización de Flash
0xDC	El protocolo de restablecimiento no está disponible
0xDD	Error de autoprueba de DXE Phase BMC
0xE8	MRC: ERR_NO_MEMORY

Codificación	Lo que indica
0xE9	MRC: ERR_LT_LOCK
0xEA	MRC: ERR_DDR_INIT
0xEB	MRC: ERR_MEM_TEST
0xEC	MRC: ERR_VENDOR_SPECIFIC
0xED	MRC: ERR_DIMM_COMPAT
0xEE	MRC: ERR_MRC_COMPATIBILIDAD
0xEF	MRC: ERR_MRC_STRUCT
0xF0	MRC: ERR_SET_VDD
0xF1	MRC: ERR_IOT_MEM_BUFFER
0xF2	MRC: ERR_RC_INTERNAL
0xF3	MRC: ERR_INVALID_REG_ACCESS
0xF4	MRC: ERR_SET_MC_FREQ
0xF5	MRC: ERR_READ_MC_FREQ
0x70	MRC: ERR_DIMM_CHANNEL
0x74	MRC: ERR_BIST_CHECK
0xF6	MRC: ERR_SMBUS
0xF7	MRC: ERR_PCU
0xF8	MRC: ERR_NGN
0xF9	MRC: ERR_INTERLEAVE_FAILURE

Parece que la configuración del hardware se bloquea (SG6000)

Es posible que el instalador de dispositivos de StorageGRID no esté disponible si los errores de hardware o de cableado impiden que los controladores de almacenamiento o el controlador SG6000-CN completen su procesamiento de arranque.

Pasos

1. Para las controladoras de almacenamiento, vea los códigos de las pantallas de siete segmentos.

   Mientras el hardware se está inicializando durante el encendido, las dos pantallas de siete segmentos muestran una secuencia de códigos. Cuando el hardware se inicia correctamente, se muestran las dos pantallas de siete segmentos `99`.

2. Revise los LED del controlador SG6000-CN y los códigos de inicio y error que aparecen en el BMC.
3. Si necesita ayuda para resolver un problema, póngase en contacto con el soporte técnico.

Información relacionada

Ver los códigos de estado de arranque para los controladores de almacenamiento SG6000

"Guía de supervisión del sistema E5700 y E2800"

Ver los indicadores de estado y los botones del controlador SG6000-CN

Ver los códigos de arranque del controlador SG6000-CN

Ver códigos de error para el controlador SG6000-CN

Solucionar problemas de conexión (SG6000)

Si tiene problemas de conexión durante la instalación del dispositivo StorageGRID, debe ejecutar los pasos de acción correctiva indicados.

No se puede conectar al dispositivo

Si no puede conectarse al dispositivo, puede haber un problema de red o es posible que la instalación del hardware no se haya completado correctamente.

Pasos

1. Si no puede conectarse con el Administrador del sistema SANtricity:
   a. Intente hacer ping al dispositivo con la dirección IP de una controladora de almacenamiento en la red de gestión para System Manager de SANtricity:
      `ping Storage_Controller_IP`
   b. Si no recibe respuesta del ping, confirme que está utilizando la dirección IP correcta.

      Use la dirección IP para el puerto de gestión 1 en cualquier controladora de almacenamiento.

   c. Si la dirección IP es correcta, compruebe el cableado del dispositivo y la configuración de la red.

      Si esto no se resuelve el problema, póngase en contacto con el soporte técnico.

   d. Si el ping se ha realizado correctamente, abra un explorador Web.
   e. Introduzca la URL para SANtricity System Manager:
      `https://Storage_Controller_IP`

      Aparece la página de inicio de sesión de SANtricity System Manager.

2. Si no puede conectarse al controlador SG6000-CN:

a. Intente hacer ping al dispositivo utilizando la dirección IP del controlador SG6000-CN:
`ping SG6000-CN_Controller_IP`

b. Si no recibe respuesta del ping, confirme que está utilizando la dirección IP correcta.

   Puede utilizar la dirección IP del dispositivo en la red de grid, la red de administración o la red de cliente.

c. Si la dirección IP es correcta, compruebe el cableado del dispositivo, los transceptores SFP y la configuración de red.

d. Si dispone de acceso físico al SG6000-CN, puede utilizar una conexión directa con la IP local permanente de enlace `169.254.0.1` para comprobar la configuración de redes de la controladora y actualizarla si es necesario. Para obtener instrucciones detalladas, consulte el paso 2 de la Acceso al instalador de dispositivos de StorageGRID.

   Si esto no se resuelve el problema, póngase en contacto con el soporte técnico.

e. Si el ping se ha realizado correctamente, abra un explorador Web.

f. Introduzca la URL para el instalador de dispositivos de StorageGRID:
`https://SG6000-CN_Controller_IP:8443`

   Aparece la página de inicio.

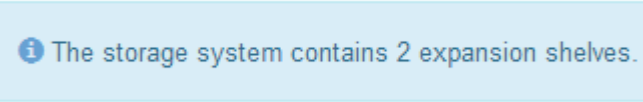
Las bandejas de expansión no aparecen en el instalador de dispositivos

Si ha instalado bandejas de expansión para el SG6060 o SG6060X y no aparecen en el instalador de dispositivos de StorageGRID, deberá verificar que las bandejas se han instalado completamente y encendido.

Acerca de esta tarea

Puede verificar que las bandejas de ampliación están conectadas al dispositivo consultando la siguiente información en el instalador de dispositivos StorageGRID:

- La página **Home** contiene un mensaje sobre las estanterías de expansión.



- La página **Advanced RAID Mode** indica por número de unidades si el aparato incluye o no estantes de expansión. Por ejemplo, en la siguiente captura de pantalla se muestran dos SSD y 178 HDD. Un SG6060 con dos bandejas de expansión contiene 180 unidades en total.

Configure RAID Mode

This appliance contains the following drives.

Type	Size	Number of drives
SSD	800 GB	2
HDD	11.8 TB	178

Si en las páginas del instalador de dispositivos StorageGRID no se indica que haya bandejas de ampliación presentes, siga este procedimiento.

Pasos

1. Compruebe que todos los cables necesarios están conectados firmemente.
2. Compruebe que sí lo ha hecho se alimenta de las bandejas de ampliación.
3. Si necesita ayuda para resolver un problema, póngase en contacto con el soporte técnico.

Reinicie el controlador SG6000-CN mientras el instalador de dispositivos StorageGRID está en ejecución

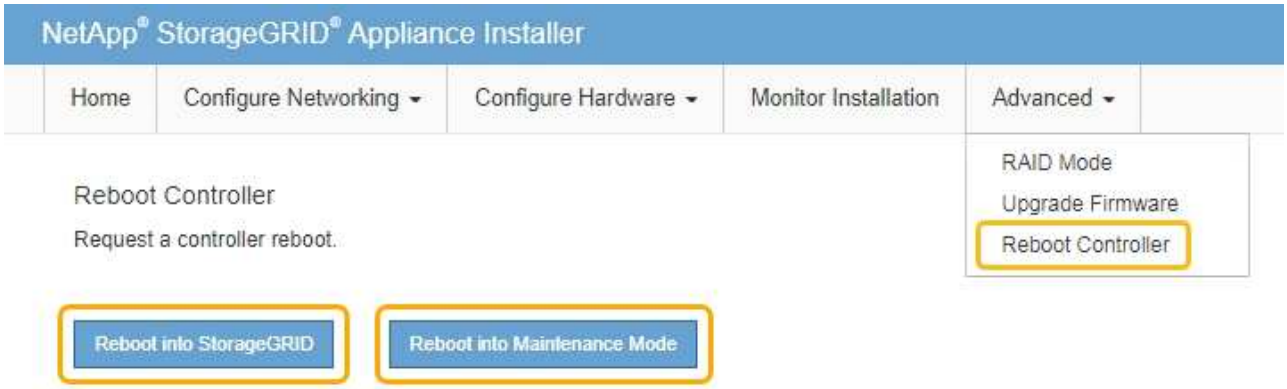
Es posible que tenga que reiniciar el controlador SG6000-CN mientras se está ejecutando el instalador de dispositivos de StorageGRID. Por ejemplo, es posible que deba reiniciar la controladora si la instalación falla.

Acerca de esta tarea

Este procedimiento sólo se aplica cuando el controlador SG6000-CN ejecuta el instalador de dispositivos StorageGRID. Una vez finalizada la instalación, este paso ya no funciona porque el instalador de dispositivos StorageGRID ya no está disponible.

Pasos

1. En el instalador del dispositivo StorageGRID, haga clic en **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:
   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



Se reinicia el controlador SG6000-CN.

Mantenimiento del dispositivo SG6000

Es posible que tenga que realizar procedimientos de mantenimiento en el dispositivo SG6000. En los procedimientos descritos en esta sección se asume que el dispositivo ya se ha puesto en marcha como nodo de almacenamiento en un sistema StorageGRID.

Para evitar interrupciones del servicio, confirme que todos los demás nodos de almacenamiento están conectados al grid antes de apagar el dispositivo o apagar el dispositivo durante un período de mantenimiento programado cuando sean aceptables. Consulte la información acerca de supervisar los estados de conexión de los nodos.

> Si alguna vez ha utilizado una regla de ILM que solo crea una copia de un objeto, debe apagar el dispositivo durante una ventana de mantenimiento programada. De lo contrario, es posible que pierda temporalmente el acceso a esos objetos durante cualquier procedimiento de mantenimiento que deje sin servicio un nodo de almacenamiento. Consulte la información acerca de gestionar objetos con gestión del ciclo de vida de la información.

Coloque el dispositivo en modo de mantenimiento

Debe colocar el aparato en modo de mantenimiento antes de realizar procedimientos de mantenimiento específicos.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso de mantenimiento o acceso raíz. Para obtener más detalles, consulte las instrucciones para administrar StorageGRID.

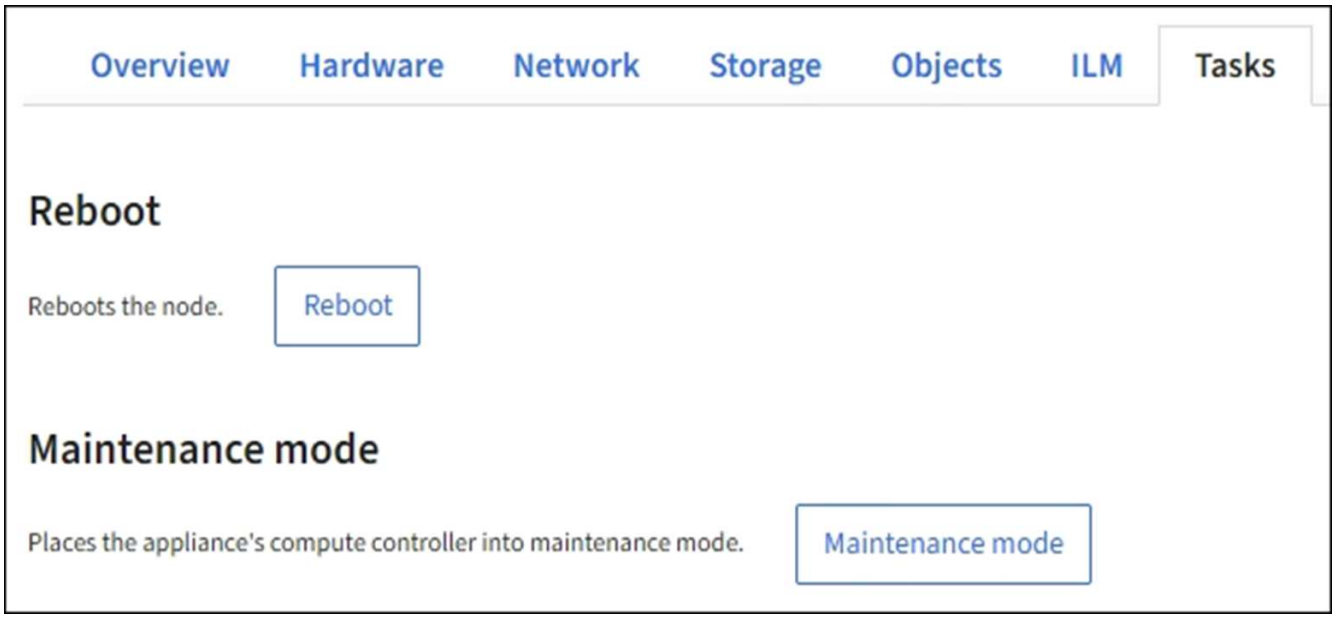
Acerca de esta tarea

En raras ocasiones, una vez que se coloca un dispositivo StorageGRID en modo de mantenimiento puede hacer que el dispositivo no esté disponible para el acceso remoto.

> La contraseña de la cuenta de administrador y las claves de host SSH para un dispositivo StorageGRID en modo de mantenimiento siguen siendo las mismas que en el momento en que el dispositivo estaba en servicio.

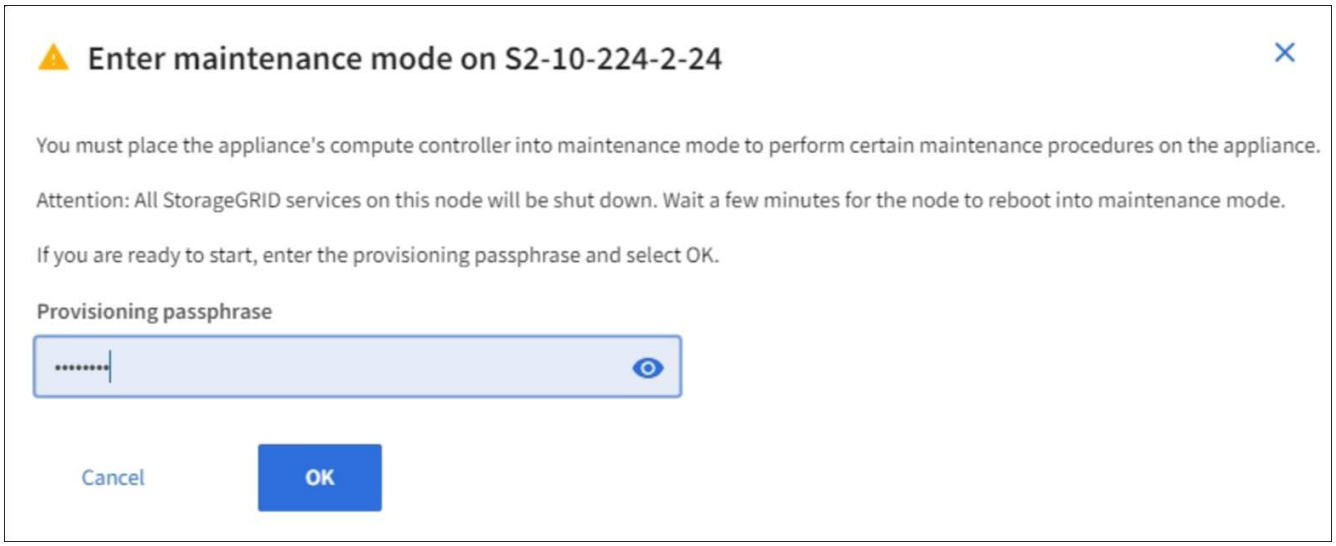
Pasos

1. En Grid Manager, seleccione **NODES**.
2. En la vista de árbol de la página Nodes, seleccione Appliance Storage Node.
3. Seleccione **tareas**.



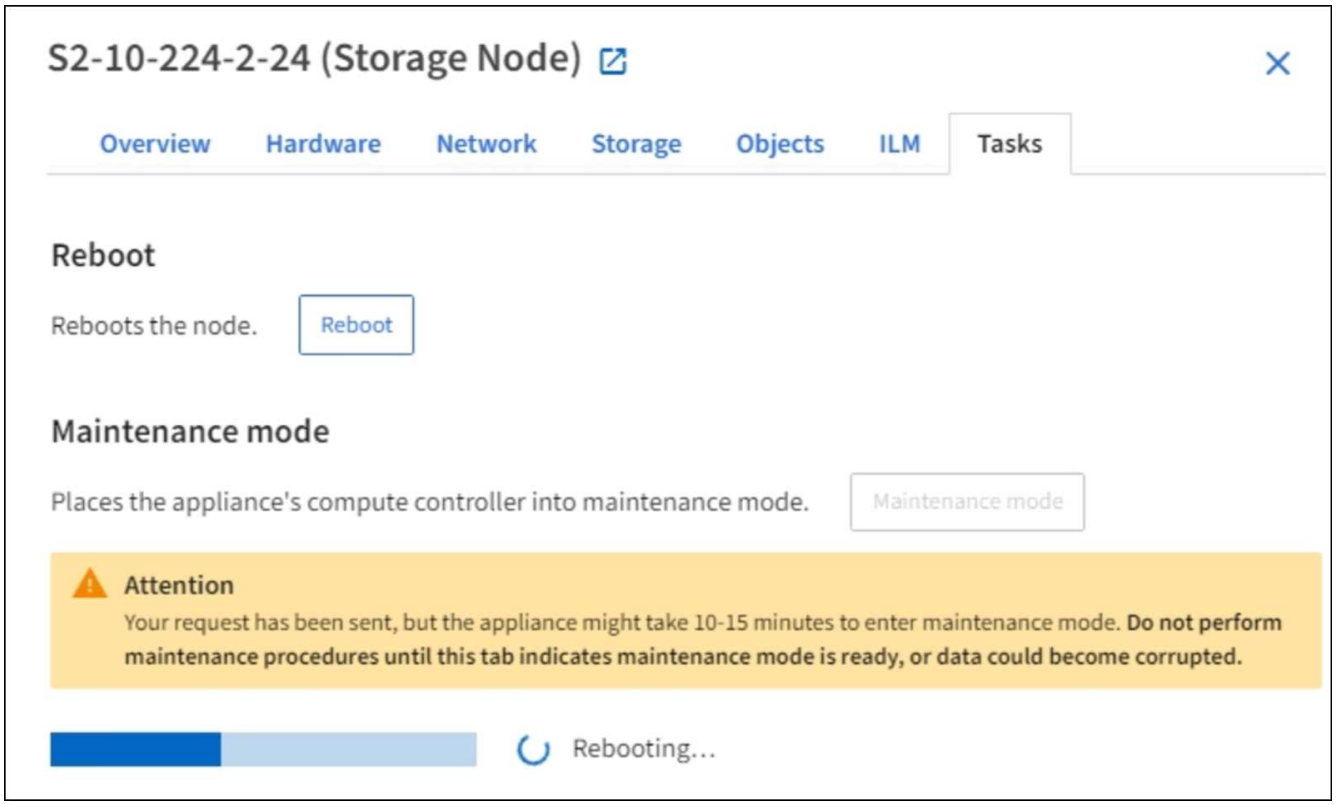
4. Seleccione **modo de mantenimiento**.

   Se muestra un cuadro de diálogo de confirmación.

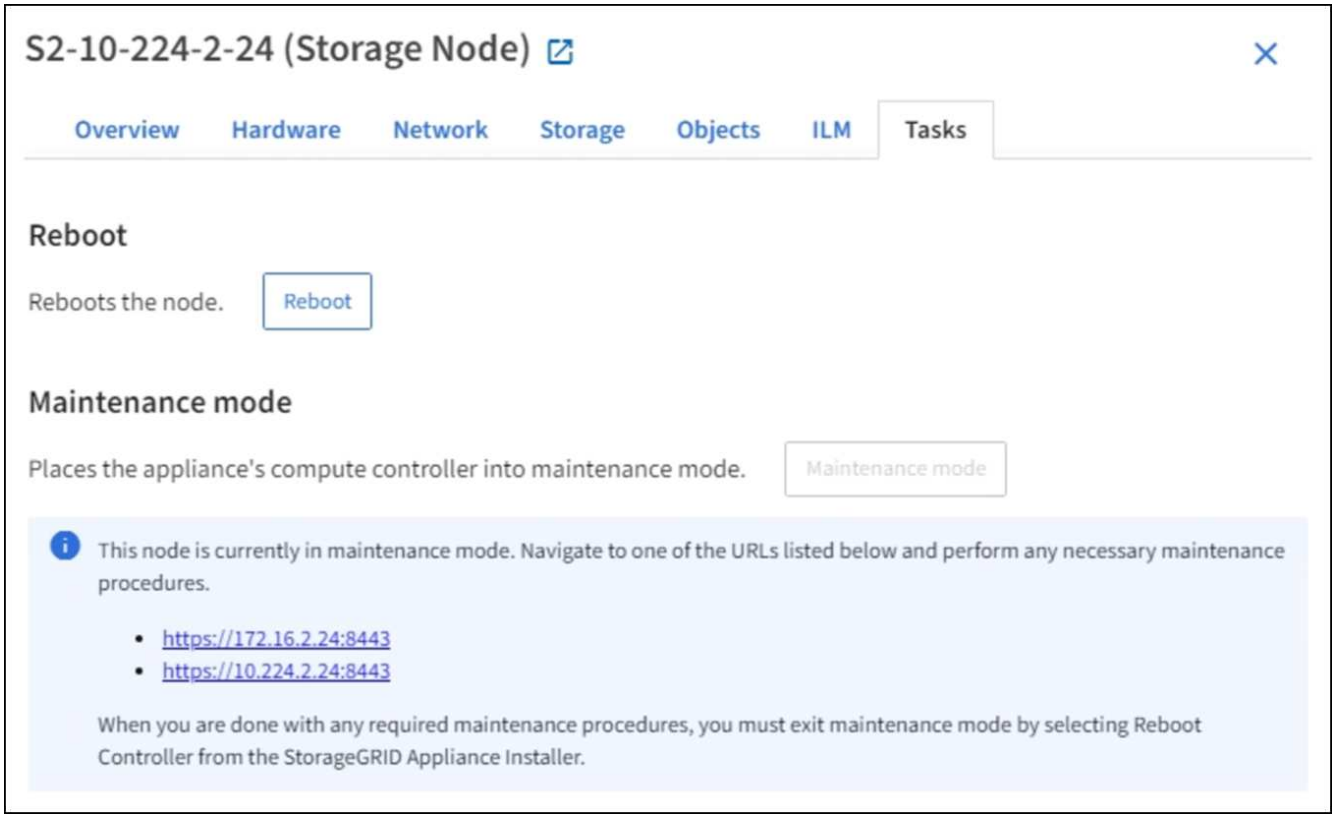


5. Introduzca la contraseña de aprovisionamiento y seleccione **Aceptar**.

   Una barra de progreso y una serie de mensajes, incluidos "solicitud enviada", "detención de StorageGRID" y "reinicio", indican que el dispositivo está llevando a cabo los pasos necesarios para entrar en el modo de mantenimiento.



Cuando el dispositivo se encuentra en modo de mantenimiento, un mensaje de confirmación enumera las URL que puede utilizar para acceder al instalador de dispositivos de StorageGRID.



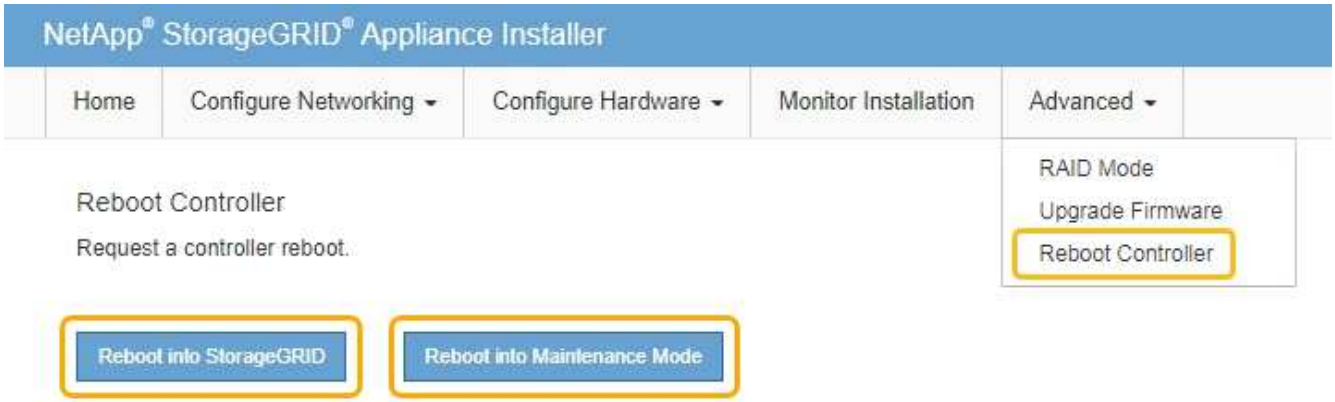
6. Para acceder al instalador de dispositivos de StorageGRID, busque cualquiera de las direcciones URL que se muestren.

Si es posible, utilice la dirección URL que contiene la dirección IP del puerto de red de administración del dispositivo.

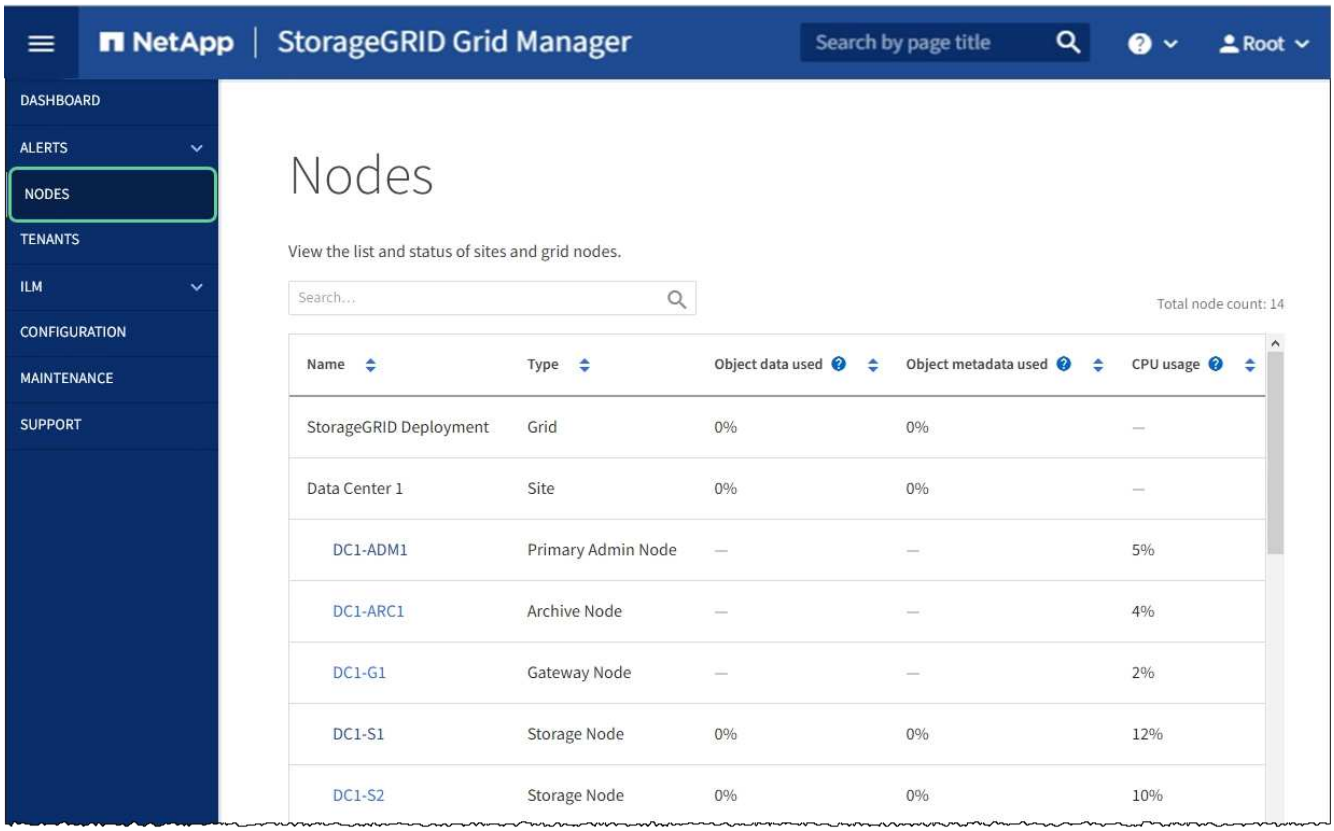
> Si tiene una conexión directa con el puerto de gestión del dispositivo, utilice `https://169.254.0.1:8443` Para acceder a la página del instalador de dispositivos de StorageGRID.

7. En el instalador de dispositivos StorageGRID, confirme que el dispositivo está en modo de mantenimiento.

8. Realice las tareas de mantenimiento necesarias.
9. Después de completar las tareas de mantenimiento, salga del modo de mantenimiento y reanude el funcionamiento normal del nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione **Reiniciar en StorageGRID**.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Actualizar el sistema operativo SANtricity en las controladoras de almacenamiento

Para garantizar el funcionamiento óptimo de la controladora de almacenamiento, debe actualizarse a la versión de mantenimiento más reciente del sistema operativo SANtricity que esté cualificado para su dispositivo StorageGRID. Consulte la herramienta de matriz de interoperabilidad de NetApp (IMT) para determinar qué versión debe utilizar. Si necesita ayuda, póngase en contacto con el soporte técnico.

Siga uno de los siguientes procedimientos según la versión de SANtricity OS instalada actualmente:

- Si la controladora de almacenamiento utiliza el sistema operativo SANtricity 08.42.20.00 (11.42) o una versión posterior, use Grid Manager para llevar a cabo la actualización.

  Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante Grid Manager

- Si la controladora de almacenamiento utiliza una versión de sistema operativo SANtricity anterior a 08.42.20.00 (11.42), use el modo de mantenimiento para realizar la actualización.

  Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante el modo de mantenimiento

> Al actualizar el sistema operativo SANtricity para el dispositivo de almacenamiento, debe seguir las instrucciones de la documentación de StorageGRID. Si usa otras instrucciones, el aparato podría quedar inoperativo.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

"Descargas de NetApp: Dispositivo de StorageGRID"

Supervisión y solución de problemas

Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante Grid Manager

Para aplicar una actualización, se deben usar Grid Manager para las controladoras de almacenamiento que actualmente utilizan SANtricity OS 08.42.20.00 (11.42) o posterior.

Lo que necesitará

- Ha consultado con la herramienta de matriz de interoperabilidad (IMT) de NetApp para confirmar que la versión del sistema operativo SANtricity que utiliza para la actualización es compatible con su dispositivo.
- Tiene el permiso de mantenimiento o acceso raíz.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene la clave de acceso de aprovisionamiento.
- Tiene acceso a la página de descargas de NetApp para SANtricity OS.

Acerca de esta tarea

No puede realizar otras actualizaciones de software (actualización de software StorageGRID o revisión) hasta que haya completado el proceso de actualización de sistema operativo SANtricity. Si intenta iniciar una revisión o una actualización de software de StorageGRID antes de que haya finalizado el proceso de actualización de SANtricity OS, se le redirigirá a la página de actualización de SANtricity OS.

No se completará el procedimiento hasta que la actualización del sistema operativo SANtricity se haya aplicado correctamente a todos los nodos aplicables seleccionados para la actualización. Es posible que tardar más de 30 minutos cargar el sistema operativo SANtricity en cada nodo (de forma secuencial) y hasta 90 minutos para reiniciar cada dispositivo de almacenamiento StorageGRID.

> Los siguientes pasos sólo son aplicables cuando se utiliza Grid Manager para realizar la actualización. No es posible actualizar las controladoras de almacenamiento en el dispositivo mediante Grid Manager cuando las controladoras utilizan SANtricity OS anteriores a 08.42.20.00 (11.42).

> Este procedimiento actualizará automáticamente la NVSRAM a la versión más reciente asociada con la actualización del sistema operativo SANtricity. No es necesario aplicar un archivo de actualización de NVSRAM aparte.

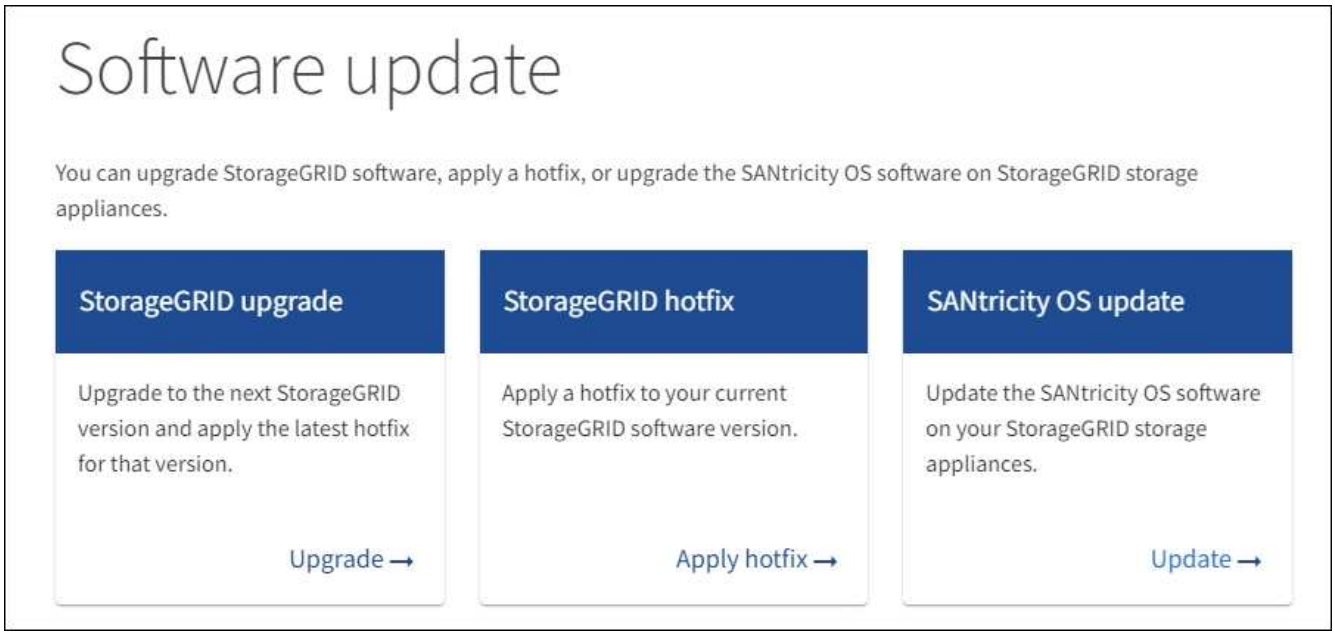
Pasos

1. Descargar el nuevo archivo de software de sistema operativo SANtricity del sitio de soporte de NetApp.

   Asegúrese de elegir la versión de sistema operativo SANtricity para las controladoras de almacenamiento.

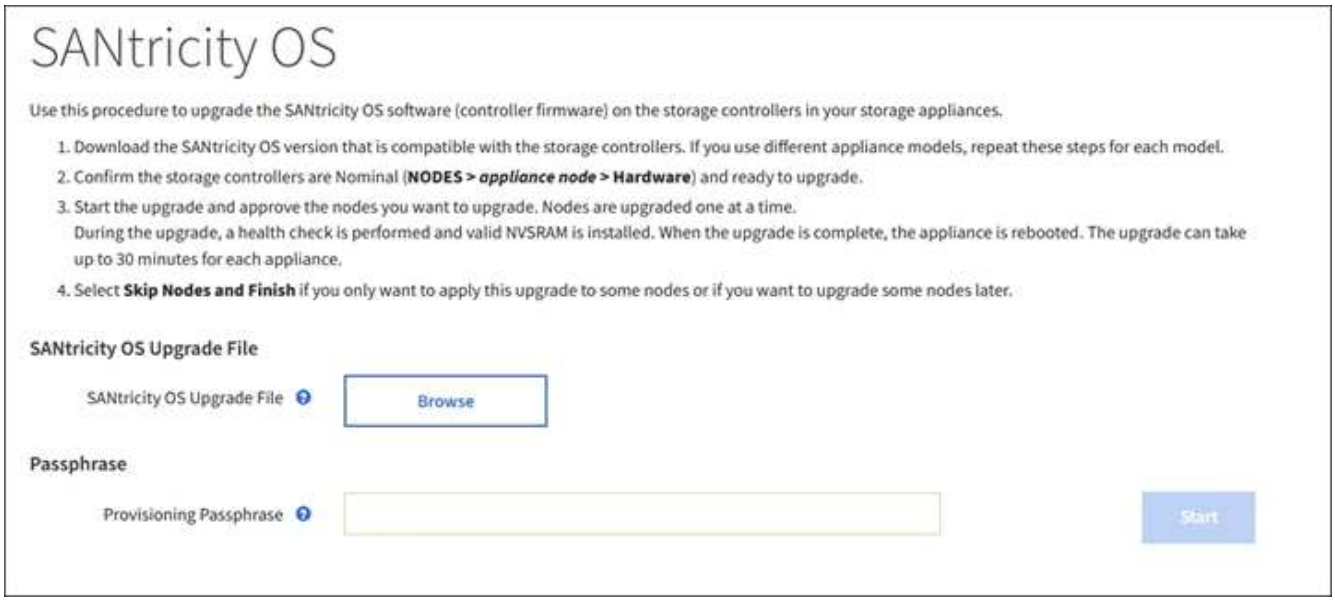
   "Descargas de NetApp: Dispositivo de StorageGRID"

2. Seleccione **MANTENIMIENTO** > **sistema** > **actualización de software**.



3. En la sección actualización del sistema operativo SANtricity, seleccione **Actualizar**.

   Se muestra la página actualización de sistema operativo SANtricity.



4. Seleccione el archivo de actualización del sistema operativo SANtricity que descargó del sitio de soporte de NetApp.

   a. Seleccione **examinar**.

   b. Localice y seleccione el archivo.

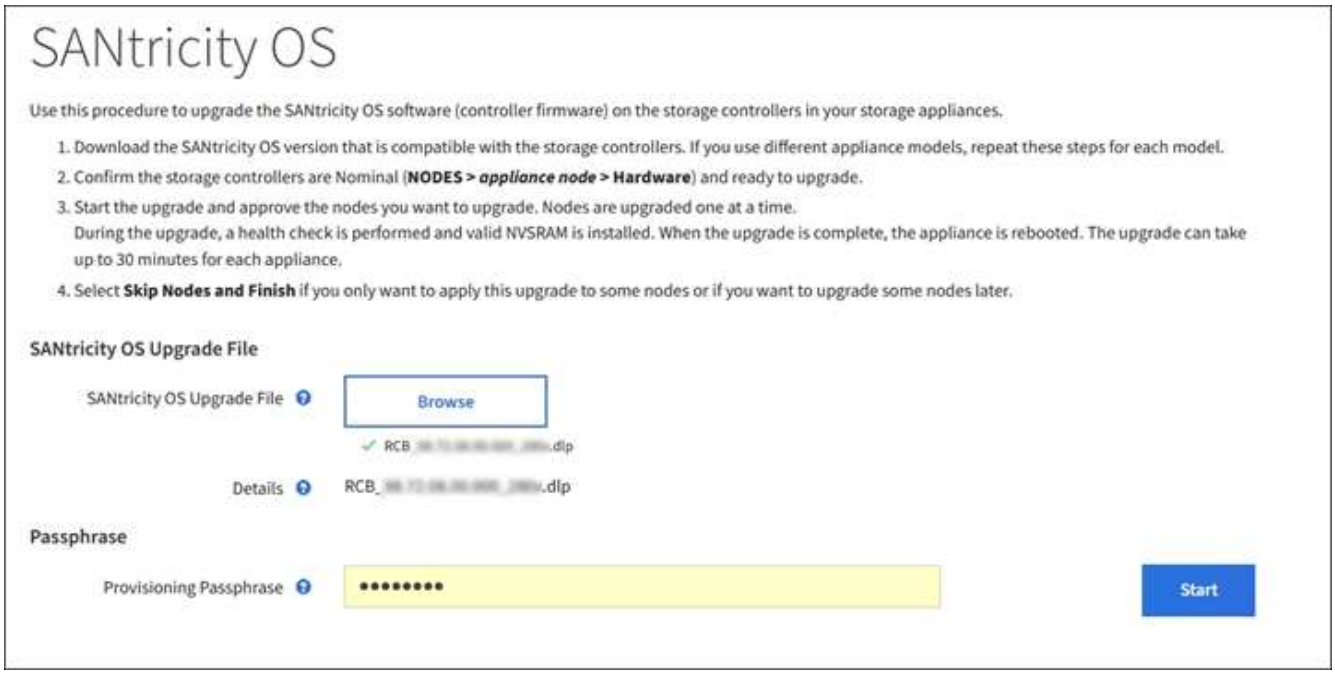
   c. Seleccione **Abrir**.

      El archivo se carga y se valida. Cuando se realiza el proceso de validación, se muestra el nombre del archivo junto al botón **examinar**.

      No cambie el nombre del archivo ya que forma parte del proceso de verificación.

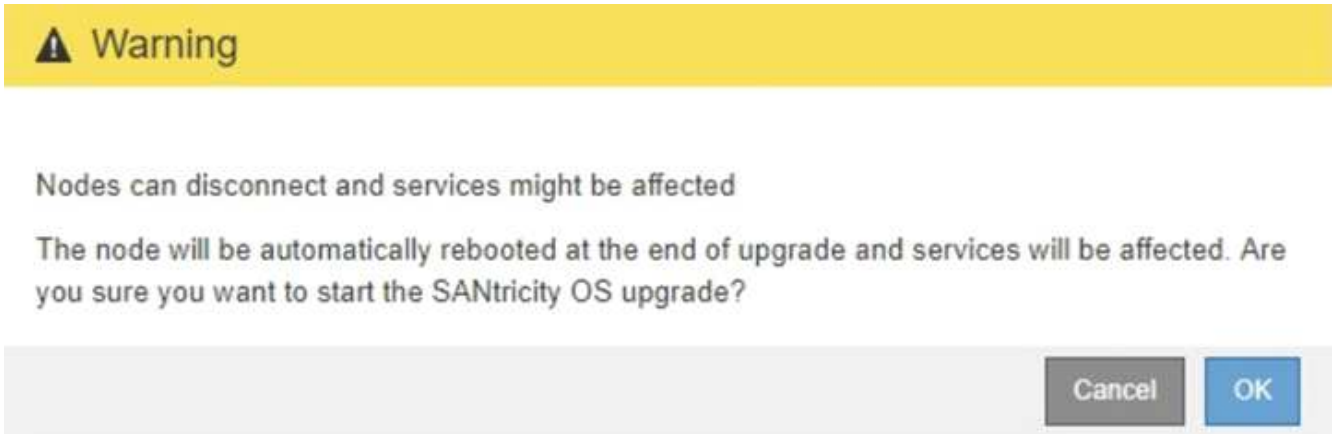
5. Introduzca la clave de acceso de aprovisionamiento.

   El botón **Iniciar** está activado.



6. Seleccione **Iniciar**.

   Aparece un cuadro de advertencia que indica que es posible que se pierda temporalmente la conexión del explorador como se reinician los servicios de los nodos actualizados.



7. Seleccione **Aceptar** para almacenar el archivo de actualización del sistema operativo SANtricity en el nodo de administración principal.

   Cuando se inicia la actualización del sistema operativo SANtricity:

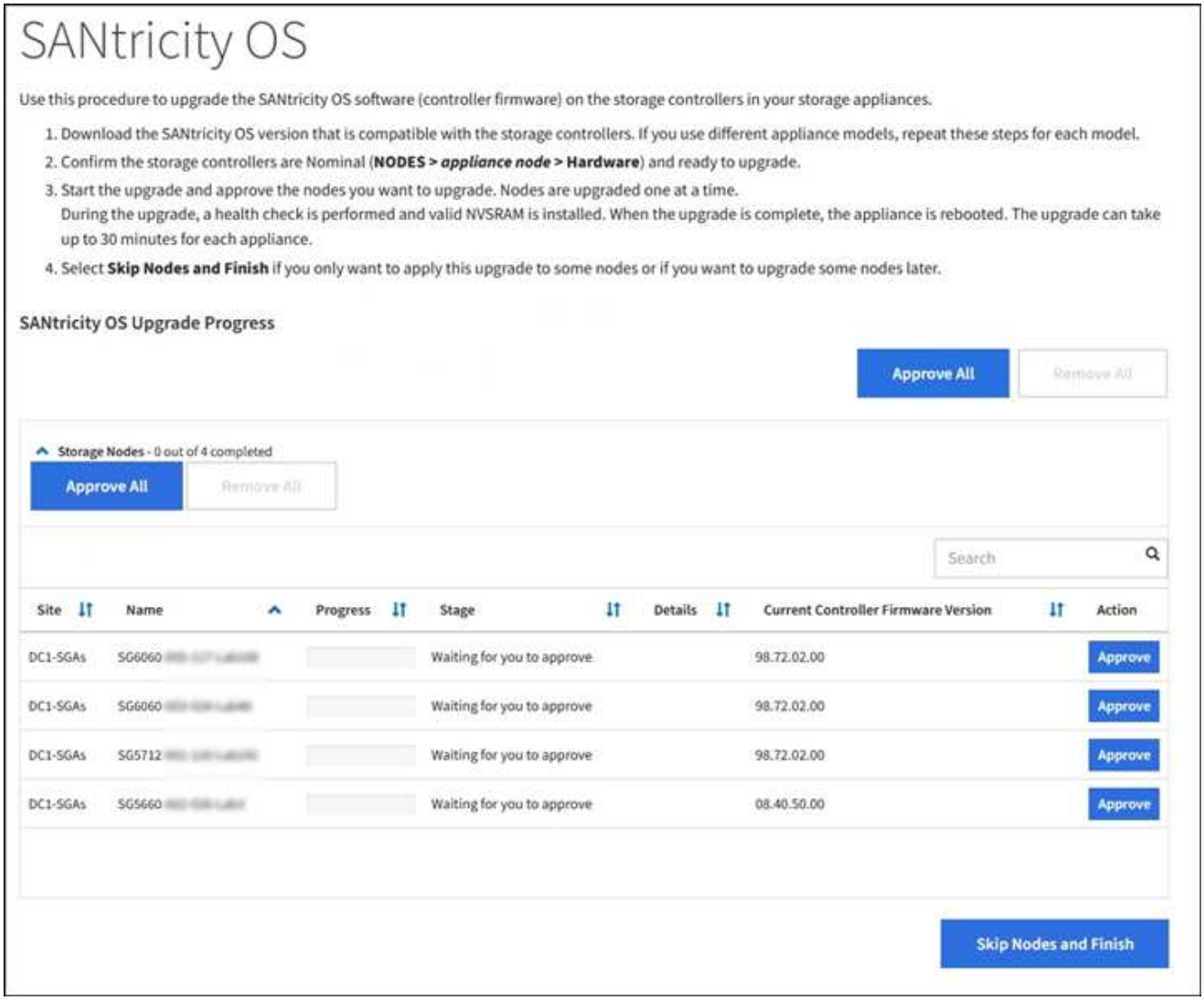
   a. Se ejecuta la comprobación del estado. Este proceso comprueba que ningún nodo tenga el estado de necesita atención.

      Si se informa de algún error, solucione y seleccione **Iniciar** de nuevo.

   b. Se muestra la tabla progreso de actualización de sistema operativo SANtricity. En esta tabla se muestran todos los nodos de almacenamiento del grid y la fase actual de la actualización de cada

nodo.

> La tabla muestra todos los nodos de almacenamiento del dispositivo. No se muestran los nodos de almacenamiento basados en software. Seleccione **aprobar** para todos los nodos que requieran la actualización.



8. Opcionalmente, ordene la lista de nodos en orden ascendente o descendente por **Sitio**, **Nombre**, **progreso**, **etapa**, **Detalles**, O **Versión actual del firmware de la controladora**. O bien, introduzca un término en el cuadro **Buscar** para buscar nodos específicos.

   Puede desplazarse por la lista de nodos utilizando las flechas izquierda y derecha de la esquina inferior derecha de la sección.

9. Apruebe los nodos de cuadrícula que está listo para agregar a la cola de actualización. Los nodos aprobados del mismo tipo se actualizan de uno en uno.

> No apruebe la actualización de SANtricity OS para un nodo de almacenamiento de dispositivos a menos que esté seguro de que el nodo esté listo para detenerse y reiniciar. Cuando la actualización de SANtricity OS se aprueba en un nodo, los servicios de ese nodo se detienen y comienza el proceso de actualización. Más tarde, cuando el nodo finaliza la actualización, el nodo del dispositivo se reinicia. Estas operaciones pueden provocar interrupciones del servicio en los clientes que se comunican con el nodo.

- Seleccione uno de los botones **aprobar todo** para agregar todos los nodos de almacenamiento a la cola de actualización de SANtricity OS.

  > 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 uno o más botones **aprobar** para agregar uno o más nodos a la cola de actualización de SANtricity OS.

  Después de seleccionar **aprobar**, el proceso de actualización determina si se puede actualizar el nodo. Si se puede actualizar un nodo, se agrega a la cola de actualización.

En algunos nodos, el archivo de actualización seleccionado no se aplica de forma intencional, y se puede completar el proceso de actualización sin actualizar estos nodos específicos. Los nodos no actualizados intencionalmente muestran una etapa de completado (intento de actualización) y muestran el motivo por el que el nodo no se actualizó en la columna Details.

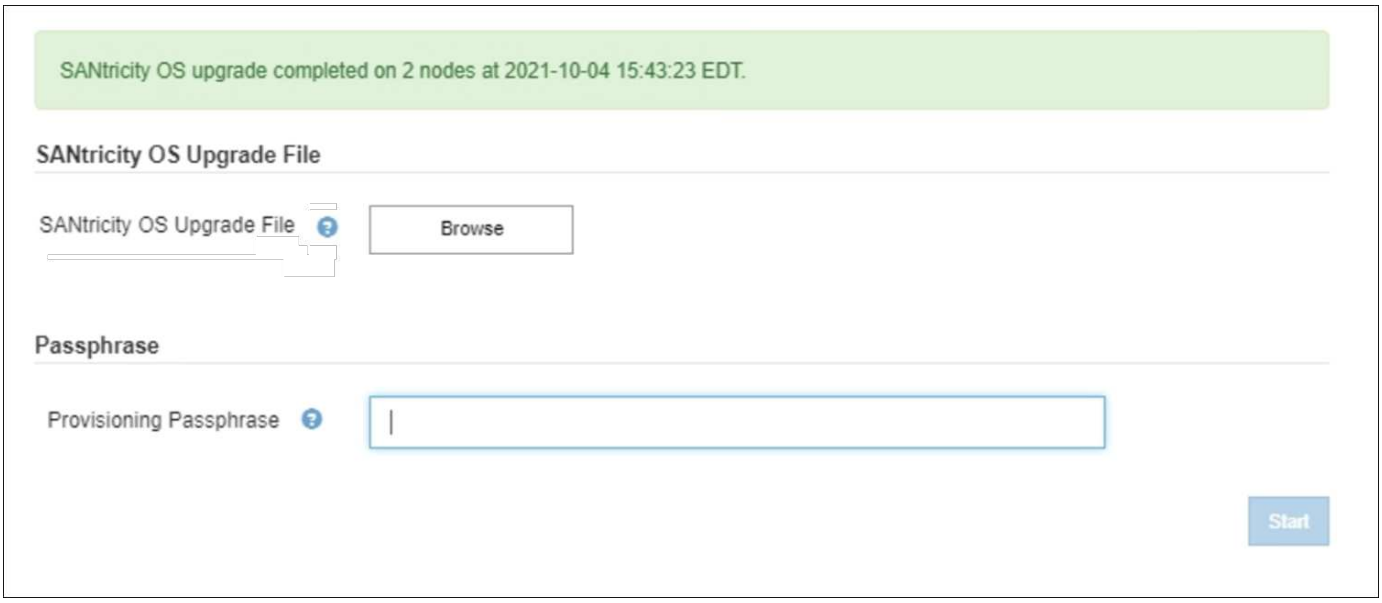
10. Si necesita eliminar un nodo o todos los nodos de la cola de actualización de SANtricity OS, seleccione **Quitar** o **Quitar todo**.

    Cuando la etapa avanza más allá de la cola, el botón **Quitar** está oculto y ya no puede quitar el nodo del proceso de actualización de SANtricity OS.

11. Espere mientras la actualización del SO SANtricity se aplica a cada nodo de grid aprobado.

    - Si alguno de los nodos muestra una etapa de error mientras se aplica la actualización del sistema operativo SANtricity, se produjo un error en la actualización del nodo. Con la ayuda del soporte técnico, es posible que deba colocar el dispositivo en modo de mantenimiento para recuperarlo.
    - Si el firmware del nodo es demasiado antiguo para actualizarse con Grid Manager, el nodo muestra una etapa de error con los detalles: "'debe utilizar el modo de mantenimiento para actualizar SANtricity OS en este nodo. Consulte las instrucciones de instalación y mantenimiento del aparato. Tras la actualización, puede utilizar esta utilidad para futuras actualizaciones». Para resolver el error, haga lo siguiente:
      i. Utilice el modo de mantenimiento para actualizar SANtricity OS en el nodo que muestre una etapa de error.
      ii. Utilice el Administrador de grid para reiniciar y completar la actualización de SANtricity OS.

    Una vez completada la actualización de SANtricity OS en todos los nodos aprobados, la tabla de progreso de la actualización de SANtricity OS se cierra y un banner verde muestra la fecha y la hora en que se completó la actualización de SANtricity OS.



1. Si no se puede actualizar un nodo, tenga en cuenta el motivo que se muestra en la columna Details y realice la acción adecuada:
   - «Ya se ha actualizado el nodo de almacenamiento». No es necesario realizar ninguna otra acción.
   - «'la actualización de SANtricity OS no es aplicable a este nodo». El nodo no tiene una controladora de almacenamiento que pueda gestionar el sistema StorageGRID. Complete el proceso de actualización sin actualizar el nodo que muestra este mensaje.
   - «'el archivo del sistema operativo SANtricity no es compatible con este nodo». El nodo requiere un archivo de SANtricity OS diferente al que seleccionó. Después de completar la actualización actual, descargue el archivo de sistema operativo SANtricity correcto para el nodo y repita el proceso de actualización.

> El proceso de actualización del sistema operativo SANtricity no se completará hasta que apruebe la actualización del sistema operativo SANtricity en todos los nodos de almacenamiento enumerados.

1. Si desea finalizar la aprobación de nodos y volver a la página de SANtricity OS para permitir la carga de un nuevo archivo de SANtricity OS, haga lo siguiente:

   a. Seleccione **Omitir nodos y Finalizar**.

      Aparece una advertencia en la que se pregunta si está seguro de que desea finalizar el proceso de actualización sin actualizar todos los nodos.

   b. Seleccione **Aceptar** para volver a la página **SANtricity OS**.

   c. Cuando esté listo para continuar aprobando nodos, vaya a. Descargue el sistema operativo SANtricity para reiniciar el proceso de actualización.

      > Los nodos ya aprobados y actualizados sin errores siguen actualizando.

2. Repita este procedimiento de actualización para todos los nodos con una etapa de finalización que requieran un archivo de actualización de sistema operativo SANtricity diferente.

   > Para cualquier nodo con el estado necesita atención, utilice el modo de mantenimiento para realizar la actualización.

Cuando repita el procedimiento de actualización, deberá aprobar los nodos actualizados anteriormente.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante el modo de mantenimiento

Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante el modo de mantenimiento

Para las controladoras de almacenamiento que utilizan actualmente el sistema operativo SANtricity con una versión anterior a 08.42.20.00 (11.42), debe utilizar el procedimiento del modo de mantenimiento para aplicar una actualización.

Lo que necesitará

- Ha consultado con la herramienta de matriz de interoperabilidad (IMT) de NetApp para confirmar que la versión del sistema operativo SANtricity que utiliza para la actualización es compatible con su dispositivo.
- Si el dispositivo StorageGRID se ejecuta en un sistema StorageGRID, el controlador SG6000-CN se ha utilizado se pone en modo de mantenimiento.

El modo de mantenimiento interrumpe la conexión a la controladora de almacenamiento.

Acerca de esta tarea

No actualice el sistema operativo SANtricity ni NVSRAM en la controladora E-Series en más de un dispositivo StorageGRID a la vez.

Actualizar más de un dispositivo StorageGRID a la vez puede provocar la falta de disponibilidad de los datos, según el modelo de puesta en marcha y las políticas de ILM.

Pasos

1. Confirme que el aparato está en modo de mantenimiento.
2. Desde un ordenador portátil de servicio, acceda a SANtricity System Manager e inicie sesión.
3. Descargue el nuevo archivo de NVSRAM y de software de sistema operativo SANtricity en el cliente de gestión.

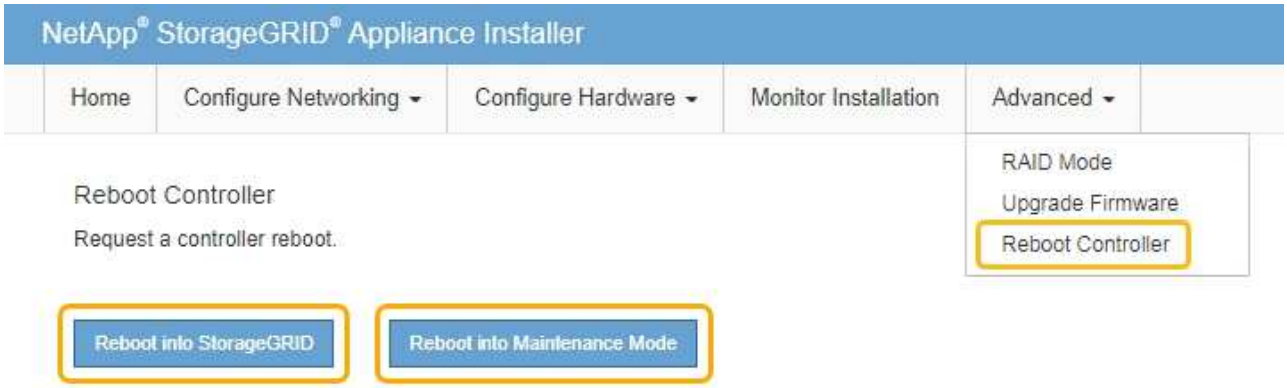
   La NVSRAM es específica del dispositivo StorageGRID. No use la descarga estándar de NVSRAM.

4. Siga las instrucciones de la guía *Upgrade SANtricity OS* o la ayuda en línea de SANtricity System Manager para actualizar el firmware y NVSRAM.

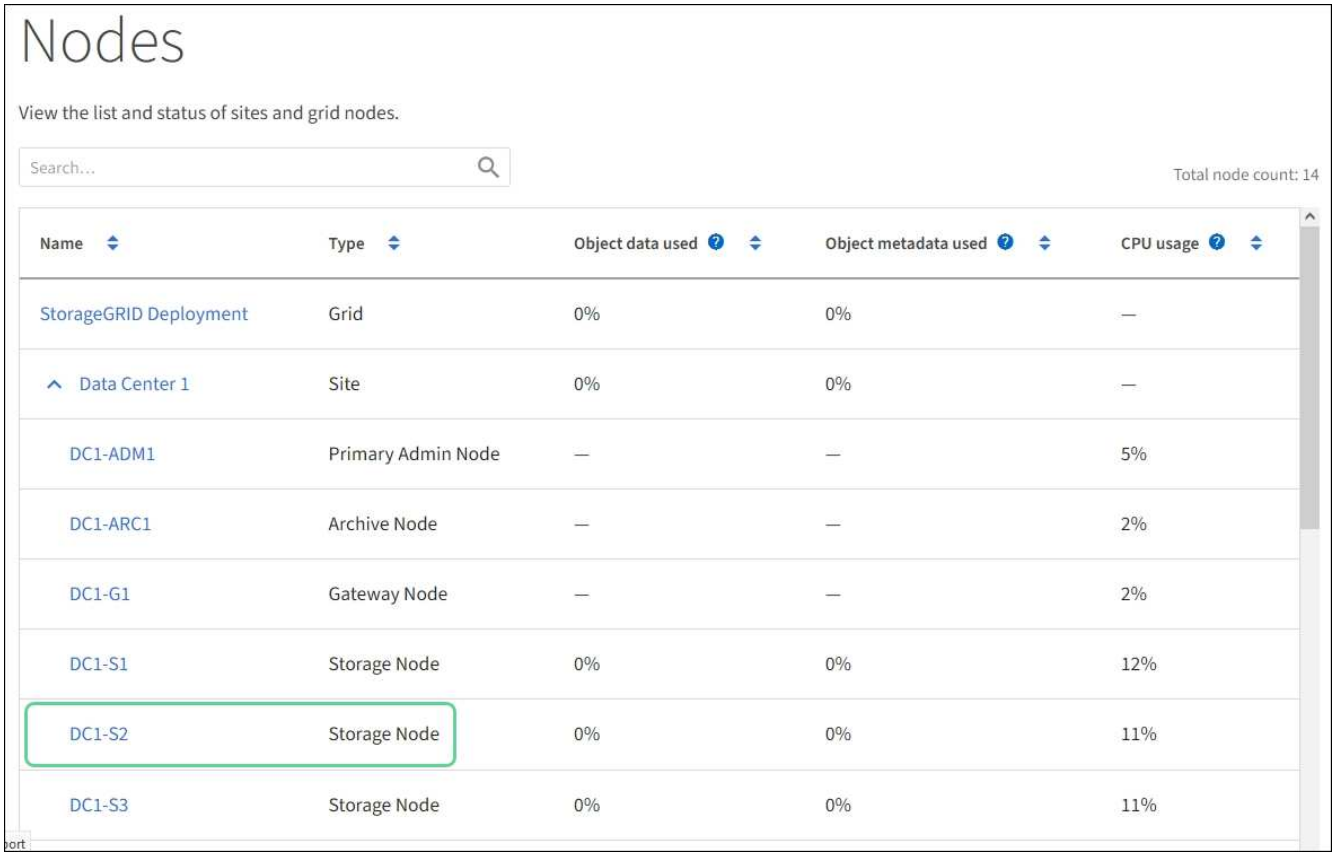
   Active los archivos de actualización inmediatamente. No aplace la activación.

5. Si este procedimiento se completó correctamente y tiene procedimientos adicionales que realizar mientras el nodo se encuentra en modo de mantenimiento, realice ahora. Cuando haya terminado, o si ha experimentado algún fallo y desea volver a empezar, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

- Seleccione **Reiniciar en StorageGRID**
- Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. Seleccione esta opción si ha experimentado algún error durante el procedimiento y desea volver a empezar. Cuando el nodo termine de reiniciarse en el modo de mantenimiento, reinicie desde el paso adecuado del procedimiento en que falló.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página nodos debe mostrar el estado normal (no hay iconos a la izquierda del nombre del nodo) para el nodo de dispositivo, lo que indica que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante Grid Manager

Actualizar el firmware de la unidad mediante System Manager de SANtricity

El firmware de la unidad se actualiza para asegurarse de tener todas las funciones y correcciones de errores más recientes.

Lo que necesitará

- El dispositivo de almacenamiento tiene el estado Optimal.
- Todas las unidades tienen el estado Optimal.
- Tiene instalada la última versión de System Manager de SANtricity que es compatible con la versión de StorageGRID.
- Ya tienes Colocó el dispositivo StorageGRID en modo de mantenimiento.

> El modo de mantenimiento interrumpe la conexión a la controladora de almacenamiento, al detener toda la actividad de I/o y colocar todas las unidades en estado sin conexión.

> No actualice el firmware de la unidad en más de un dispositivo StorageGRID a la vez. Si lo hace, puede provocar la falta de disponibilidad de los datos, según el modelo de puesta en marcha y las políticas de ILM.

Pasos

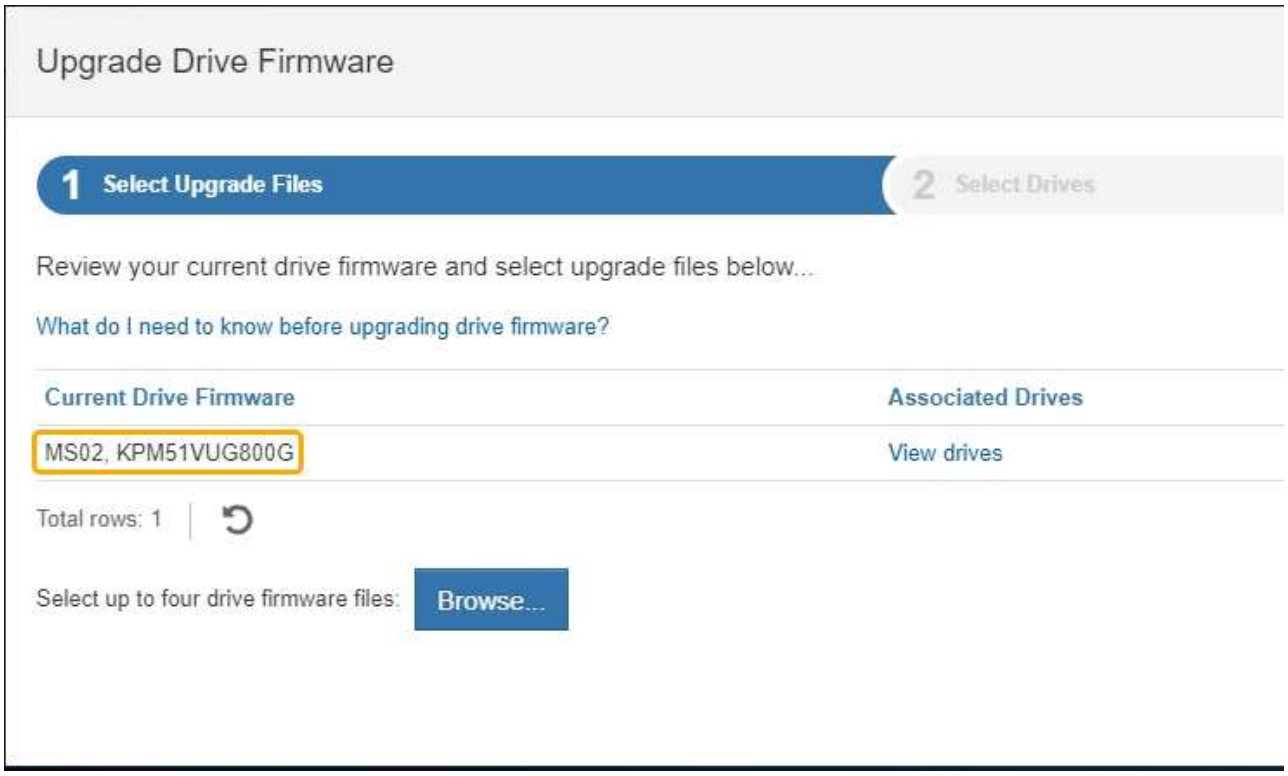
1. Confirme que el aparato está en modo de mantenimiento.
2. Acceda a System Manager de SANtricity mediante uno de estos métodos:
   - Utilice el instalador del dispositivo StorageGRID y seleccione **Avanzado** > **Administrador del sistema SANtricity**
   - Utilice SANtricity System Manager para acceder a la dirección IP de la controladora de almacenamiento:
     `https://Storage_Controller_IP`
3. Si es necesario, introduzca el nombre de usuario y la contraseña del administrador del sistema SANtricity.
4. Compruebe la versión de firmware de la unidad instalada actualmente en el dispositivo de almacenamiento:

   a. En el Administrador del sistema de SANtricity, seleccione **SOPORTE** > **Centro de actualización**.

   b. En actualización del firmware de la unidad, seleccione **Iniciar actualización**.

      El firmware de la unidad de actualización muestra los archivos de firmware de la unidad instalados actualmente.

   c. Tenga en cuenta las revisiones de firmware de la unidad actuales y los identificadores de unidades en la columna firmware de la unidad actual.



En este ejemplo:

- La revisión del firmware de la unidad es **MS02**.
- El identificador de la unidad es **KPM51VUG800G**.

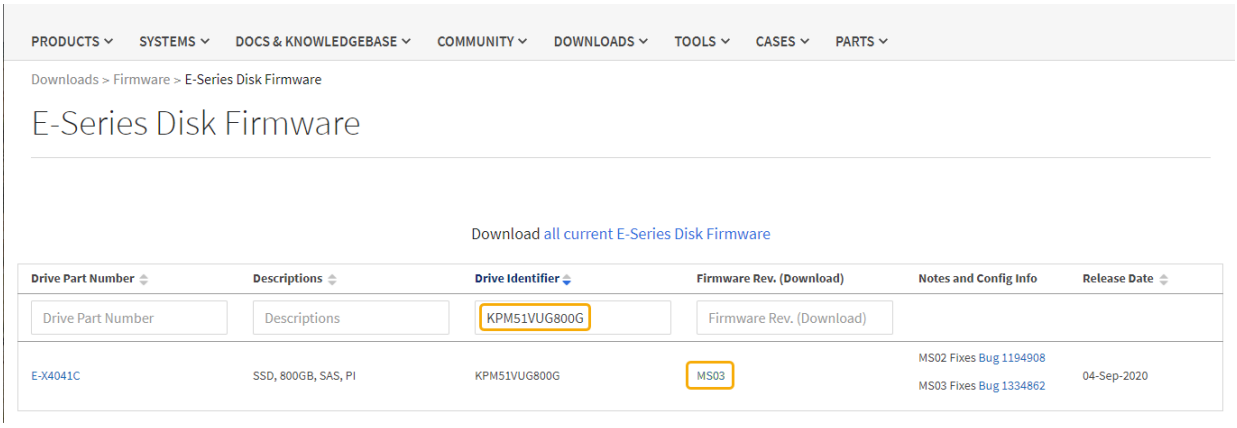
Seleccione **Ver unidades** en la columna unidades asociadas para mostrar dónde están instaladas estas unidades en el dispositivo de almacenamiento.

a. Cierre la ventana Actualizar firmware de la unidad.

5. Descargue y prepare la actualización del firmware de la unidad disponible:
   a. En actualización del firmware de la unidad, seleccione **Soporte de NetApp**.
   b. En el sitio de soporte de NetApp, seleccione la pestaña **Descargas** y, a continuación, seleccione **firmware de las unidades de disco E-Series**.

      Se muestra la página firmware del disco E-Series.

   c. Busque cada **Identificador de unidad** instalado en el dispositivo de almacenamiento y compruebe que cada identificador de unidad tiene la última revisión de firmware.
      - Si la revisión del firmware no es un enlace, este identificador de unidad tiene la revisión de firmware más reciente.
      - Si se enumeran uno o varios números de pieza de unidad para un identificador de unidad, estas unidades tienen disponible una actualización de firmware. Puede seleccionar cualquier enlace para descargar el archivo de firmware.



d. Si aparece una revisión posterior del firmware, seleccione el enlace en la revisión del firmware (Descargar) para descargar una `.zip` archivo que contiene el archivo de firmware.

e. Extraiga (descomprima) los archivos de almacenamiento del firmware de la unidad que descargó del sitio de soporte.

6. Instale la actualización del firmware de la unidad:

a. En el Administrador del sistema de SANtricity, en actualización del firmware de la unidad, seleccione **comenzar actualización**.

b. Seleccione **examinar** y seleccione los nuevos archivos de firmware de la unidad que descargó del sitio de soporte.

   Los archivos de firmware de la unidad tienen un nombre de archivo similar a `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`.

   Es posible seleccionar hasta cuatro archivos de firmware de la unidad, uno por vez. Si más de un archivo de firmware de la unidad es compatible con la misma unidad, se muestra un error de conflicto de archivo. Decida qué archivo de firmware de la unidad desea usar para la actualización y elimine el otro.

c. Seleccione **Siguiente**.

   Select Drives enumera las unidades que se pueden actualizar con los archivos de firmware seleccionados.

   Solo se muestran las unidades que son compatibles.

   El firmware seleccionado para la unidad aparece en **firmware propuesto**. Si debe cambiar este firmware, seleccione **Atrás**.

d. Seleccione **actualización sin conexión (paralelo)**.

   Es posible usar el método de actualización sin conexión debido a que el dispositivo está en modo de mantenimiento, donde se detiene la actividad de I/o de todas las unidades y todos los volúmenes.

> No continúe a menos que esté seguro de que el aparato está en modo de mantenimiento. Si no se coloca el dispositivo en modo de mantenimiento antes de iniciar una actualización del firmware de la unidad sin conexión, se pueden perder datos.

e. En la primera columna de la tabla, seleccione la o las unidades que desea actualizar.

   La práctica recomendada es actualizar todas las unidades del mismo modelo a la misma revisión de firmware.

f. Seleccione **Inicio** y confirme que desea realizar la actualización.

   Si necesita detener la actualización, seleccione **Detener**. Se completa cualquier descarga de firmware actualmente en curso. Se cancela cualquier descarga de firmware que no haya comenzado.

   > Si se detiene la actualización del firmware de la unidad, podrían producirse la pérdida de datos o la falta de disponibilidad de las unidades.

g. (Opcional) para ver una lista de los elementos actualizados, seleccione **Guardar registro**.

   El archivo de registro se guarda en la carpeta de descargas del explorador con el nombre `latest-upgrade-log-timestamp.txt`.

   Si se produce alguno de los siguientes errores durante el procedimiento de actualización, realice la acción recomendada.

   - **Unidades asignadas con errores**

     La causa de este error puede ser que la unidad no tenga la firma apropiada. Asegúrese de que la unidad afectada sea una unidad autorizada. Póngase en contacto con el soporte técnico para obtener más información.

   Al reemplazar una unidad, asegúrese de que la capacidad de la unidad de reemplazo sea igual o mayor que la de la unidad con error que desea reemplazar.

Puede reemplazar la unidad con error mientras la cabina de almacenamiento recibe I/O.

- **Compruebe la matriz de almacenamiento**
  - Asegúrese de que se haya asignado una dirección IP a cada controladora.
  - Asegúrese de que ninguno de los cables conectados a la controladora esté dañado.
  - Asegúrese de que todos los cables estén conectados firmemente.
- **Unidades de repuesto en caliente integradas**

  Es necesario corregir esta condición de error para poder actualizar el firmware.

- **Grupos de volúmenes incompletos**

  Si uno o varios grupos de volúmenes o pools de discos se muestran incompletos, es necesario corregir esta condición de error para poder actualizar el firmware.

- **Operaciones exclusivas (que no sean análisis de medios en segundo plano/paridad) que se estén ejecutando actualmente en cualquier grupo de volúmenes**

  Si existe una o varias operaciones exclusivas en curso, es necesario completarlas para poder actualizar el firmware. Utilice System Manager para supervisar el progreso de las operaciones.

- **Volúmenes que faltan**

Es necesario corregir la condición de volumen ausente para poder actualizar el firmware.

- **Cualquiera de los controladores en un estado distinto al óptimo**

  Se requiere atención en una de las controladoras de la cabina de almacenamiento. Es necesario corregir esta condición para poder actualizar el firmware.

- **La información de partición de almacenamiento no coincide entre los gráficos de objetos del controlador**

  Se produjo un error durante la validación de los datos en las controladoras. Póngase en contacto con el soporte técnico para resolver este problema.

- **La verificación del controlador de base de datos de SPM falla**

  Se produjo un error en la base de datos de asignación de particiones de almacenamiento de una controladora. Póngase en contacto con el soporte técnico para resolver este problema.

- **Validación de la base de datos de configuración (si es compatible con la versión del controlador de la matriz de almacenamiento)**

  Se produjo un error en la base de datos de configuración de una controladora. Póngase en contacto con el soporte técnico para resolver este problema.

- **Comprobaciones relacionadas con MEL**

  Póngase en contacto con el soporte técnico para resolver este problema.

- **Se notificaron más de 10 eventos críticos MEL o informativos DDE en los últimos 7 días**

  Póngase en contacto con el soporte técnico para resolver este problema.

- **Se notificaron más de 2 Eventos críticos MEL de página 2C en los últimos 7 días**

  Póngase en contacto con el soporte técnico para resolver este problema.

- **Se notificaron más de 2 eventos críticos MEL del canal de unidad degradado en los últimos 7 días**

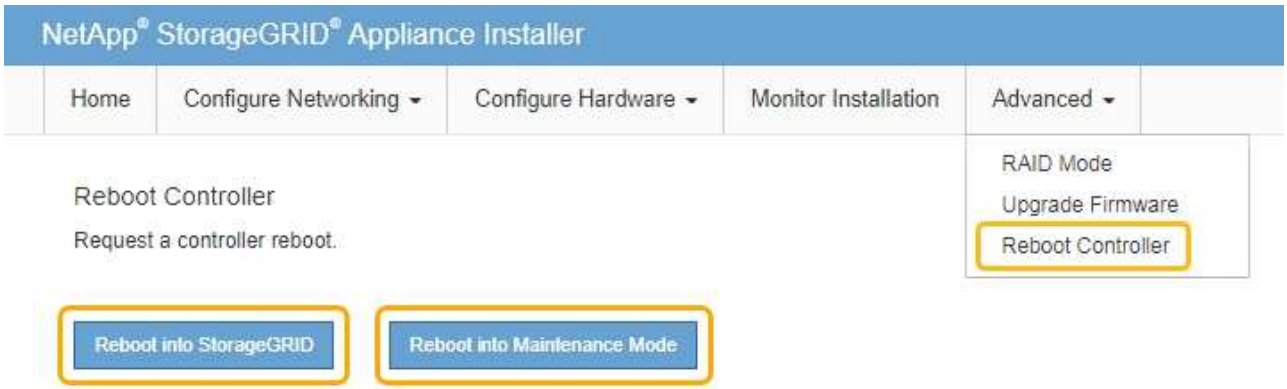
  Póngase en contacto con el soporte técnico para resolver este problema.

- * Más de 4 entradas cruciales MEL en los últimos 7 días*

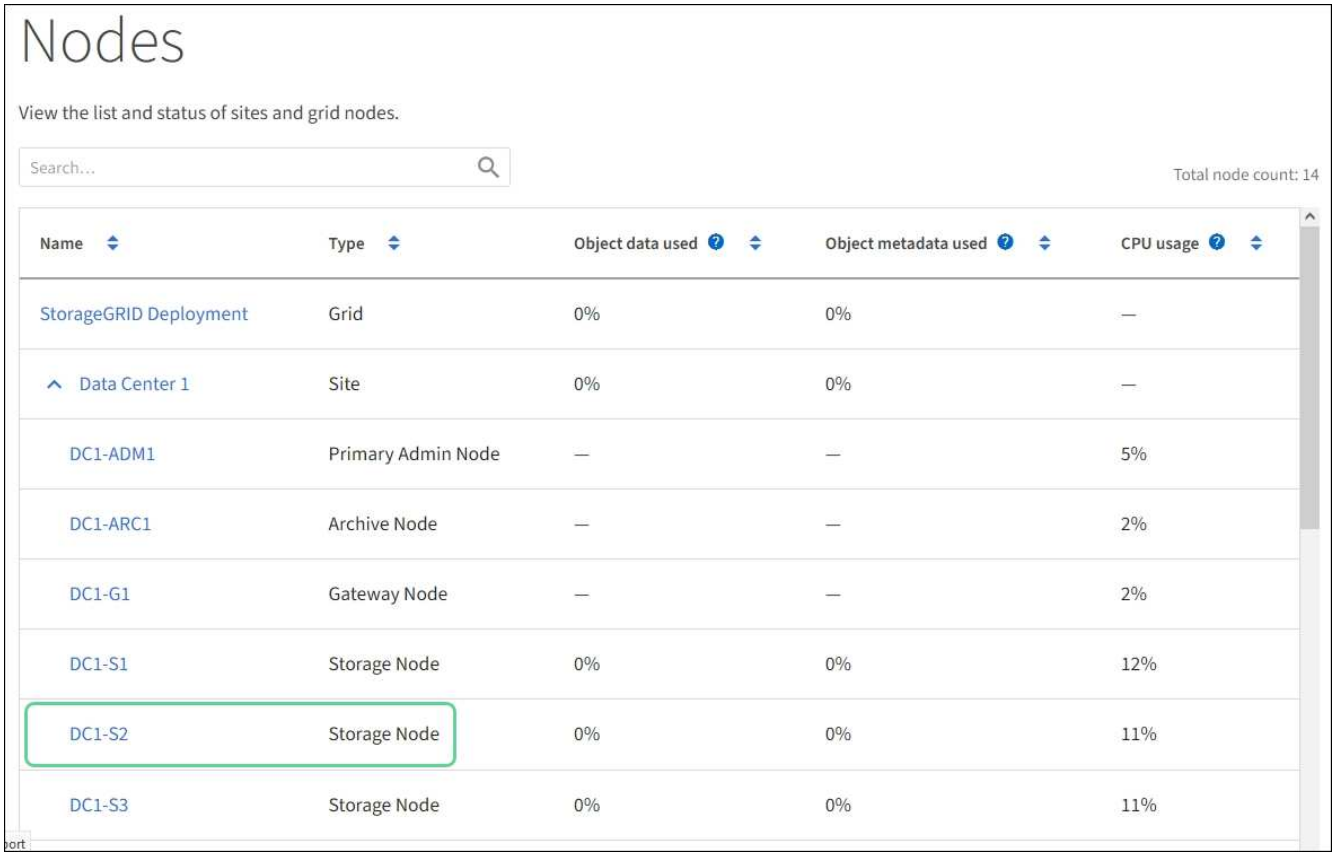
  Póngase en contacto con el soporte técnico para resolver este problema.

7. Si este procedimiento se completó correctamente y tiene procedimientos adicionales que realizar mientras el nodo se encuentra en modo de mantenimiento, realice ahora. Cuando haya terminado, o si ha experimentado algún fallo y desea volver a empezar, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID**
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. Seleccione esta opción si ha experimentado algún error durante el procedimiento y desea volver a empezar. Cuando el nodo termine de reiniciarse en el modo de mantenimiento, reinicie desde el paso adecuado del procedimiento en que falló.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página nodos debe mostrar el estado normal (no hay iconos a la izquierda del nombre del nodo) para el nodo de dispositivo, lo que indica que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Actualizar el sistema operativo SANtricity en las controladoras de almacenamiento

Añada la bandeja de expansión al SG6060 implementado

Para aumentar la capacidad de almacenamiento, es posible añadir una o dos bandejas de expansión a un SG6060 o SG6060X que ya se ha puesto en marcha en un sistema

StorageGRID.

Lo que necesitará

- Debe tener la clave de acceso de aprovisionamiento.
- Debe ejecutar StorageGRID 11.4 o una versión posterior.
- Tiene la bandeja de ampliación y dos cables SAS por cada bandeja de ampliación.
- Ha localizado físicamente el dispositivo de almacenamiento en el que va a añadir la bandeja de ampliación en el centro de datos.

  Ubique la controladora en el centro de datos

Acerca de esta tarea

Para añadir una bandeja de expansión, debe realizar estos pasos de alto nivel:

- Instale la tornillería en el armario o rack.
- Coloque el SG6060 o SG6060X en el modo de mantenimiento.
- Conecte la bandeja de expansión a la bandeja de controladoras E2860 o a otra bandeja de expansión.
- Inicie la ampliación con el instalador de dispositivos de StorageGRID
- Espere hasta que se hayan configurado los nuevos volúmenes.

Completar el procedimiento para una o dos bandejas de expansión debe llevar una hora o menos por nodo del dispositivo. Para minimizar el tiempo de inactividad, los siguientes pasos le indican que debe instalar las nuevas bandejas de expansión y unidades antes de colocar el SG6060 o SG6060X en modo de mantenimiento. El resto de los pasos deben tardar entre 20 y 30 minutos aproximadamente por nodo de dispositivo.

Pasos

1. Siga las instrucciones para instalar bandejas de 60 unidades en un armario o rack.

   SG6060 y SG606060X: Instale bandejas de 60 unidades en el armario o rack

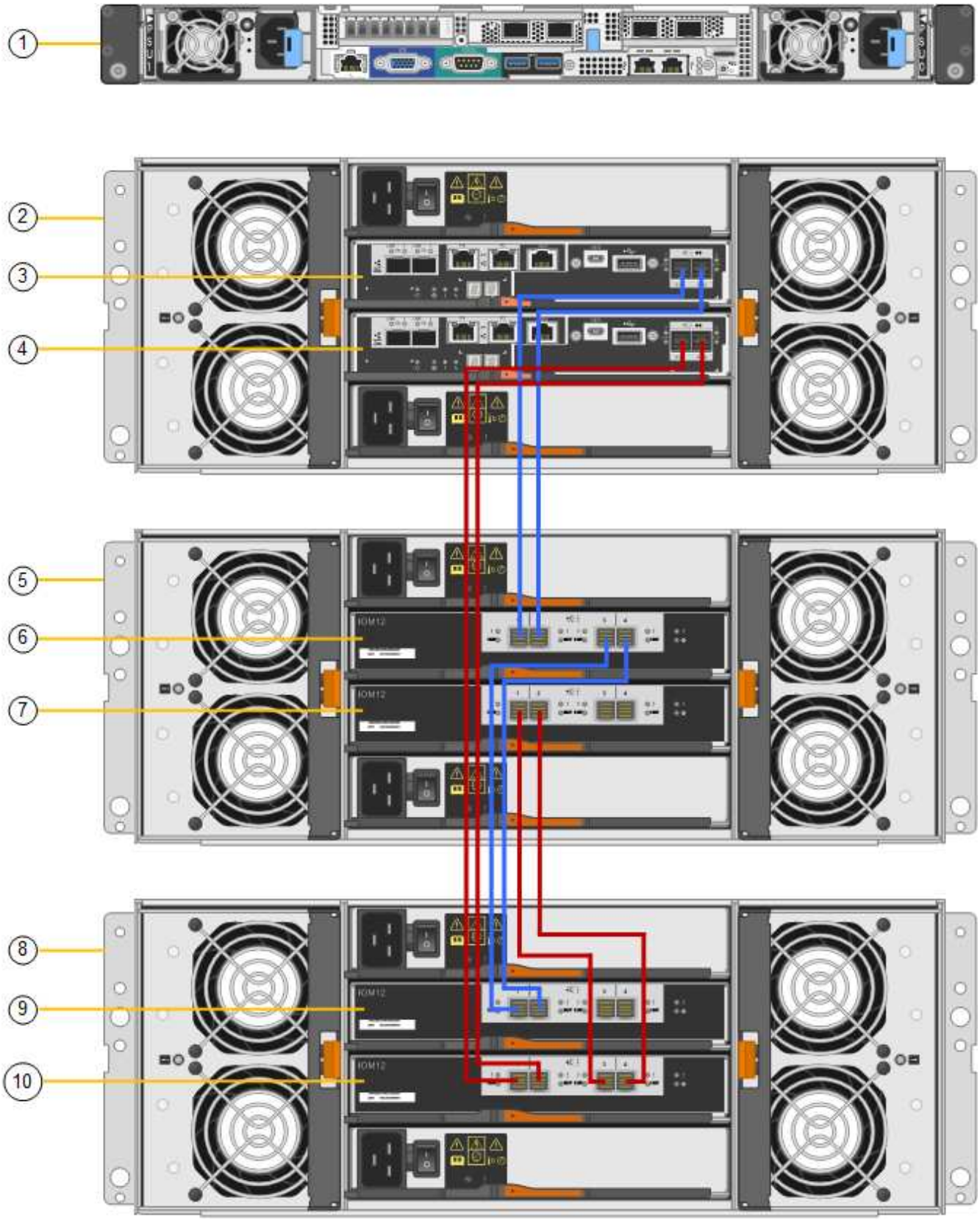
2. Siga las instrucciones de instalación de las unidades.

   SG6060 y SG6060X: Instalación de las unidades

3. Desde Grid Manager, Coloque el controlador SG6000-CN en modo de mantenimiento.
4. Conecte cada bandeja de expansión a la bandeja de controladoras E2860 como se muestra en el diagrama.

   Este dibujo muestra dos estantes de expansión. Si solamente tiene una, conecte IOM A a la controladora A y conecte el IOM B a la controladora B.

   Se muestra el SG6060. El cableado de expansión para el SG606060X es idéntico.



Llamada	Descripción
1	SG6000-CN

Llamada	Descripción
2	Bandeja de controladoras E2860
3	Controladora a
4	Controladora B
5	Bandeja de expansión 1
6	IOM A para la bandeja de ampliación 1
7	IOM B para la bandeja de expansión 1
8	Bandeja de expansión 2
9	IOM A para bandeja de expansión 2
10	IOM B para la bandeja de expansión 2

5. Conecte los cables de alimentación y aplique alimentación a las bandejas de expansión.
   a. Conecte un cable de alimentación a cada una de las dos unidades de alimentación de cada bandeja de expansión.
   b. Conecte los dos cables de alimentación de cada bandeja de expansión a dos PDU diferentes en el armario o rack.
   c. Encienda los dos switches de alimentación para cada bandeja de expansión.
      - No apague los interruptores de alimentación durante el proceso de encendido.
      - Es posible que los ventiladores de las bandejas de ampliación sean muy ruidosos cuando se inician por primera vez. El ruido fuerte durante el arranque es normal.
6. Supervise la página de inicio del instalador de dispositivos de StorageGRID.

   En cinco minutos aproximadamente, las bandejas de expansión finalizan y son detectadas por el sistema. En la página Inicio, se muestra el número de bandejas de expansión nuevas detectadas y el botón Iniciar ampliación está habilitado.

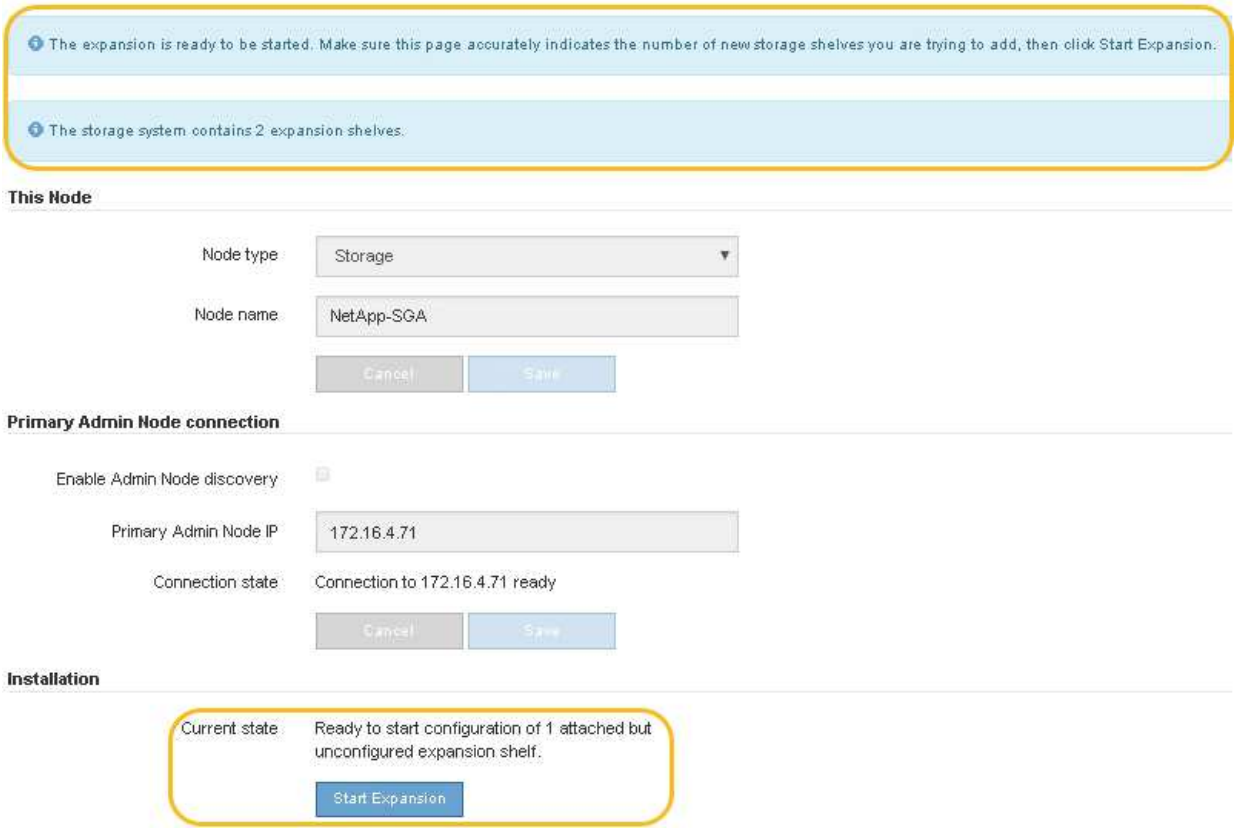
   La captura de pantalla muestra ejemplos de los mensajes que podrían aparecer en la página de inicio, en función del número de bandejas de expansión existentes o nuevas, como se indica a continuación:

   - El banner con un círculo en la parte superior de la página indica el número total de bandejas de expansión detectadas.
     - El banner indica el número total de bandejas de expansión, si las bandejas están configuradas y puestas en marcha o nuevas y sin configurar.
     - Si no se detectan bandejas de expansión, el banner no aparecerá.
   - El mensaje con un círculo en la parte inferior de la página indica que una expansión está lista para iniciarse.
     - El mensaje indica el número de nuevas bandejas de expansión que StorageGRID detecta.

"'adjunto'" indica que se ha detectado el estante. "'Unconfigured'" indica que la bandeja es nueva y aún no se ha configurado mediante el instalador de dispositivos de StorageGRID.

> Las bandejas de expansión que ya se han implementado no se incluyen en este mensaje. Se incluyen en el recuento en el banner en la parte superior de la página.

- No aparecerá el mensaje si no se detectan nuevas bandejas de expansión.



7. Si es necesario, resuelva los problemas descritos en los mensajes de la página de inicio.

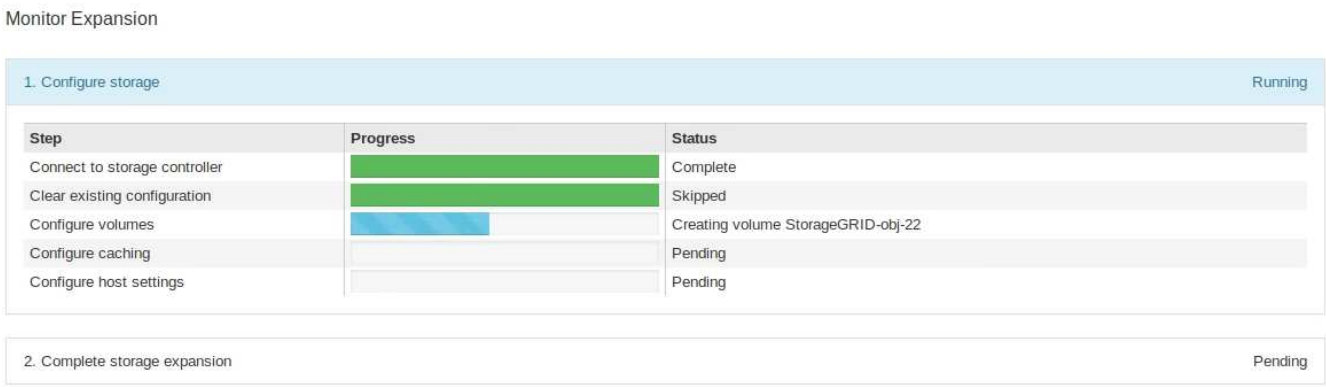
   Por ejemplo, use System Manager de SANtricity para resolver cualquier problema de hardware de almacenamiento.

8. Compruebe que la cantidad de bandejas de expansión que se muestra en la página Inicio coincide con la cantidad de bandejas de expansión que se está añadiendo.

   > Si no se detectan las bandejas de expansión nuevas, compruebe que se hayan conectado correctamente y que se hayan encendido.

9. haga clic en **Iniciar expansión** para configurar las bandejas de expansión y hacer que estén disponibles para el almacenamiento de objetos.
10. Supervise el progreso de la configuración de la bandeja de ampliación.

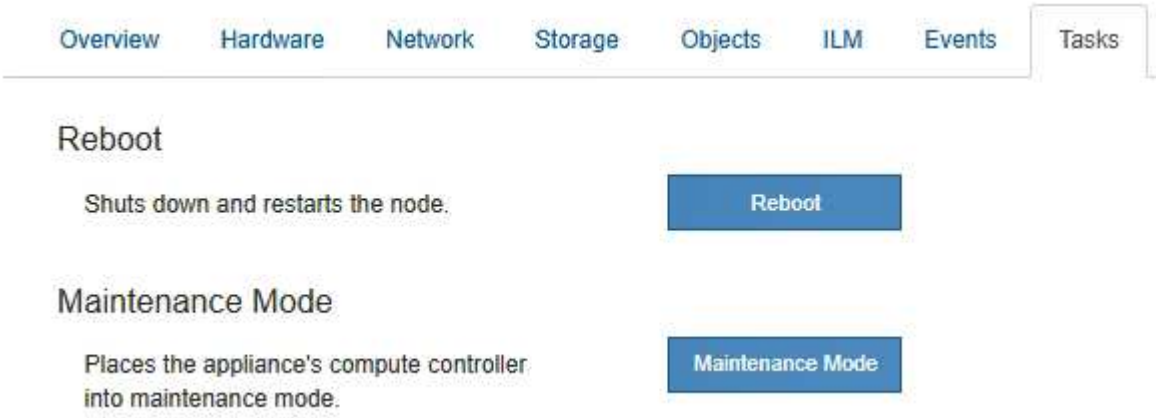
    Las barras de progreso aparecen en la página Web, igual que durante la instalación inicial.



Una vez completada la configuración, el dispositivo se reinicia automáticamente para salir del modo de mantenimiento y volver a unirse a la cuadrícula. Este proceso puede llevar hasta 20 minutos.

> Para volver a intentar la configuración de la bandeja de expansión si falla, vaya al instalador del dispositivo StorageGRID, seleccione **Avanzado Reiniciar controlador** y, a continuación, seleccione **Reiniciar en modo de mantenimiento**. Cuando se haya reiniciado el nodo, vuelva a intentar el configuración de la bandeja de ampliación.

Una vez completado el reinicio, la ficha **tareas** se parece a la siguiente captura de pantalla:



11. Compruebe el estado del nodo de almacenamiento del dispositivo y las nuevas bandejas de ampliación.
    a. En Grid Manager, seleccione **NODOS** y compruebe que el nodo de almacenamiento del dispositivo tiene un icono de Marca de verificación verde.

       El icono de Marca de comprobación de color verde significa que no hay alertas activas y que el nodo está conectado a la cuadrícula. Para obtener una descripción de los iconos de nodo, consulte las instrucciones para supervisar y solucionar problemas de StorageGRID.

    b. Seleccione la ficha **almacenamiento** y confirme que se muestran 16 almacenes de objetos nuevos en la tabla almacenamiento de objetos para cada bandeja de expansión que agregó.
    c. Compruebe que cada bandeja de expansión nueva tenga el estado de bandeja nominal y un estado de configuración de configurado.

Información relacionada

Cajas de desembalaje (SG6000 y SG6060X)

SG6060 y SG606060X: Instale bandejas de 60 unidades en el armario o rack

SG6060 y SG6060X: Instalación de las unidades

Supervisión y solución de problemas

Encender y apagar el LED de identificación de la controladora

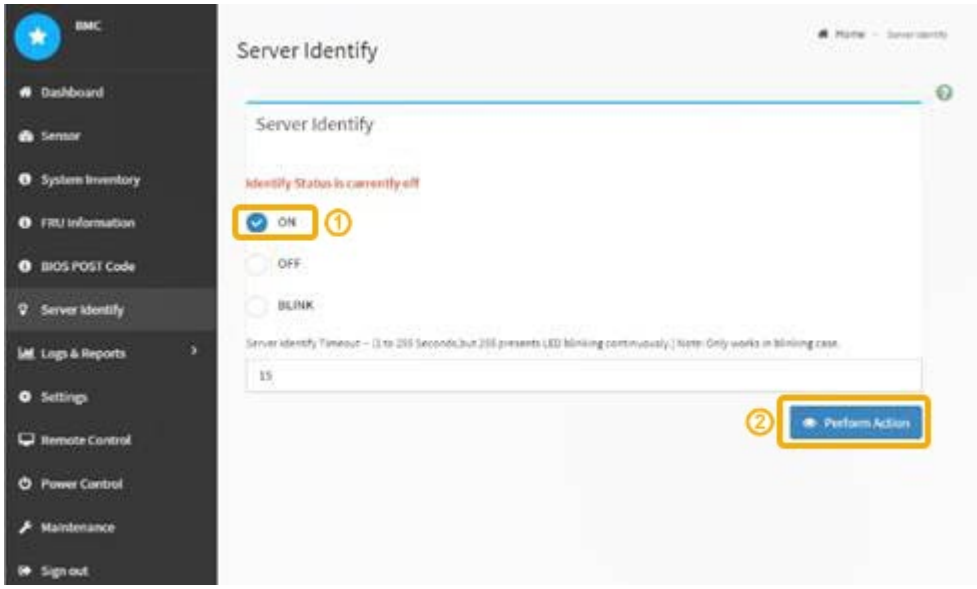
El LED de identificación azul de la parte frontal y trasera de la controladora se puede encender para ayudar a localizar el dispositivo en un centro de datos.

Lo que necesitará

Debe tener la dirección IP del BMC del controlador que desea identificar.

Pasos

1. Acceda a la interfaz del BMC del controlador.
2. Seleccione **Server Identify**.
3. Seleccione **ON** y, a continuación, seleccione **realizar acción**.



Resultado

Los LED de identificación azules se iluminan en la parte frontal (mostrada) y en la parte posterior del controlador.

Si hay un panel frontal instalado en la controladora, es posible que le resulte difícil ver el LED de identificación frontal.

Después de terminar

Para apagar el controlador Identify LED:

- Pulse el interruptor Identify LED del panel frontal del controlador.
- En la interfaz del controlador BMC, seleccione **Server Identify**, seleccione **OFF** y, a continuación, seleccione **realizar acción**.

Los LED azules de identificación de la parte frontal y trasera del controlador se apagan.

Información relacionada

Verifique el adaptador de bus de host de Fibre Channel que desea sustituir

Ubique la controladora en el centro de datos

Acceda a la interfaz de BMC

Ubique la controladora en el centro de datos

Localice la controladora para que pueda realizar tareas de mantenimiento o actualizaciones del hardware.

Lo que necesitará

- Ha determinado qué controlador requiere mantenimiento.

(Opcional) para ayudarle a localizar la controladora en el centro de datos, encienda el LED de identificación azul.

Encender y apagar el LED de identificación de la controladora

Pasos

1. Encuentre la controladora que requiere mantenimiento en el centro de datos.
   - Busque un LED de identificación azul iluminado en la parte frontal o posterior de la controladora.

     El LED de identificación frontal se encuentra detrás del panel frontal de la controladora y puede ser difícil ver si el panel frontal está instalado.

   - Compruebe si las etiquetas adjuntas a la parte frontal de cada controlador tienen un número de pieza coincidente.
2. Retire el embellecedor frontal del controlador, si se ha instalado, para acceder a los controles e indicadores del panel frontal.
3. Opcional: Apague el LED azul de identificación si lo ha utilizado para localizar el controlador.
   - Pulse el interruptor Identify LED del panel frontal del controlador.
   - Use la interfaz del BMC del controlador.

     Encender y apagar el LED de identificación de la controladora

Información relacionada

Quite el HBA Fibre Channel

Retire el controlador SG6000-CN del armario o bastidor

Apague el controlador SG6000-CN

Sustituir el controlador de almacenamiento en el SG6000

Es posible que deba sustituir una controladora serie E2800 o EF570 si no funciona de forma óptima o si ha fallado.

Lo que necesitará

- Tiene una controladora de sustitución con el mismo número de pieza que la controladora que desea sustituir.

- Tiene etiquetas para identificar cada cable conectado a la controladora.
- Tiene una muñequera ESD o ha tomado otras precauciones antiestáticas.
- Tiene un destornillador Phillips del número 1.
- Tiene las instrucciones de E-Series para reemplazar una controladora en configuración doble.

> No confíe en las instrucciones de E-Series para sustituir una controladora en el dispositivo StorageGRID, ya que los procedimientos no son los mismos.

- Localizó físicamente el dispositivo de almacenamiento en el que va a reemplazar la controladora en el centro de datos.

  Ubique la controladora en el centro de datos

Acerca de esta tarea

Puede determinar si tiene una controladora con errores de dos maneras:

- Recovery Guru en System Manager de SANtricity le dirige al usuario reemplazar la controladora.
- El LED de alerta ámbar del controlador está encendido, lo que indica que el controlador tiene un fallo.

> Si ambas controladoras de la bandeja tienen encendidos los LED de atención de ambas controladoras, póngase en contacto con el soporte técnico para obtener ayuda.

Si su dispositivo contiene dos controladoras de almacenamiento, es posible sustituir una de las controladoras mientras el dispositivo está encendido y realizar operaciones de lectura/escritura, siempre que se cumplan las siguientes condiciones:

- La segunda controladora de la bandeja tiene el estado óptimo.
- El campo «'Aceptar para eliminar'» del área Detalles de Recovery Guru en System Manager de SANtricity muestra Sí, lo que indica que es seguro eliminar este componente.

> Cuando sea posible, coloque el aparato en modo de mantenimiento para este procedimiento de sustitución con el fin de minimizar el posible impacto de errores o fallos imprevistos.

> Si la segunda controladora de la bandeja no tiene el estado óptimo o si Recovery Guru indica que no es correcto quitar la controladora, póngase en contacto con el soporte técnico.

Al sustituir una controladora, debe quitar la batería de la controladora original e instalarla en la controladora de reemplazo. En algunos casos, es posible que también necesite quitar la tarjeta de interfaz del host de la controladora original e instalarla en la controladora de reemplazo.

> En la mayoría de los modelos de dispositivos, las controladoras de almacenamiento no incluyen tarjetas de interfaz del host (HIC).

Esta tarea consta de las siguientes partes:

1. Prepare
2. Desconectar la controladora
3. Quite la controladora

4. Mueva la batería a la nueva controladora
5. Si es necesario, mueva HIC a una nueva controladora
6. Sustituya la controladora

Prepare

Pasos

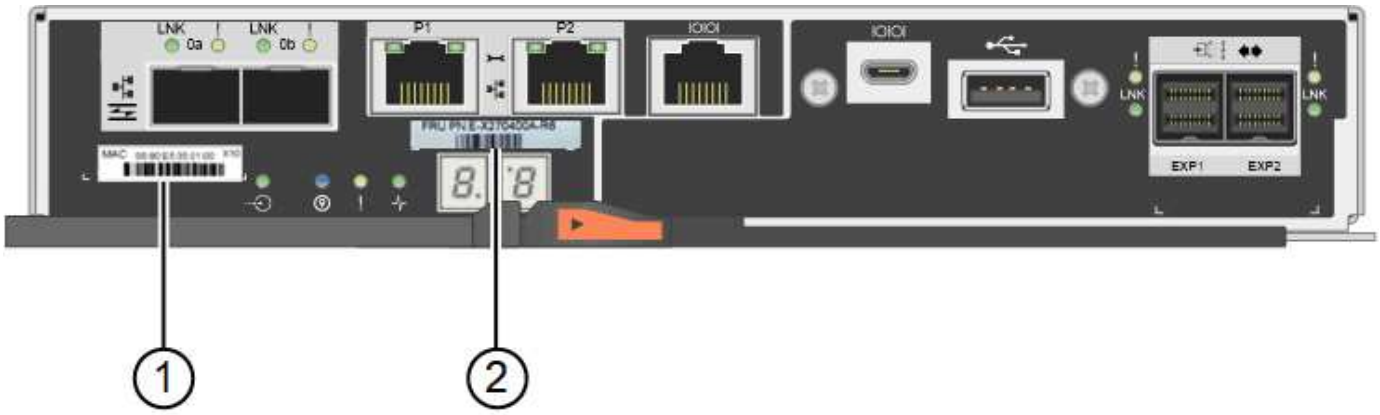
1. Desembale el nuevo controlador y configúrelo en una superficie plana y sin estática.

   Guarde los materiales de embalaje que se van a utilizar durante el envío del controlador que ha fallado.

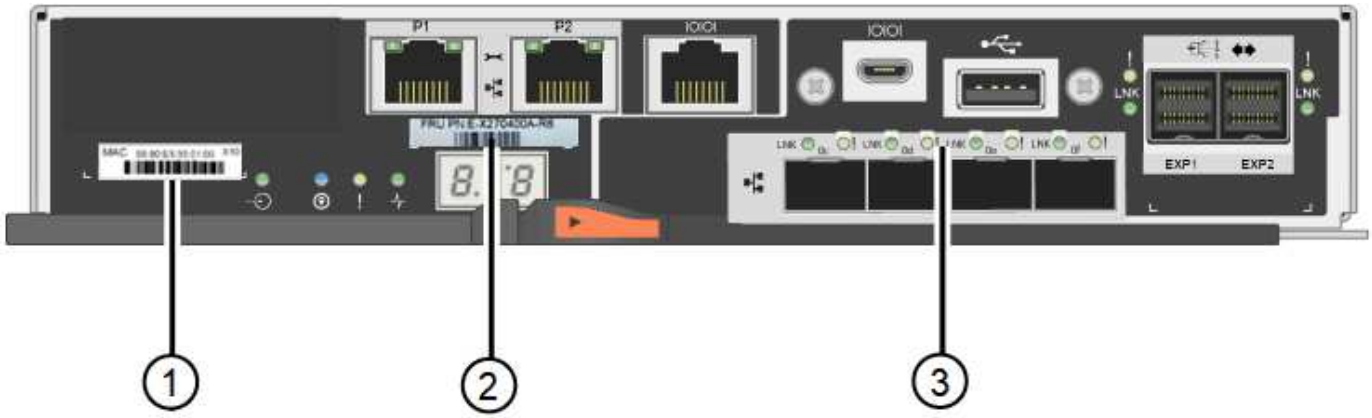
2. Localice las etiquetas de dirección MAC y número de pieza de FRU en la parte posterior de la controladora de reemplazo.

Estas figuras muestran la controladora E2800A y la controladora E2800B. El procedimiento para sustituir las controladoras de la serie E2800 y la controladora EF570 es idéntico.

E2800A Storage Controller



E2800B Storage Controller



Etiqueta	componente	Descripción
1	Dirección MAC	La dirección MAC para el puerto de gestión 1 ("'P1 en el E2800A y 0a en la E2800B'"). Si utilizó DHCP para obtener la dirección IP de la controladora original, necesitará esta dirección para conectarse a la nueva controladora.
2	Número de pieza de FRU	El número de pieza de FRU. Este número debe coincidir con el número de pieza de repuesto de la controladora instalada actualmente.
3	HIC de 4 puertos	La tarjeta de interfaz del host (HIC) de 4 puertos. Esta tarjeta se debe mover al nuevo controlador cuando realice la sustitución. **Nota**: El controlador E2800A no tiene HIC.

Desconectar la controladora

Pasos

1. Prepárese para quitar el controlador. SANtricity System Manager se utiliza para realizar estos pasos.

   a. Confirmar que el número de pieza de repuesto de la controladora con errores es el mismo que el número de pieza de FRU de la controladora de reemplazo.

   Cuando una controladora tiene un error y se debe sustituir, el número de pieza de repuesto se muestra en el área Detalles de Recovery Guru. Si necesita encontrar este número manualmente, puede buscar en la ficha **base** del controlador.

   > **Posible pérdida de acceso a datos #8212;** Si los dos números de pieza no son iguales, no intente este procedimiento.

   a. Realice un backup de la base de datos de configuración.

   Si se produce un problema al quitar una controladora, puede usar el archivo guardado para restaurar la configuración.

   b. Recopile datos de soporte del dispositivo.

   > La recogida de datos de soporte antes y después de reemplazar un componente garantiza que se pueda enviar un conjunto completo de registros al soporte técnico en caso de que el reemplazo no resuelva el problema.

   c. Cambie la controladora que desea sustituir sin conexión.

Quite la controladora

Pasos

1. Retire el controlador del dispositivo:

   a. Coloque una muñequera ESD o tome otras precauciones antiestáticas.

b. Etiquete los cables y desconecte los cables y SFP.

> Para evitar un rendimiento degradado, no gire, pliegue, pellizque ni pellizque los cables.

c. Suelte el controlador del aparato apretando el pestillo del asa de la leva hasta que se suelte y, a continuación, abra el asa de leva a la derecha.

d. Con dos manos y el mango de la leva, deslice el controlador para sacarlo del aparato.

> Utilice siempre dos manos para soportar el peso del controlador.

e. Coloque el controlador sobre una superficie plana y sin estática con la cubierta extraíble hacia arriba.

f. Retire la cubierta presionando el botón y deslizando la cubierta hacia fuera.

Mueva la batería a la nueva controladora

Pasos

1. Retire la batería de la controladora con errores e instálela en la controladora de reemplazo:

   a. Confirme que el LED verde dentro del controlador (entre la batería y los DIMM) está apagado.

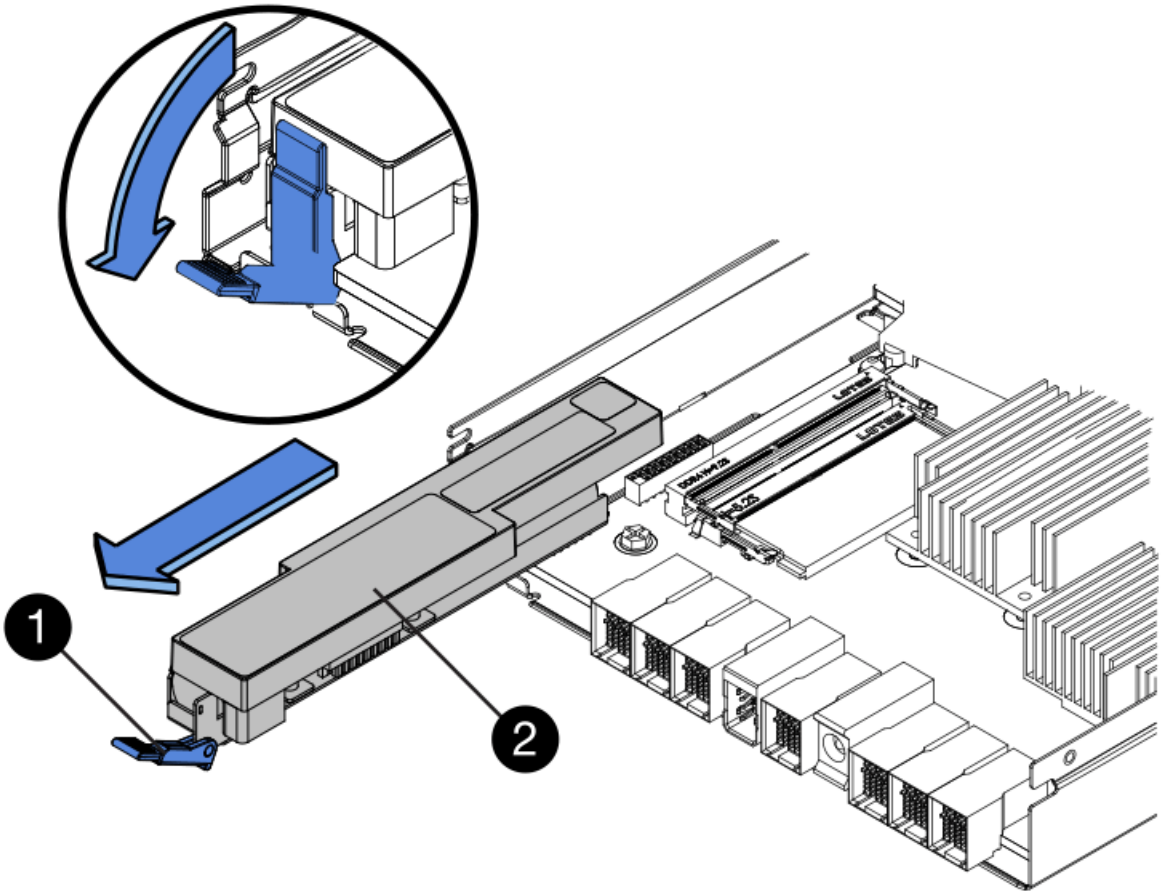
   Si este LED verde está encendido, el controlador sigue utilizando la batería. Debe esperar a que este LED se apague antes de quitar los componentes.

Elemento	Descripción
1	LED de caché interna activa

Elemento	Descripción
2	Batería

b. Localice el pestillo de liberación azul de la batería.

c. Para desenganchar la batería, presione el pestillo de liberación hacia abajo y hacia fuera del controlador.



Elemento	Descripción
1	Pestillo de liberación de la batería
2	Batería

d. Levante la batería y deslícela fuera del controlador.

e. Retire la cubierta del controlador de recambio.

f. Oriente el controlador de repuesto de manera que la ranura de la batería quede orientada hacia usted.

g. Inserte la batería en el controlador en un ángulo ligeramente descendente.

Debe insertar la brida metálica de la parte frontal de la batería en la ranura de la parte inferior del controlador y deslizar la parte superior de la batería por debajo del pasador de alineación pequeño del

lado izquierdo del controlador.

h. Mueva el pestillo de la batería hacia arriba para fijar la batería.

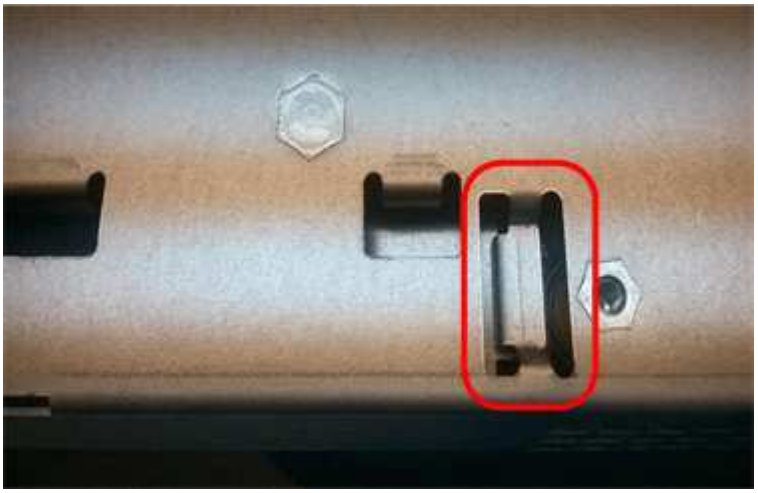
   Cuando el pestillo hace clic en su lugar, la parte inferior del pestillo se engancha a una ranura metálica del chasis.

i. Dé la vuelta al controlador para confirmar que la batería está instalada correctamente.

> **Posible daño de hardware** — la brida metálica de la parte frontal de la batería debe estar completamente insertada en la ranura del controlador (como se muestra en la primera figura). Si la batería no está instalada correctamente (como se muestra en la segunda figura), la brida metálica podría entrar en contacto con la placa del controlador, causando daños.

- **Correcto — la brida metálica de la batería está completamente insertada en la ranura del controlador:**

- **Incorrecto — la brida metálica de la batería no está insertada en la ranura del controlador:**



2. Vuelva a colocar la cubierta del controlador.

Si es necesario, mueva HIC a una nueva controladora

Pasos

1. Si la controladora con errores incluye una tarjeta de interfaz del host (HIC), mueva la HIC de la controladora con error a la controladora de reemplazo.

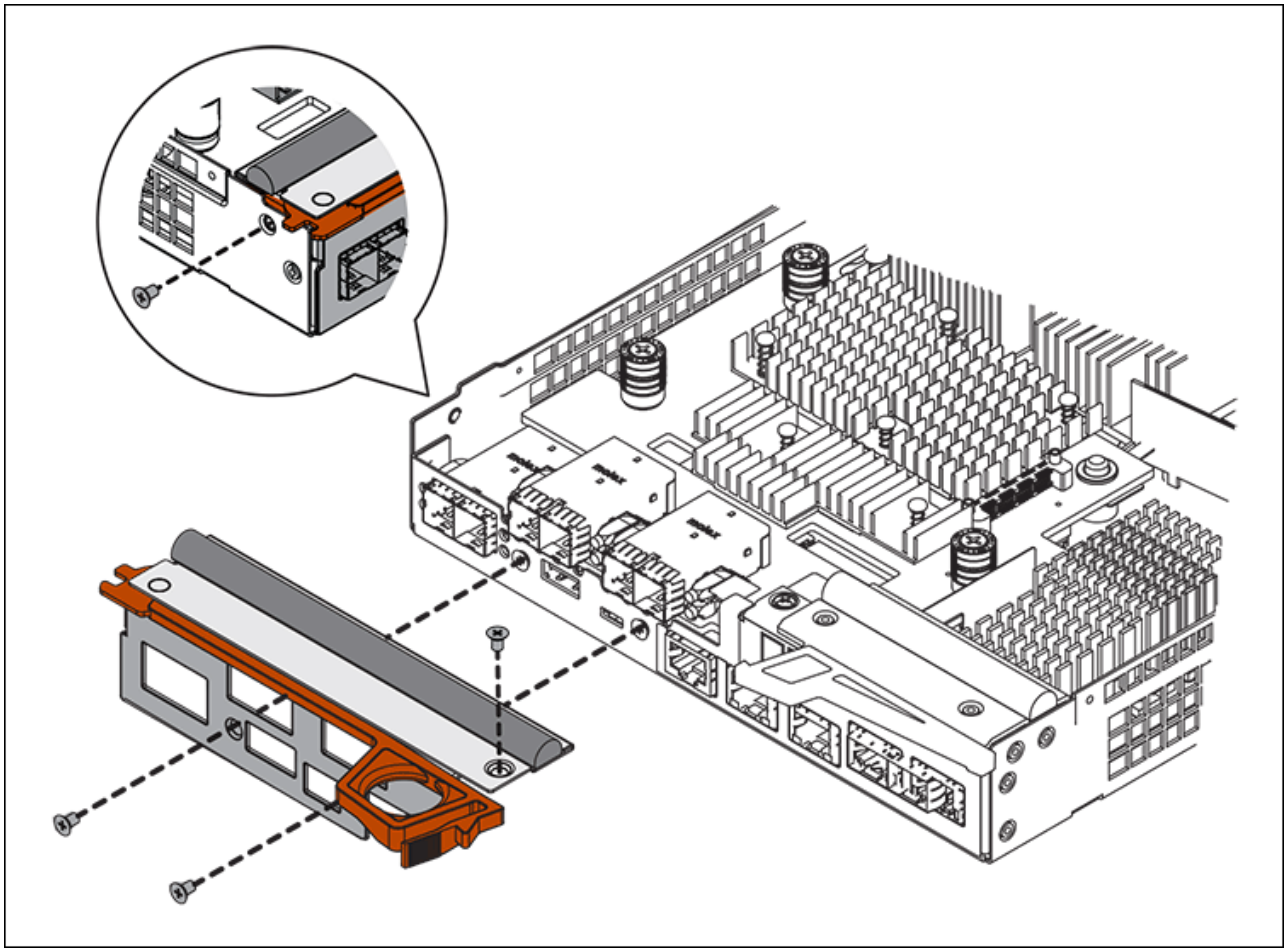
   Una HIC independiente se utiliza únicamente para la controladora E2800B. La HIC se monta en la placa del controlador principal e incluye dos conectores SPF.

   > Las ilustraciones de este procedimiento muestran una HIC de 2 puertos. La HIC de la controladora puede tener una cantidad de puertos diferente.

2. Si la controladora no tiene una HIC (E2800A), reemplace la cubierta de la controladora. Si la controladora tiene una HIC (E2800B), continúe a. Mueva la HIC de la controladora con errores a la controladora de reemplazo.

   a. Si está equipado con una HIC, mueva la HIC de la controladora con error a la controladora de reemplazo.
   b. Quite todos los SFP de la HIC.
   c. Con un destornillador Phillips del número 1, quite los tornillos que conectan la placa frontal de HIC a la controladora.

      Hay cuatro tornillos: Uno en la parte superior, uno en el lateral y dos en la parte delantera.

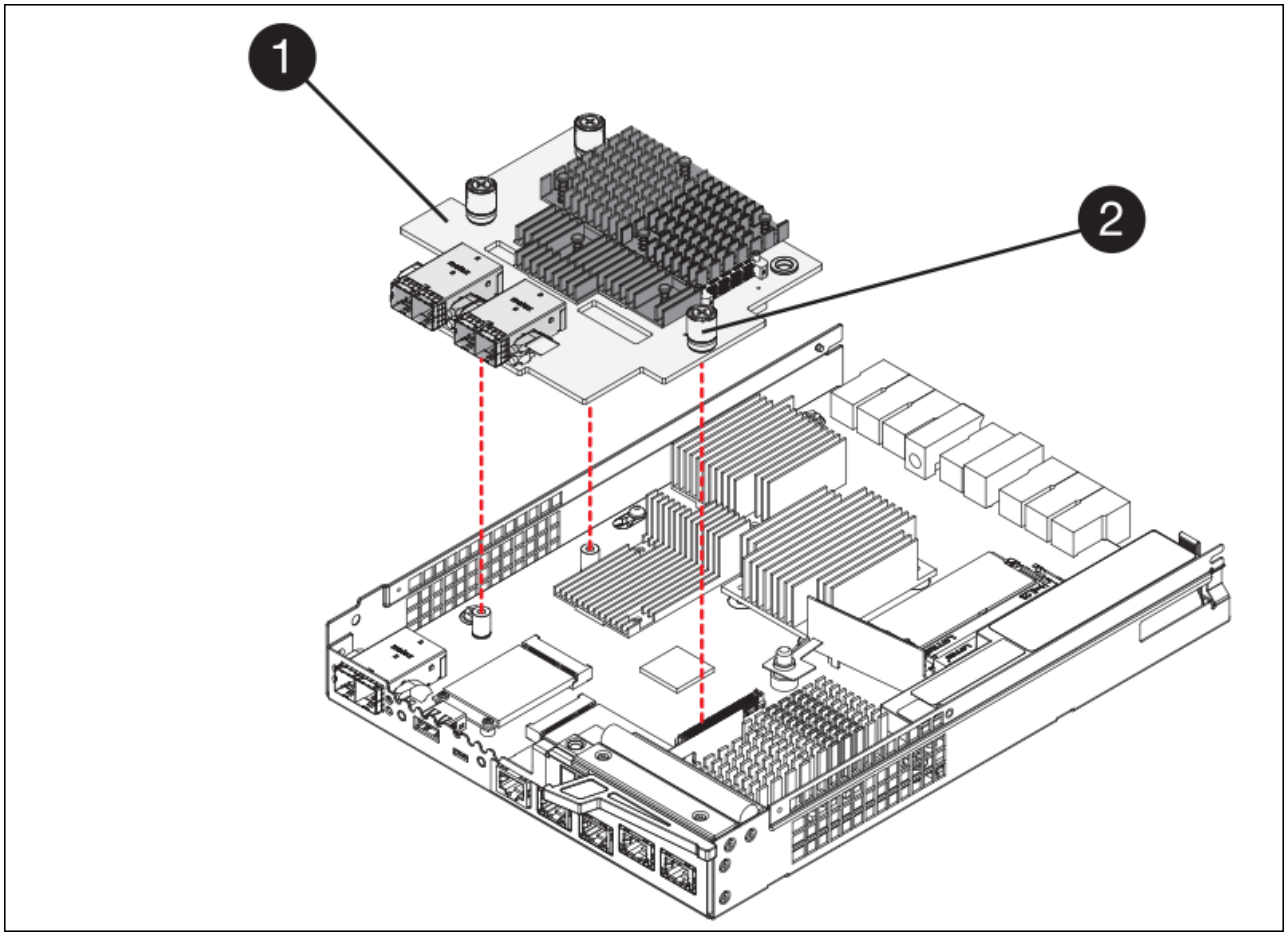


   d. Quite la placa frontal de HIC.

e. Con los dedos o un destornillador Phillips, afloje los tres tornillos de ajuste manual que fijan la HIC a la tarjeta controladora.

f. Retire con cuidado la tarjeta HIC de la tarjeta controladora levantando la tarjeta y deslizándola hacia atrás.

> Tenga cuidado de no arañar ni golpear los componentes en la parte inferior de la HIC o en la parte superior de la tarjeta de la controladora.



Etiqueta	Descripción
1	Tarjeta de interfaz del host
2	Tornillos de apriete manual

g. Coloque la HIC en una superficie sin estática.

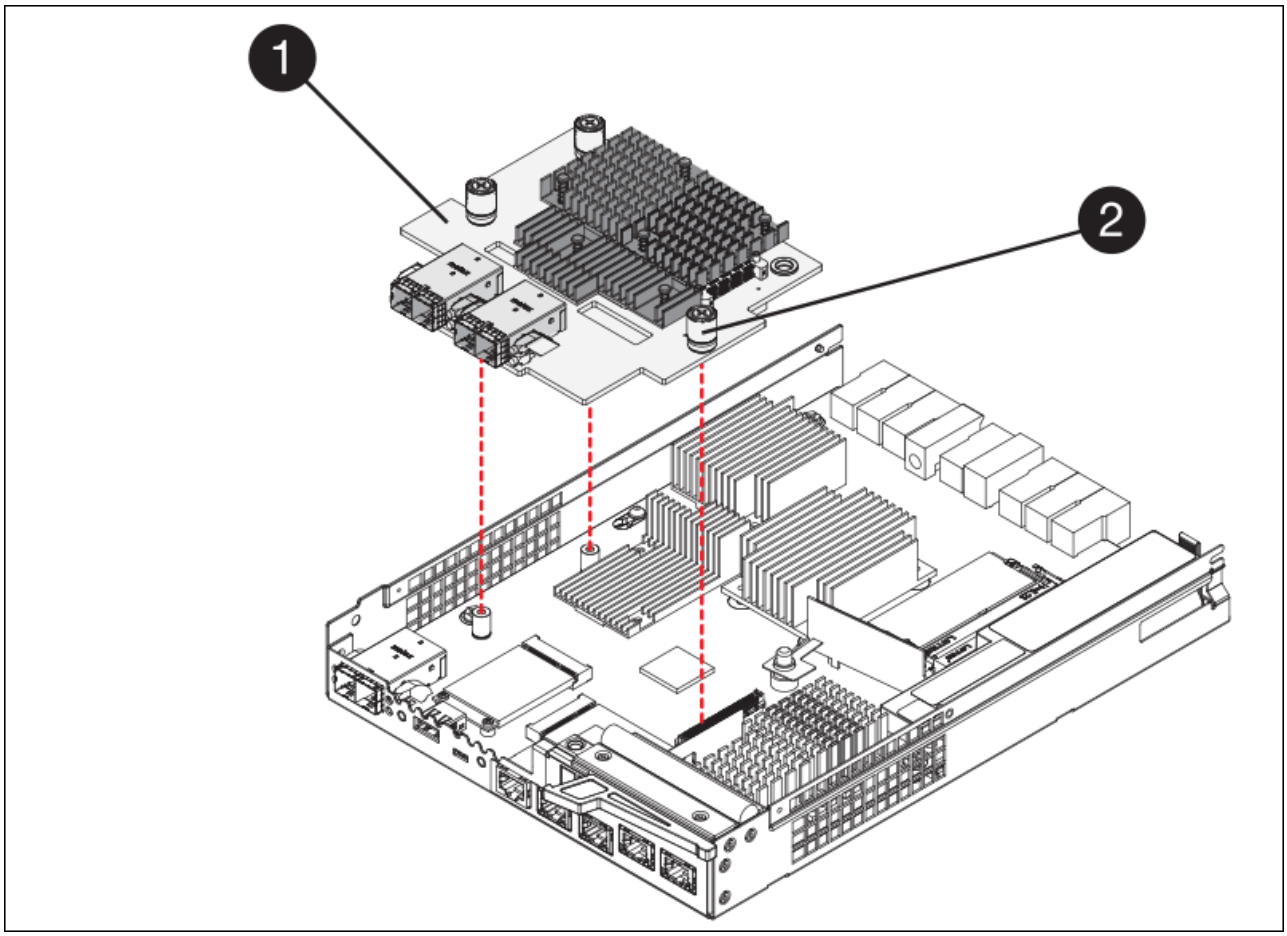
h. Con un destornillador Phillips del número 1, quite los cuatro tornillos que fijan la placa frontal vacía al controlador de repuesto y quite la placa frontal.

i. Alinee los tres tornillos de apriete manual de la HIC con los orificios correspondientes de la controladora de reemplazo y alinee el conector de la parte inferior de la HIC con el conector de la interfaz HIC de la tarjeta controladora.

   Tenga cuidado de no arañar ni golpear los componentes en la parte inferior de la HIC o en la parte superior de la tarjeta de la controladora.

j. Baje con cuidado la HIC en su lugar y coloque el conector de la HIC presionando suavemente en la HIC.

> **Posible daño en el equipo** — tenga mucho cuidado de no pellizcar el conector de la cinta de oro para los LED del controlador entre la HIC y los tornillos de mariposa.

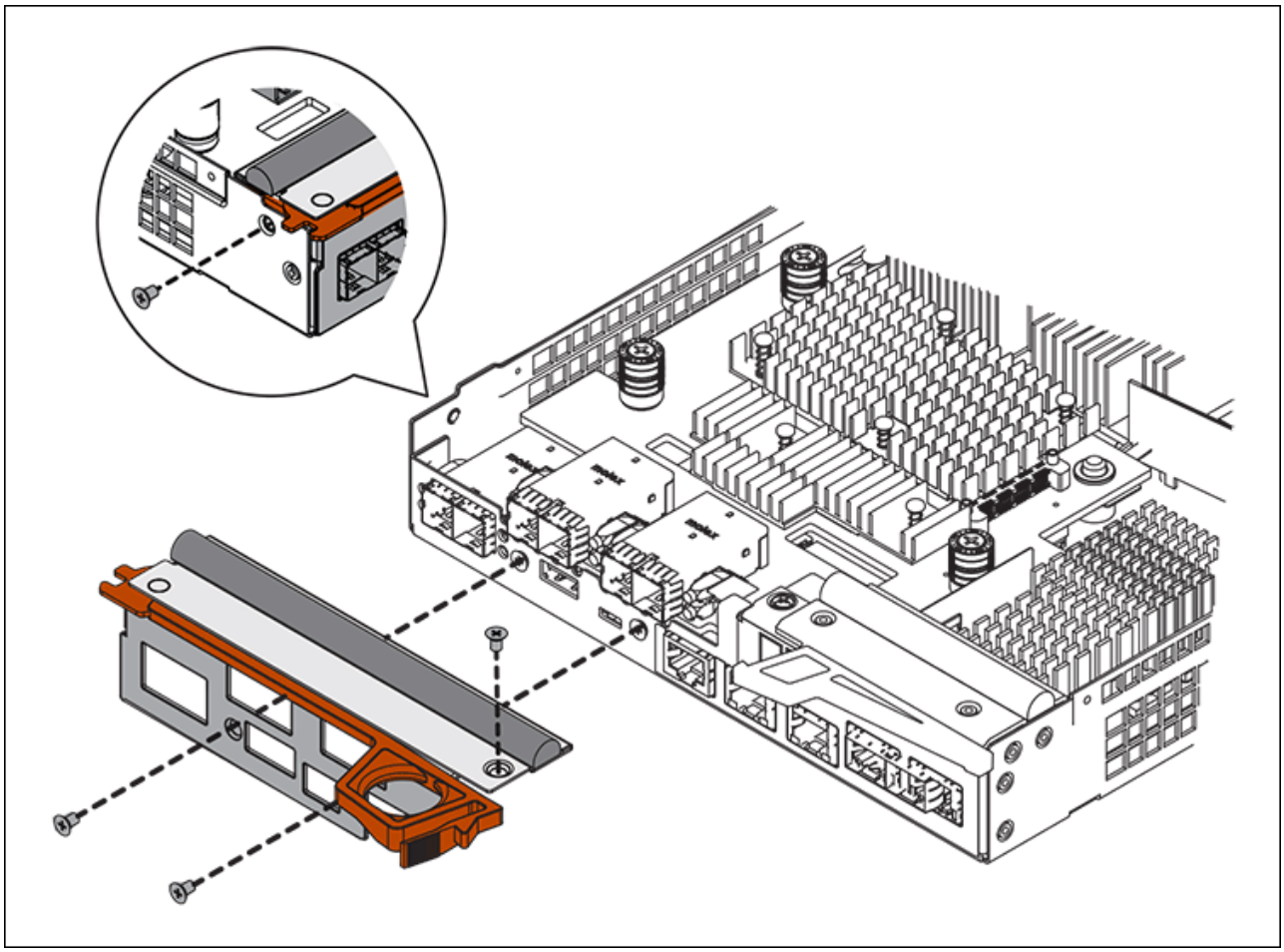


Etiqueta	Descripción
1	Tarjeta de interfaz del host
2	Tornillos de apriete manual

a. Apriete a mano los tornillos de mariposa HIC.

   No utilice un destornillador, o puede apretar los tornillos en exceso.

b. Con un destornillador Phillips del número 1, conecte la placa frontal de la HIC que quitó de la controladora original a la nueva controladora con cuatro tornillos.



c. Vuelva a instalar todos los SFP que se hayan quitado en la HIC.

Sustituya la controladora

Pasos

1. Instale el controlador de repuesto en el aparato.
   a. Dé la vuelta al controlador de modo que la cubierta extraíble quede orientada hacia abajo.
   b. Con el mango de la leva en la posición abierta, deslice el controlador completamente en el aparato.
   c. Mueva la palanca de leva hacia la izquierda para bloquear el controlador en su sitio.
   d. Sustituya los cables y SFP.
   e. Si la controladora original utilizó DHCP para la dirección IP, busque la dirección MAC en la etiqueta ubicada en la parte posterior de la controladora de reemplazo. Solicite al administrador de red que asocie la red DNS y la dirección IP de la controladora que quitó con la dirección MAC de la controladora de reemplazo.

   > Si la controladora original no utilizó DHCP para la dirección IP, la nueva controladora adoptará la dirección IP de la controladora que quitó.

2. Coloque la controladora en línea mediante System Manager de SANtricity:
   a. Seleccione **hardware**.
   b. Si el gráfico muestra las unidades, seleccione **Mostrar parte posterior de la bandeja**.

c. Seleccione la controladora que desea colocar en línea.

d. Seleccione **colocar en línea** en el menú contextual y confirme que desea realizar la operación.

e. Compruebe que la pantalla de siete segmentos muestra el estado de `99`.

3. Confirme que el estado de la nueva controladora es óptimo y recoja datos de soporte.

Tras sustituir la pieza, devuelva la pieza que ha fallado a NetApp, tal y como se describe en las instrucciones de RMA incluidas con el kit. Consulte "Retorno de artículo sustituciones" para obtener más información.

Información relacionada

"Sitio de documentación para sistemas E-Series y EF-Series de NetApp"

Sustituya los componentes de hardware en la bandeja de controladoras de almacenamiento

Si se produce un problema de hardware, es posible que deba sustituir un componente de la bandeja de controladoras de almacenamiento.

Lo que necesitará

- Tiene el procedimiento de sustitución del hardware E-Series.
- Ha localizado físicamente el dispositivo de almacenamiento en el que va a reemplazar componentes de hardware de la bandeja de almacenamiento en el centro de datos.

  Ubique la controladora en el centro de datos

Acerca de esta tarea

Para sustituir la batería en el controlador de almacenamiento, consulte las instrucciones de estas instrucciones para sustituir un controlador de almacenamiento. Estas instrucciones describen cómo extraer un controlador del aparato, extraer la batería del controlador, instalar la batería y sustituir el controlador.

Para obtener instrucciones sobre las otras unidades reemplazables de campo (FRU) en las bandejas de las controladoras, acceda a los procedimientos de E-Series para realizar el mantenimiento del sistema.

FRU	Consulte las instrucciones
Batería	StorageGRID (estas instrucciones): Sustituir una controladora de almacenamiento
Unidad	E-Series: • Sustitución de unidad (60 unidades) • Sustitución de unidad (12 o 24 unidades)
Contenedor de alimentación	E-Series • Sustituir contenedor de alimentación (60 unidades) • Sustitución de la fuente de alimentación (12 o 24 unidades)

FRU	Consulte las instrucciones
Contenedor de ventilador (solo bandejas de 60 unidades)	E-Series: Sustituir contenedor de ventilador (60 unidades)
Cajón de unidades (solo bandejas de 60 unidades)	E-Series: Sustitución del cajón de unidades (60 unidades)

Información relacionada

"Sitio de documentación para sistemas E-Series y EF-Series de NetApp"

Sustituya la controladora de almacenamiento

Sustituya los componentes de hardware en la bandeja de expansión de 60 unidades opcional

Es posible que deba sustituir un módulo de entrada/salida, un suministro de alimentación o un ventilador de la bandeja de expansión.

Lo que necesitará

- Tiene el procedimiento de sustitución del hardware E-Series.
- Ha localizado físicamente el dispositivo de almacenamiento en el que va a reemplazar componentes de hardware de bandeja de expansión en el centro de datos.

  Ubique la controladora en el centro de datos

Acerca de esta tarea

Para sustituir un módulo de entrada/salida (IOM) en una bandeja de expansión de 60 unidades, consulte las instrucciones de estas instrucciones para sustituir una controladora de almacenamiento.

Para sustituir una fuente de alimentación o un ventilador en una bandeja de expansión de 60 unidades, acceda a los procedimientos de E-Series para mantener el hardware de 60 unidades.

FRU	Consulte las instrucciones de E-Series para
Módulo de entrada/salida (IOM)	Reemplazar un IOM
Contenedor de alimentación	Sustituir contenedor de alimentación (60 unidades)
Contenedor de ventilador	Sustituir contenedor de ventilador (60 unidades)

Apague el controlador SG6000-CN

Apague el controlador SG6000-CN para realizar el mantenimiento de hardware.

Lo que necesitará

Ha localizado físicamente el controlador SG6000-CN que requiere mantenimiento en el centro de datos. Consulte Ubique la controladora en el centro de datos.

Acerca de esta tarea

Para evitar interrupciones del servicio, confirme que todos los demás nodos de almacenamiento están conectados al grid antes de apagar la controladora o apagar la controladora durante una ventana de mantenimiento programada cuando sea posible periodos de interrupción del servicio. Consulte la información acerca de supervisar los estados de conexión de los nodos.

> Si alguna vez ha utilizado una regla de ILM que crea solamente una copia de un objeto, debe apagar la controladora durante una ventana de mantenimiento programada. De lo contrario, es posible que pierda temporalmente el acceso a esos objetos durante este procedimiento. Consulte "Gestión de objetos con la gestión del ciclo de vida de la información".

Pasos

1. Apague el controlador SG6000-CN:

> Debe realizar un apagado controlado de la controladora introduciendo los comandos especificados a continuación. Se recomienda realizar un apagado controlado cuando sea posible para evitar alertas innecesarias, garantizar que haya logs completos disponibles y evitar interrupciones del servicio.

   a. Si aún no ha iniciado sesión en el nodo de grid, inicie sesión con PuTTY u otro cliente ssh:
      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. Apague el controlador SG6000-CN:

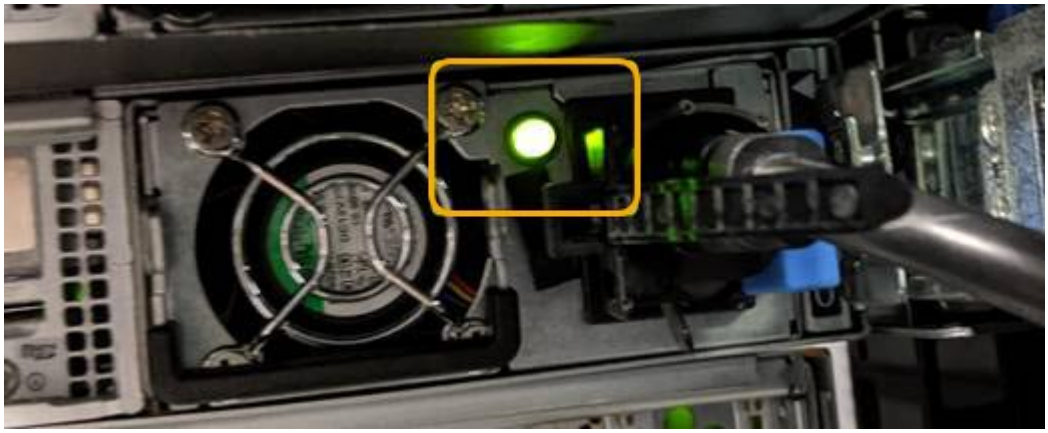
```
shutdown -h now
```

   Este comando puede tardar hasta 10 minutos en completarse.

2. Utilice uno de los siguientes métodos para verificar que el controlador SG6000-CN está apagado:
   - Observe el LED de alimentación azul de la parte frontal de la controladora y confirme que está apagado.

   - Observe los LED verdes de ambos sistemas de alimentación de la parte posterior del controlador y

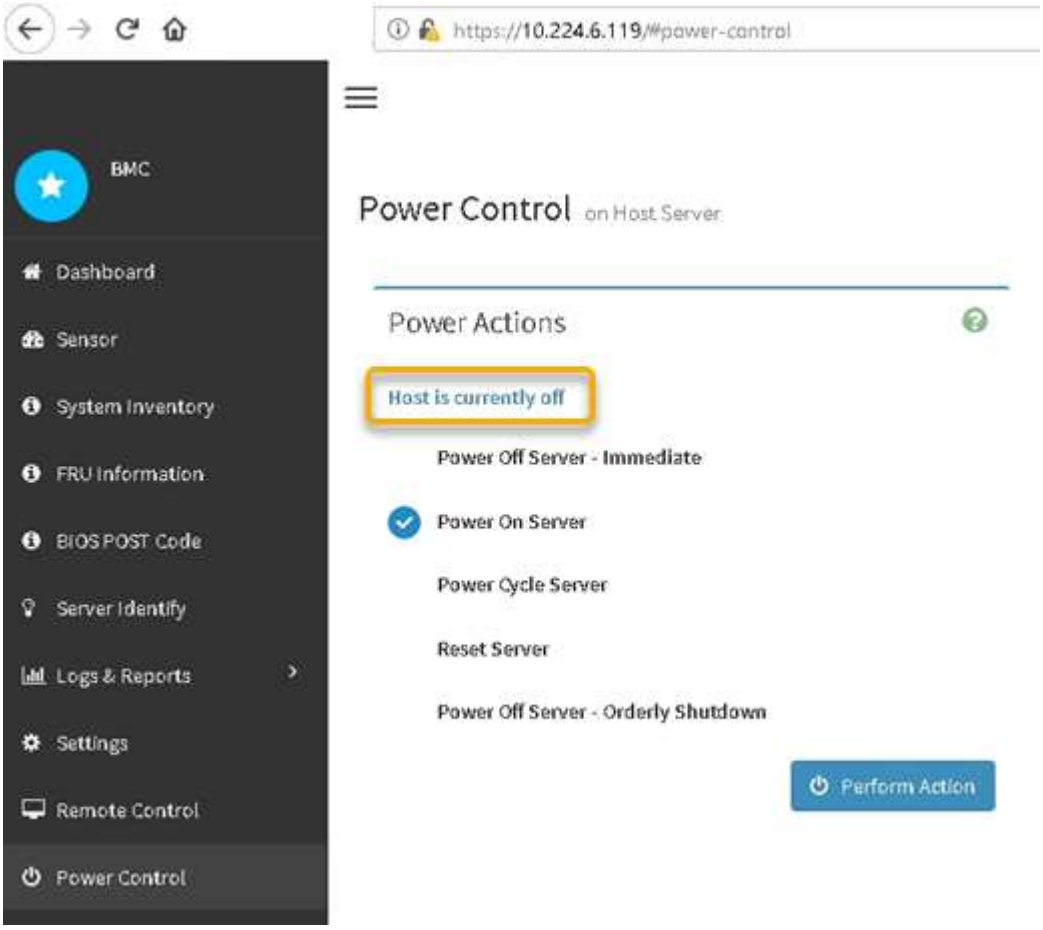
confirme que parpadean a una velocidad normal (aproximadamente un parpadeo por segundo).



- Use la interfaz del BMC del controlador:
  i. Acceda a la interfaz del BMC del controlador.

     Acceda a la interfaz de BMC

  ii. Seleccione **Control de alimentación**.
  iii. Compruebe que las acciones de alimentación indican que el host está apagado actualmente.



Información relacionada

Retire el controlador SG6000-CN del armario o bastidor

Encienda el controlador SG6000-CN y compruebe el funcionamiento

Encienda la controladora después de completar el mantenimiento.

Lo que necesitará

- Instaló la controladora en un armario o rack y conecta los cables de datos y alimentación.

  Vuelva a instalar el controlador SG6000-CN en el armario o bastidor

- Localizó físicamente la controladora en el centro de datos.

  Ubique la controladora en el centro de datos

Pasos

1. Encienda el controlador SG6000-CN y supervise los LED del controlador y los códigos de inicio mediante uno de los siguientes métodos:

   - Pulse el interruptor de alimentación de la parte frontal del controlador.

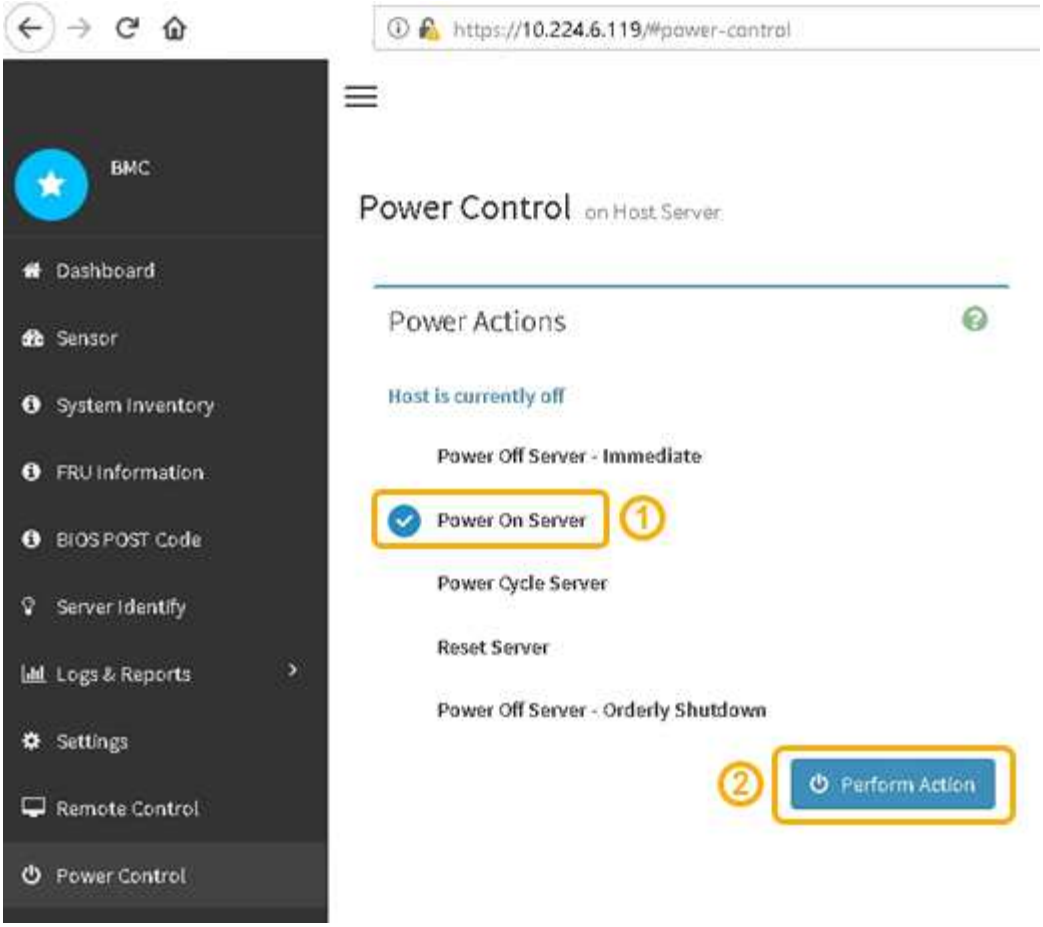
   - Use la interfaz del BMC del controlador:

     i. Acceda a la interfaz del BMC del controlador.

     Acceda a la interfaz de BMC

     ii. Seleccione **Control de alimentación**.

     iii. Seleccione **encendido del servidor** y, a continuación, seleccione **realizar acción**.



Utilice la interfaz de BMC para supervisar el estado de inicio.

2. Confirme que el controlador del dispositivo se muestra en Grid Manager y sin alertas.

   La controladora puede tardar hasta 20 minutos en mostrarse en Grid Manager.

3. Confirme que el nuevo controlador SG6000-CN está completamente operativo:

   a. Inicie sesión en el nodo de la cuadrícula mediante PuTTY u otro cliente ssh:

      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 el siguiente comando y compruebe que devuelve el resultado esperado:
   `cat /sys/class/fc_host/*/port_state`

   Resultado esperado:

```
Online
Online
Online
Online
```

Si no se devuelve el resultado esperado, póngase en contacto con el soporte técnico.

c. Introduzca el siguiente comando y compruebe que devuelve el resultado esperado:
`cat /sys/class/fc_host/*/speed`

Resultado esperado:

```
16 Gbit
16 Gbit
16 Gbit
16 Gbit
```

+
Si no se devuelve el resultado esperado, póngase en contacto con el soporte técnico.

a. En la página Nodes de Grid Manager, asegúrese de que el nodo del dispositivo esté conectado a la cuadrícula y no tenga ninguna alerta.

> No desconecte otro nodo del dispositivo a menos que este dispositivo tenga un icono verde.

4. Opcional: Instale el panel frontal, si se ha quitado uno.

Información relacionada

Ver los indicadores de estado y los botones del controlador SG6000-CN

Ver los códigos de estado de arranque para los controladores de almacenamiento SG6000

Sustituir el controlador SG6000-CN

Es posible que deba sustituir el controlador SG6000-CN si no funciona de forma óptima o si ha fallado.

Lo que necesitará

- Tiene una controladora de sustitución con el mismo número de pieza que la controladora que desea sustituir.
- Tiene etiquetas para identificar cada cable conectado a la controladora.
- Localizó físicamente la controladora para reemplazar en el centro de datos.

  Ubique la controladora en el centro de datos

Acerca de esta tarea

No se podrá acceder al nodo de almacenamiento del dispositivo cuando sustituya el controlador SG6000-CN. Si el controlador SG6000-CN funciona lo suficiente, puede realizar una parada controlada al inicio de este procedimiento.

> Si va a sustituir la controladora antes de instalar el software StorageGRID, es posible que no pueda acceder al instalador de dispositivos de StorageGRID inmediatamente después de completar este procedimiento. Aunque puede acceder al instalador del dispositivo StorageGRID desde otros hosts de la misma subred que el dispositivo, no puede acceder al mismo desde hosts de otras subredes. Esta condición debe resolverse dentro de los 15 minutos (cuando se agota cualquier entrada de caché ARP para el tiempo de espera original de la controladora); asimismo, puede borrar la condición de inmediato mediante la purga manual de todas las entradas antiguas de la caché ARP desde el enrutador o la puerta de enlace local.

Pasos

1. Muestre las configuraciones actuales del aparato y regístrelas.
   a. Inicie sesión en el dispositivo que se va a sustituir:
      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: **`run-host-command ipmitool lan print`** Para mostrar las configuraciones actuales de BMC del dispositivo.
2. Si el controlador SG6000-CN funciona lo suficiente como para permitir un apagado controlado, apague el controlador SG6000-CN.

   Apague el controlador SG6000-CN

3. Si alguna de las interfaces de red de este dispositivo StorageGRID está configurada para DHCP, es posible que deba actualizar las asignaciones de permisos DHCP permanentes en los servidores DHCP para hacer referencia a las direcciones MAC del dispositivo de reemplazo. La actualización garantiza que el dispositivo tenga asignadas las direcciones IP esperadas.
   a. Busque la etiqueta de dirección MAC en la parte frontal del controlador SG6000-CN y determine la dirección MAC del puerto de red de administración.

      > La etiqueta de dirección MAC incluye la dirección MAC para el puerto de gestión del BMC.
      >
      > Para determinar la dirección MAC del puerto de red de administración, debe agregar **2** al número hexadecimal de la etiqueta. Por ejemplo, si la dirección MAC de la etiqueta termina en **09**, la dirección MAC del puerto de administración finalizará en **0B**. Si la dirección MAC de la etiqueta termina en **(*y*)FF**, la dirección MAC del puerto de administración finalizará en **(*y*+1)01**. Puede realizar este cálculo fácilmente abriendo Calculadora en Windows, establecerlo en modo Programador, seleccionando hex, escribiendo la dirección MAC y, a continuación, escribiendo **+ 2 =**.

   b. Solicite al administrador de red que asocie la red DNS y la dirección IP de la controladora que quitó

con la dirección MAC de la controladora de reemplazo.

> Debe asegurarse de que todas las direcciones IP de la controladora original se hayan actualizado antes de aplicar alimentación a la controladora de reemplazo. De lo contrario, la controladora obtendrá nuevas direcciones IP de DHCP cuando se arranca y es posible que no pueda volver a conectarse a StorageGRID. Este paso se aplica a todas las redes StorageGRID conectadas a la controladora.

> Si la controladora original usaba la dirección IP estática, la nueva controladora adoptará automáticamente las direcciones IP de la controladora que se quitó.

4. Desmontaje y sustitución del controlador SG6000-CN:
   a. Etiquete los cables y desconecte los cables y cualquier transceptor SFP+ o SFP28.

      > Para evitar un rendimiento degradado, no gire, pliegue, pellizque ni pellizque los cables.

   b. Quite la controladora que ha fallado del armario o rack.
   c. Instale la controladora de reemplazo en el armario o rack.
   d. Sustituya los cables y cualquier transceptores SFP+ o SFP28.
   e. Encienda la controladora y supervise los LED y los códigos de arranque de la controladora.
5. Si el dispositivo donde sustituyó la controladora usaba un servidor de gestión de claves (KMS) para cifrar los datos, es posible que se necesite una configuración adicional para que el nodo pueda unirse al grid. Si el nodo no se une automáticamente a la cuadrícula, asegúrese de que estas opciones de configuración se hayan transferido a la nueva controladora y configure manualmente todos los ajustes que no tengan la configuración esperada:
   - "Configure las conexiones StorageGRID"
   - "Configure el cifrado de nodo para el dispositivo"
6. Inicie sesión en el dispositivo con la controladora reemplazada:
   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.
7. Restaure la conectividad de red de BMC para el dispositivo. Existen dos opciones:
   - Utilice IP estáticas, máscara de red y puerta de enlace
   - Utilice DHCP para obtener una IP, una máscara de red y una puerta de enlace

     i. Para restaurar la configuración de BMC para utilizar una IP estática, una máscara de red y una puerta de enlace, escriba los siguientes comandos:

     `run-host-command ipmitool lan set 1 ipsrc static`

     `run-host-command ipmitool lan set 1 ipaddr Appliance_IP`

     `run-host-command ipmitool lan set 1 netmask Netmask_IP`

```
run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```

i. Para restaurar la configuración de BMC a fin de utilizar DHCP a fin de obtener una IP, una máscara de red y una puerta de enlace, introduzca el siguiente comando:

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```

8. Después de restaurar la conectividad de red de BMC, conéctese a la interfaz de BMC para auditar y restaurar cualquier configuración de BMC personalizada adicional que pueda haber aplicado. Por ejemplo, se debe confirmar la configuración de los destinos de capturas SNMP y las notificaciones por correo electrónico. Consulte "Configurar la interfaz de BMC".
9. Confirme que el nodo del dispositivo aparece en Grid Manager y que no aparece ninguna alerta.

Información relacionada

SG6000-CN: Instalación en armario o bastidor

Ver los indicadores de estado y los botones del controlador SG6000-CN

Ver los códigos de arranque del controlador SG6000-CN

Sustituya una o ambas fuentes de alimentación en el controlador SG6000-CN

El controlador SG6000-CN tiene dos fuentes de alimentación para redundancia. Si uno de los suministros de alimentación falla, debe reemplazarla por Lo antes posible. para garantizar que la controladora de computación tenga alimentación redundante. Ambas fuentes de alimentación que funcionan en la controladora deben ser del mismo modelo y vatios.

Lo que necesitará

- Estableció la ubicación física en el centro de datos de la controladora con la fuente de alimentación que debe sustituirse.

  Ubicar la controladora en un centro de datos

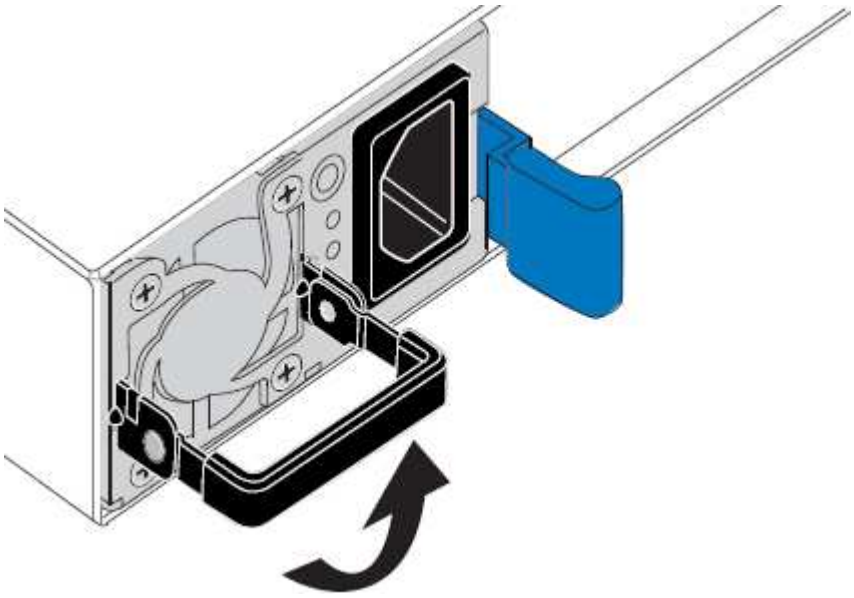
- Si solo va a sustituir un suministro de alimentación:
  - Ha desembalado la unidad de suministro de alimentación de repuesto y se ha asegurado de que es el mismo modelo y vataje que la unidad de suministro de alimentación que desea sustituir.
  - Ha confirmado que la otra fuente de alimentación está instalada y en funcionamiento.
- Si va a sustituir ambos suministros de alimentación al mismo tiempo:
  - Ha desembalado las unidades de suministro de alimentación de repuesto y se ha asegurado de que sean del mismo modelo y vataje.

Acerca de esta tarea

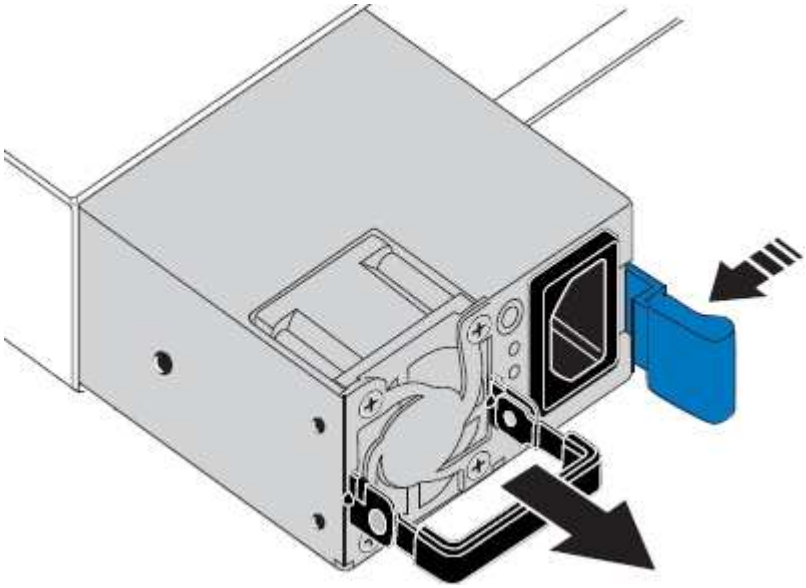
La figura muestra las dos unidades de alimentación del controlador SG6000-CN, a las que se puede acceder desde la parte posterior del controlador. Utilice este procedimiento para sustituir una o ambas fuentes de alimentación. Si va a sustituir ambas fuentes de alimentación, primero debe realizar un apagado controlado del aparato.

Pasos

1. Si sólo va a sustituir una fuente de alimentación, no es necesario apagar el aparato. Vaya a la Desenchufe el cable de alimentación paso. Si va a sustituir ambas fuentes de alimentación al mismo tiempo, haga lo siguiente antes de desconectar los cables de alimentación:
   a. Coloque el dispositivo en modo de mantenimiento.
   b. Apague el aparato.
2. desenchufe el cable de alimentación de cada fuente de alimentación que vaya a sustituirse.
3. Levante la palanca de leva en el primer suministro que se va a sustituir.



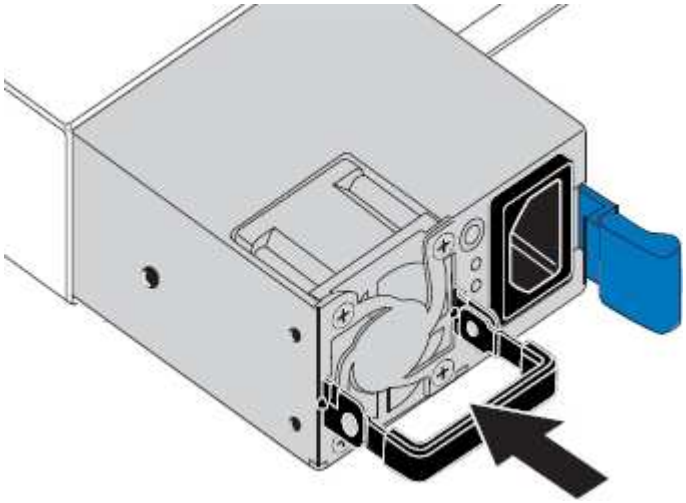
4. Presione el pestillo azul y saque la fuente de alimentación.



5. Con el pestillo azul a la derecha, deslice la fuente de alimentación de repuesto hacia el chasis.

> Ambas fuentes de alimentación deben ser del mismo modelo y vataje.

Asegúrese de que el pestillo azul está en el lado derecho cuando deslice la unidad de sustitución en.



6. Empuje la palanca de leva hacia abajo para fijar la fuente de alimentación de repuesto.
7. Si va a sustituir ambas fuentes de alimentación, repita los pasos 2 a 6 para sustituir la segunda fuente de alimentación.
8. Conecte los cables de alimentación a las unidades sustituidas y aplique alimentación.
9. Si colocó el aparato en modo de mantenimiento, salga del modo de mantenimiento. En el instalador del dispositivo StorageGRID, seleccione **Avanzado Reiniciar controlador** y, a continuación, seleccione **Reiniciar en StorageGRID**.

Retire el controlador SG6000-CN del armario o bastidor

Retire el controlador SG6000-CN de un armario o rack para acceder a la cubierta superior o para mover el controlador a una ubicación diferente.

Lo que necesitará

- Tiene etiquetas para identificar cada cable que está conectado al controlador SG6000-CN.
- Ha localizado físicamente el controlador SG6000-CN en el que realiza tareas de mantenimiento en el centro de datos.

  Ubique la controladora en el centro de datos

- Ha apagado el controlador SG6000-CN.

  Apague el controlador SG6000-CN

> No apague la controladora con el switch de alimentación.

Pasos

1. Etiquete y desconecte los cables de alimentación de la controladora.

2. Envuelva el extremo de la correa de la muñequera ESD alrededor de su muñeca y fije el extremo de la pinza a una masa metálica para evitar descargas estáticas.
3. Etiquete y desconecte los cables de datos de la controladora y cualquier transceptor SFP+ o SFP28.

   Para evitar un rendimiento degradado, no gire, pliegue, pellizque ni pellizque los cables.

4. Afloje los dos tornillos cautivos del panel frontal del controlador.

5. Deslice el controlador SG6000-CN hacia adelante para sacarlo del rack hasta que los raíles de montaje se extiendan completamente y oirá un clic en los pestillos de ambos lados.

   Se puede acceder a la cubierta superior del controlador.

6. Opcional: Si va a extraer completamente la controladora del armario o rack, siga las instrucciones del kit de raíl para quitar la controladora de los rieles.

Información relacionada

Retire la cubierta del controlador SG6000-CN

Vuelva a instalar el controlador SG6000-CN en el armario o bastidor

Vuelva a instalar la controladora en un armario o rack cuando finalice el mantenimiento del hardware.

Lo que necesitará

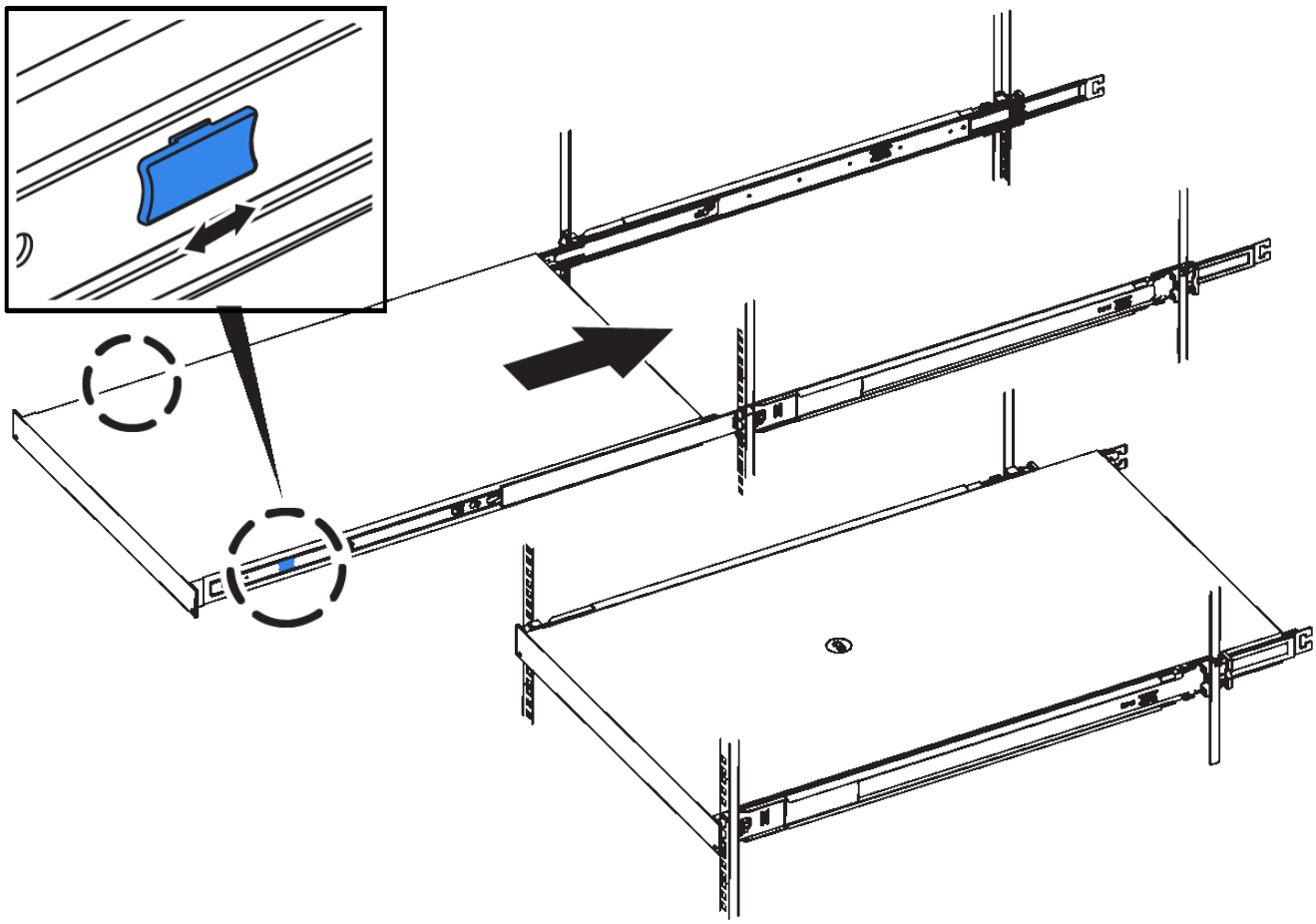
Ha vuelto a instalar la cubierta del controlador.

Vuelva a instalar la cubierta del controlador SG6000-CN

Pasos

1. Presione el riel azul para liberar ambos rieles de bastidor al mismo tiempo y deslice el controlador SG6000-CN en el rack hasta que esté completamente asentado.

   Cuando no pueda mover el controlador más, tire de los pestillos azules a ambos lados del chasis para deslizar el controlador completamente.



No conecte el panel frontal hasta que haya encendido la controladora.

2. Apriete los tornillos cautivos del panel frontal del controlador para fijar el controlador en el rack.

3. Envuelva el extremo de la correa de la muñequera ESD alrededor de su muñeca y fije el extremo de la pinza a una masa metálica para evitar descargas estáticas.
4. Vuelva a conectar los cables de datos de la controladora y cualquier transceptor SFP+ o SFP28.

Para evitar un rendimiento degradado, no gire, pliegue, pellizque ni pellizque los cables.

Aparato de cable (SG6000)

5. Vuelva a conectar los cables de alimentación de la controladora.

Conexión de los cables de alimentación y alimentación (SG6000)

Después de terminar

Es posible reiniciar el controlador.

Encienda el controlador SG6000-CN y compruebe el funcionamiento

Retire la cubierta del controlador SG6000-CN

Retire la cubierta del controlador para acceder a los componentes internos para realizar tareas de mantenimiento.

Lo que necesitará

Retire el controlador del armario o rack para acceder a la cubierta superior.

Retire el controlador SG6000-CN del armario o bastidor

Pasos

1. Asegúrese de que el pestillo de la cubierta del controlador SG6000-CN no esté bloqueado. Si es necesario, gire un cuarto de vuelta el cierre de plástico azul en la dirección de desbloqueo, como se muestra en el bloqueo del pestillo.
2. Gire el pestillo hacia arriba y hacia atrás hacia la parte trasera del chasis del controlador SG6000-CN hasta que se detenga; a continuación, levante con cuidado la cubierta del chasis y déjela a un lado.

Envuelva el extremo de la correa de una muñequera ESD alrededor de la muñeca y fije el extremo de la pinza a una masa metálica para evitar descargas estáticas al trabajar en el interior del controlador SG6000-CN.

Información relacionada

Quite el HBA Fibre Channel

Vuelva a instalar la cubierta del controlador SG6000-CN

Vuelva a instalar la cubierta del controlador cuando finalice el mantenimiento interno del hardware.

Lo que necesitará

Completó todos los procedimientos de mantenimiento dentro del controlador.

Pasos

1. Con el pestillo de la cubierta abierto, sujete la cubierta por encima del chasis y alinee el orificio del pestillo de la cubierta superior con el pasador del chasis. Cuando la cubierta esté alineada, bájela en el chasis.

2. Gire el pestillo de la cubierta hacia adelante y hacia abajo hasta que se detenga y la cubierta se asiente completamente en el chasis. Compruebe que no hay separaciones a lo largo del borde delantero de la cubierta.

   Si la cubierta no está completamente asentada, es posible que no pueda deslizar el controlador SG6000-CN en el rack.

3. Opcional: Gire un cuarto de vuelta el cierre de plástico azul en el sentido de bloqueo, como se muestra en el bloqueo del pestillo, para bloquearlo.

Después de terminar

Vuelva a instalar la controladora en el armario o rack.

Vuelva a instalar el controlador SG6000-CN en el armario o bastidor

Sustituya el HBA Fibre Channel en el controlador SG6000-CN

Es posible que deba sustituir el adaptador de bus de host (HBA) Fibre Channel en el controlador SG6000-CN si no funciona de forma óptima o si ha fallado.

Verifique el adaptador de bus de host de Fibre Channel que desea sustituir

Si no está seguro del adaptador de bus de host (HBA) Fibre Channel que debe sustituirse, complete este procedimiento para identificarlo.

Lo que necesitará

- Dispone del número de serie del dispositivo de almacenamiento o del controlador SG6000-CN en los que es necesario sustituir el HBA Fibre Channel.

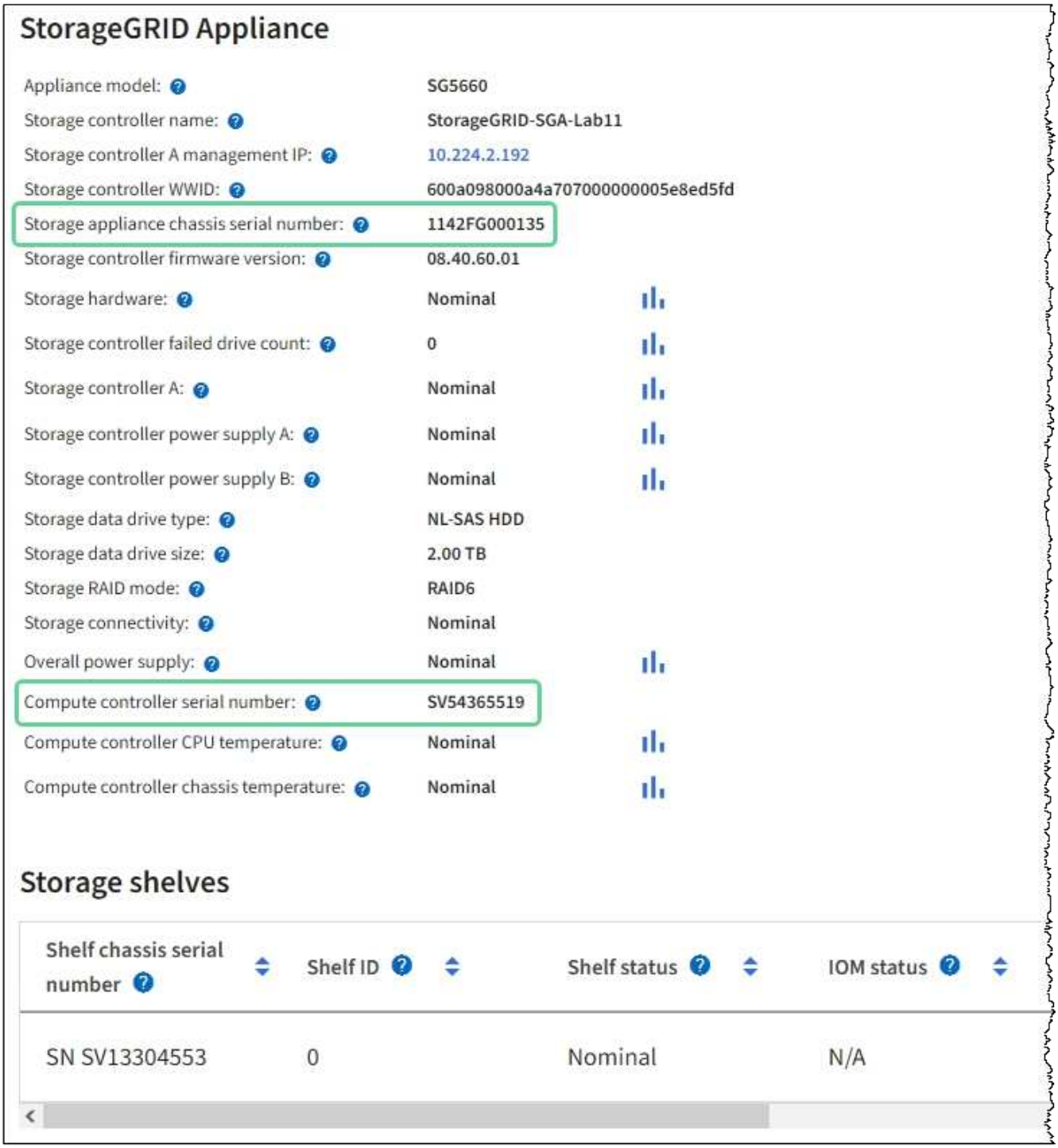
> Si el número de serie del dispositivo de almacenamiento que contiene el HBA Fibre Channel que va a sustituir comienza por la letra Q, no aparecerá en el Grid Manager. Debe comprobar las etiquetas adjuntas a la parte frontal de cada controlador SG6000-CN del centro de datos hasta que encuentre una coincidencia.

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

Pasos

1. En Grid Manager, seleccione **NODES**.
2. En la tabla de la página Nodes, seleccione un dispositivo Storage Node.
3. Seleccione la ficha **hardware**.

   Compruebe el **número de serie del chasis del dispositivo de almacenamiento** y el **número de serie del controlador de computación** en la sección StorageGRID Appliance. Consulte si uno de estos números de serie coincide con el número de serie del dispositivo de almacenamiento en el que desea sustituir el HBA Fibre Channel. Si coincide alguno de los números de serie, ha encontrado el dispositivo correcto.



   - Si no se muestra la sección dispositivo StorageGRID, el nodo seleccionado no es un dispositivo

StorageGRID. Seleccione un nodo diferente en la vista de árbol.

- Si el modelo de dispositivo no es SG6060 ni SG6060X, seleccione un nodo diferente en la vista de árbol.
- Si los números de serie no coinciden, seleccione un nodo diferente en la vista de árbol.

4. Después de ubicar el nodo en el que es necesario reemplazar el adaptador de bus de host de Fibre Channel, escriba la dirección IP de BMC de la controladora de computación que aparece en la sección StorageGRID Appliance.

   Puede usar esta dirección IP para encender el LED de identificación de controladora de computación, para ayudarle a localizar el dispositivo en el centro de datos.

   Enciende y apaga el LED de identificación de la controladora

Información relacionada

Quite el HBA Fibre Channel

Quite el HBA Fibre Channel

Es posible que deba sustituir el adaptador de bus de host (HBA) Fibre Channel en el controlador SG6000-CN si no funciona de forma óptima o si ha fallado.

Lo que necesitará

- Tiene el adaptador de bus de host de Fibre Channel de sustitución correcto.
- Ya tienes "Se determina qué controladora SG6000-CN contiene el HBA Fibre Channel que debe reemplazar".
- Ya tienes "Ubicado físicamente el controlador SG6000-CN" en el centro de datos.
- Ya tienes "Apague el controlador SG6000-CN".

  Es necesario realizar un apagado controlado antes de retirar la controladora del rack.

- Ya tienes "ha quitado la controladora del armario o el rack".
- Ya tienes "ha quitado la cubierta del controlador".

Acerca de esta tarea

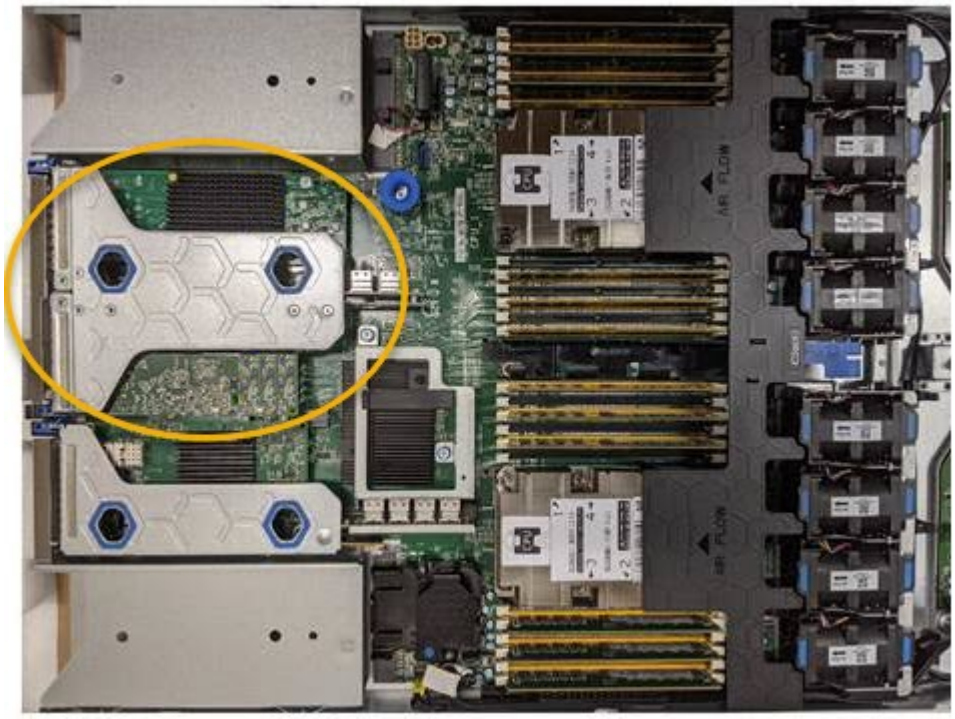
Para evitar interrupciones del servicio, confirme que todos los demás nodos de almacenamiento están conectados al grid antes de iniciar la sustitución de un HBA Fibre Channel o sustituya el adaptador durante un periodo de mantenimiento programado cuando normalmente se esperan periodos de interrupción del servicio. Consulte la información acerca de "supervisar los estados de conexión de los nodos".

Si alguna vez ha utilizado una regla de ILM que crea solamente una copia de un objeto, debe reemplazar el HBA de Fibre Channel durante una ventana de mantenimiento programada. De lo contrario, es posible que pierda temporalmente el acceso a esos objetos durante este procedimiento. Consulte la información acerca de "por qué no debe utilizar replicación de copia única".

Pasos

1. Envuelva el extremo de la correa de la muñequera ESD alrededor de su muñeca y fije el extremo de la pinza a una masa metálica para evitar descargas estáticas.

2. Localice el conjunto de la tarjeta vertical situado en la parte posterior de la controladora que contiene el HBA Fibre Channel.



3. Sujete el conjunto del elevador a través de los orificios marcados en azul y levántelo con cuidado hacia arriba. Mueva el conjunto de la tarjeta vertical hacia la parte frontal del chasis a medida que lo levante para permitir que los conectores externos de sus adaptadores instalados se retiren del chasis.
4. Coloque la tarjeta vertical sobre una superficie antiestática plana con el lado del marco metálico hacia abajo para acceder a los adaptadores.

El conjunto de tarjeta vertical tiene dos adaptadores: Un HBA Fibre Channel y un adaptador de red Ethernet. El adaptador de bus de host de Fibre Channel se indica en la ilustración.

5. Abra el pestillo azul del adaptador (en un círculo) y retire con cuidado el HBA Fibre Channel del conjunto de la tarjeta vertical. Rote ligeramente el adaptador para ayudar a extraer el adaptador de su conector. No utilice una fuerza excesiva.
6. Coloque el adaptador sobre una superficie plana antiestática.

Después de terminar

Instale el HBA Fibre Channel de repuesto.

Vuelva a instalar el HBA Fibre Channel

Vuelva a instalar el HBA Fibre Channel

El adaptador de bus de host de Fibre Channel de repuesto se instala en la misma ubicación que el que se ha quitado.

Lo que necesitará

- Tiene el adaptador de bus de host de Fibre Channel de sustitución correcto.
- Ha quitado el adaptador de bus de host de Fibre Channel existente.

  Quite el HBA Fibre Channel

Pasos

1. Envuelva el extremo de la correa de la muñequera ESD alrededor de su muñeca y fije el extremo de la pinza a una masa metálica para evitar descargas estáticas.
2. Retire el HBA Fibre Channel de repuesto de su embalaje.
3. Con el pestillo azul del adaptador en la posición abierta, alinee el HBA Fibre Channel con su conector en el conjunto de la tarjeta vertical y, a continuación, presione con cuidado el adaptador en el conector hasta que esté completamente asentado.

   El conjunto de tarjeta vertical tiene dos adaptadores: Un HBA Fibre Channel y un adaptador de red Ethernet. El adaptador de bus de host de Fibre Channel se indica en la ilustración.

4. Localice el orificio de alineación en el conjunto de la tarjeta vertical (en un círculo) que se alinea con un pasador guía en la placa base para garantizar la correcta colocación del conjunto de la tarjeta vertical.

5. Coloque el conjunto de la tarjeta vertical en el chasis, asegurándose de que está alineado con el conector y la clavija guía de la placa base; a continuación, inserte el conjunto de la tarjeta vertical.
6. Presione con cuidado el conjunto de la tarjeta vertical en su lugar a lo largo de su línea central, junto a los orificios marcados en azul, hasta que esté completamente asentado.
7. Retire las tapas protectoras de los puertos HBA Fibre Channel en los que volverá a instalar los cables.

Después de terminar

Si no dispone de ningún otro procedimiento de mantenimiento que realizar en el controlador, vuelva a instalar la cubierta del controlador.

Vuelva a instalar la cubierta del controlador SG6000-CN

Cambiar la configuración del enlace del controlador SG6000-CN

Puede cambiar la configuración del enlace Ethernet del controlador SG6000-CN. Puede cambiar el modo de enlace de puerto, el modo de enlace de red y la velocidad del enlace.

Lo que necesitará

El aparato se ha estado se colocó en modo de mantenimiento.

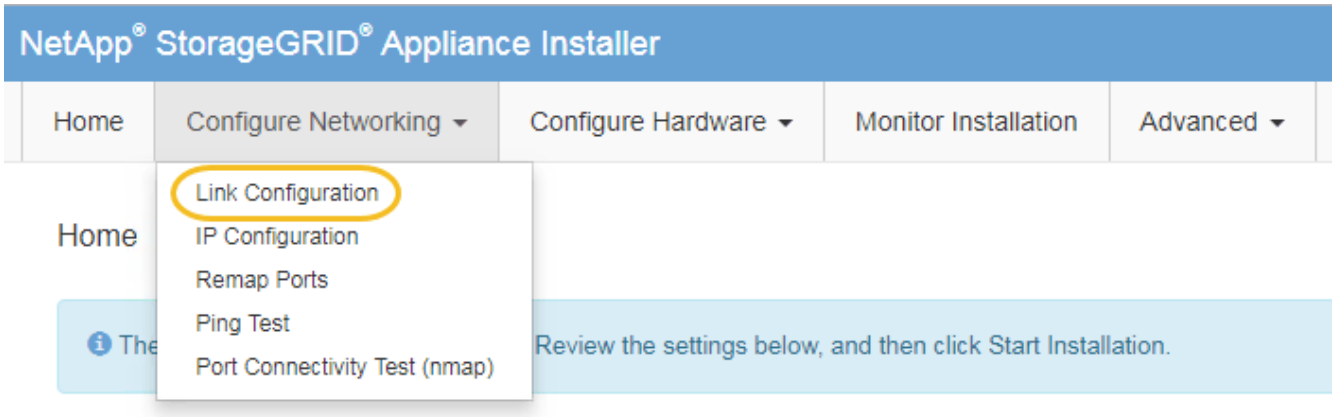
Acerca de esta tarea

Las opciones para cambiar la configuración del enlace Ethernet del controlador SG6000-CN incluyen:

- Cambiando **modo de enlace de puerto** de fijo a agregado, o de agregado a fijo
- Cambio del **modo de enlace de red** de Active-Backup a LACP o de LACP a Active-Backup
- Habilitar o deshabilitar el etiquetado de VLAN, o cambiar el valor de una etiqueta de VLAN
- Cambio de la velocidad de enlace.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Configurar la red Configuración del enlace**.



2. realice los cambios deseados en la configuración del enlace.

   Para obtener más información sobre las opciones, consulte Configuración de enlaces de red (SG6000).

3. Cuando esté satisfecho con sus selecciones, haga clic en **Guardar**.

   > Puede perder la conexión si ha realizado cambios en la red o el enlace que está conectado a través de. Si no vuelve a conectarse en un minuto, vuelva a introducir la URL del instalador de dispositivos StorageGRID utilizando una de las otras direcciones IP asignadas al dispositivo:
   > **`https://Appliance_Controller_IP:8443`**

   Si ha realizado cambios en la configuración de VLAN, es posible que la subred del dispositivo haya cambiado. Si necesita cambiar las direcciones IP del dispositivo, siga el Configurar las direcciones IP instrucciones.

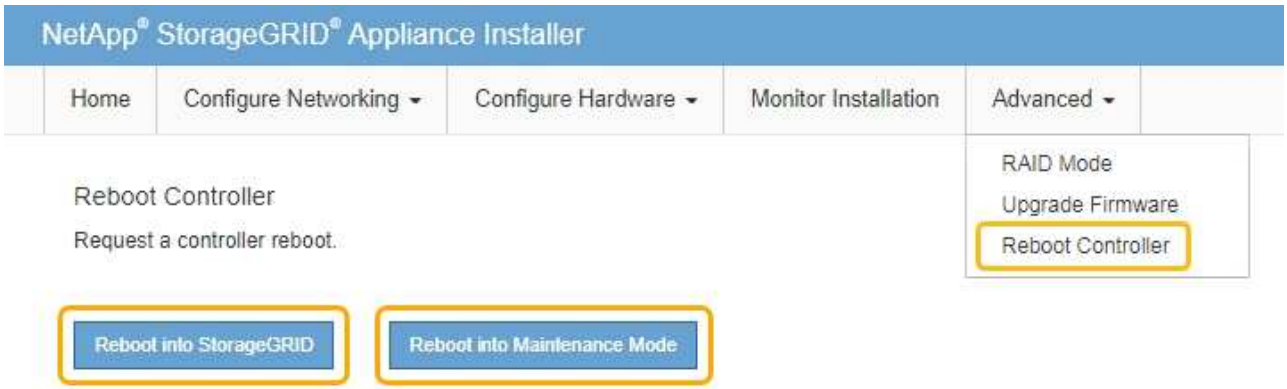
   Configure las direcciones IP de StorageGRID

4. Seleccione **Configurar redes Prueba de ping** en el menú.
5. Utilice la herramienta Ping Test para comprobar la conectividad a las direcciones IP en cualquier red que pudiera haber sido afectada por los cambios de configuración de vínculos realizados en cambios de configuración del enlace paso.

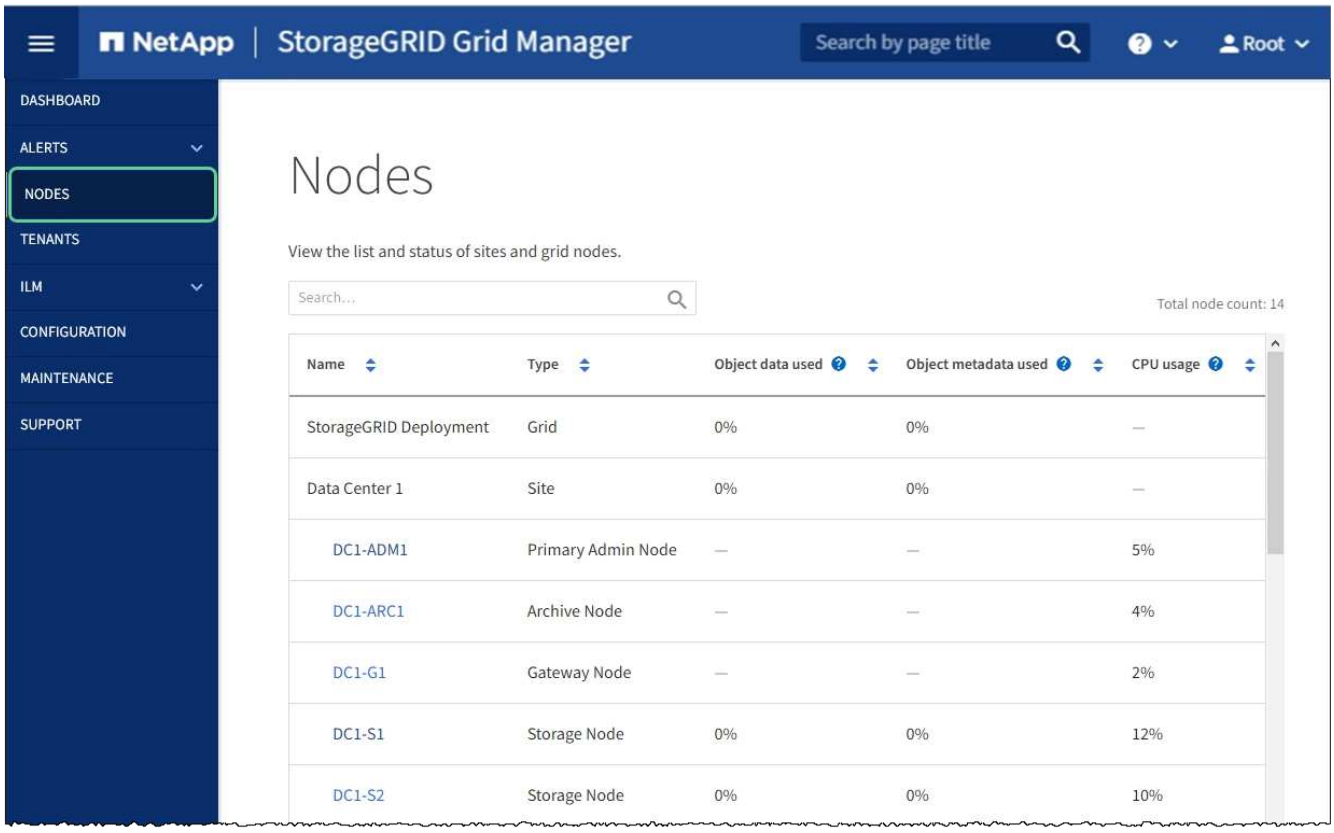
   Además de cualquier otra prueba que elija realizar, confirme que puede hacer ping a la dirección IP de red de cuadrícula del nodo de administración principal y a la dirección IP de red de cuadrícula de al menos otro nodo de almacenamiento. Si es necesario, vuelva al cambios de configuración del enlace avance y corrija cualquier problema con la configuración de los enlaces.

6. Una vez satisfecho de que los cambios de configuración de los enlaces están funcionando y que se tienen que realizar procedimientos adicionales mientras el nodo se encuentra en modo de mantenimiento, estos deben realizarse ahora. Cuando haya terminado, o si ha experimentado algún fallo y desea volver a empezar, seleccione **Avanzado Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID**
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. Seleccione esta opción si ha experimentado algún error durante el procedimiento y desea volver a empezar. Cuando el nodo termine de reiniciarse en el modo de mantenimiento, reinicie desde el paso adecuado del procedimiento en que falló.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Cambie la configuración de MTU

Puede cambiar la configuración de MTU que asigne al configurar las direcciones IP para el nodo del dispositivo.

Acerca de esta tarea

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. Los valores de MTU no tienen que ser iguales para todos los tipos de red.

Para cambiar la configuración de MTU sin reiniciar el nodo del dispositivo, Utilice la herramienta Cambiar IP.

Si la red de cliente o administrador no se configuró en el instalador de dispositivos de StorageGRID durante la instalación inicial, Cambie la configuración de MTU con el modo de mantenimiento.

Cambie la configuración de MTU mediante la herramienta Cambiar IP

Lo que necesitará

Usted tiene la `Passwords.txt` Archivo para utilizar la herramienta Cambiar IP.

Pasos

Acceda a la herramienta Cambiar IP y actualice la configuración de MTU como se describe en Cambie la configuración de red de los nodos.

Cambie la configuración de MTU con el modo de mantenimiento

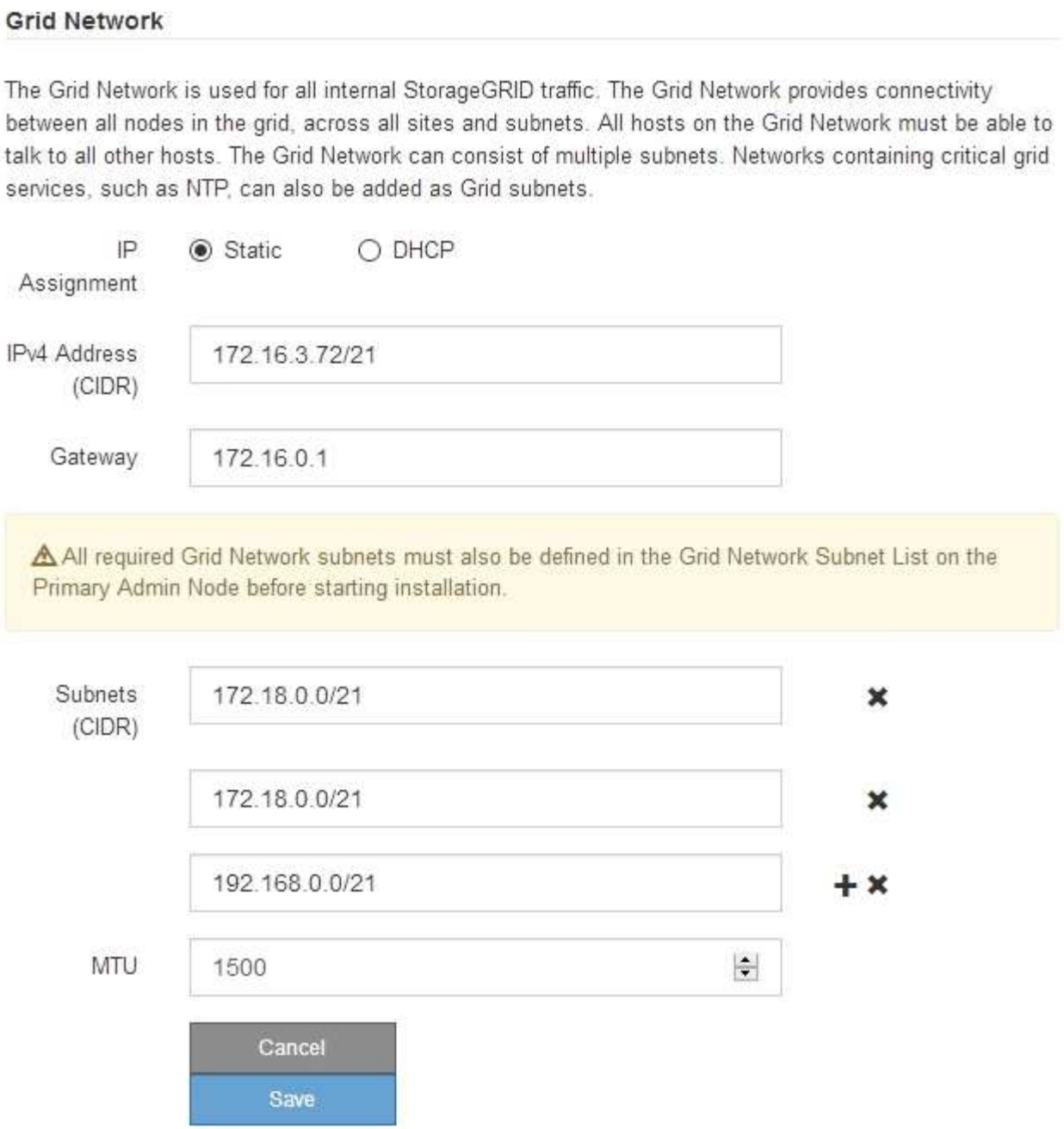
Cambie la configuración de MTU mediante el modo de mantenimiento si no puede acceder a estas opciones con la herramienta Cambiar IP.

Lo que necesitará

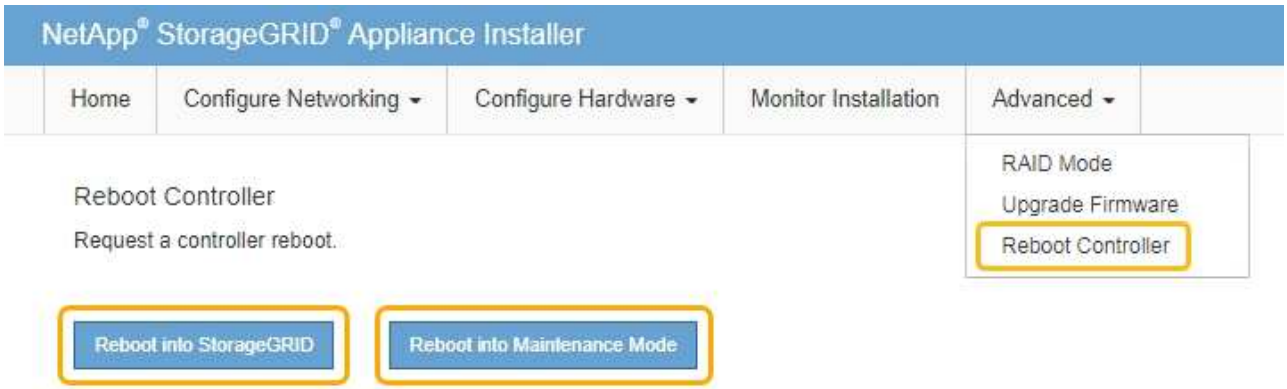
El aparato se ha estado se colocó en modo de mantenimiento.

Pasos

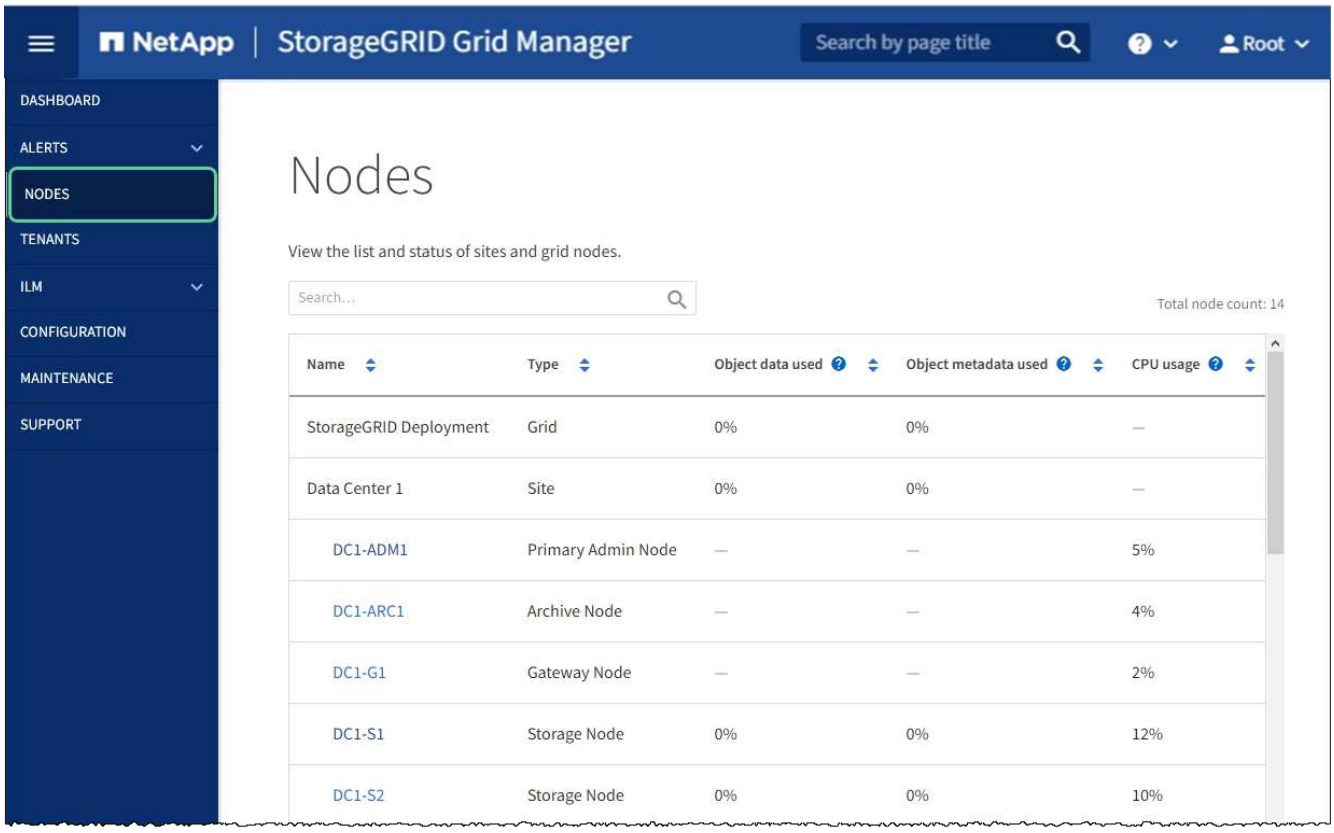
1. En el instalador del dispositivo StorageGRID, seleccione **Configurar redes** > **Configuración IP**.
2. Realice los cambios deseados en la configuración de MTU para la red de grid, la red de administración y la red de cliente.



3. Cuando esté satisfecho con los ajustes, seleccione **Guardar**.
4. Si este procedimiento se completó correctamente y tiene procedimientos adicionales que realizar mientras el nodo se encuentra en modo de mantenimiento, realice ahora. Cuando haya terminado, o si ha experimentado algún fallo y desea volver a empezar, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:
    - Seleccione **Reiniciar en StorageGRID**
    - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. Seleccione esta opción si ha experimentado algún error durante el procedimiento y desea volver a empezar. Cuando el nodo termine de reiniciarse en el modo de mantenimiento, reinicie desde el paso adecuado del procedimiento en que falló.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Administre StorageGRID

Comprobar la configuración del servidor DNS

Puede comprobar y cambiar temporalmente los servidores del sistema de nombres de dominio (DNS) que está utilizando actualmente este nodo de dispositivo.

Lo que necesitará

El aparato se ha estado se colocó en modo de mantenimiento.

Acerca de esta tarea

Es posible que deba cambiar la configuración del servidor DNS si un dispositivo cifrado no puede conectarse con el servidor de gestión de claves (KMS) o un clúster KMS porque el nombre de host del KMS se especificó como un nombre de dominio en lugar de una dirección IP. Cualquier cambio realizado en la configuración de DNS del dispositivo es temporal y se pierde al salir del modo de mantenimiento. Para que estos cambios sean permanentes, especifique los servidores DNS en Grid Manager (**MAINTENANCE** > **Network** > **servidores DNS**).

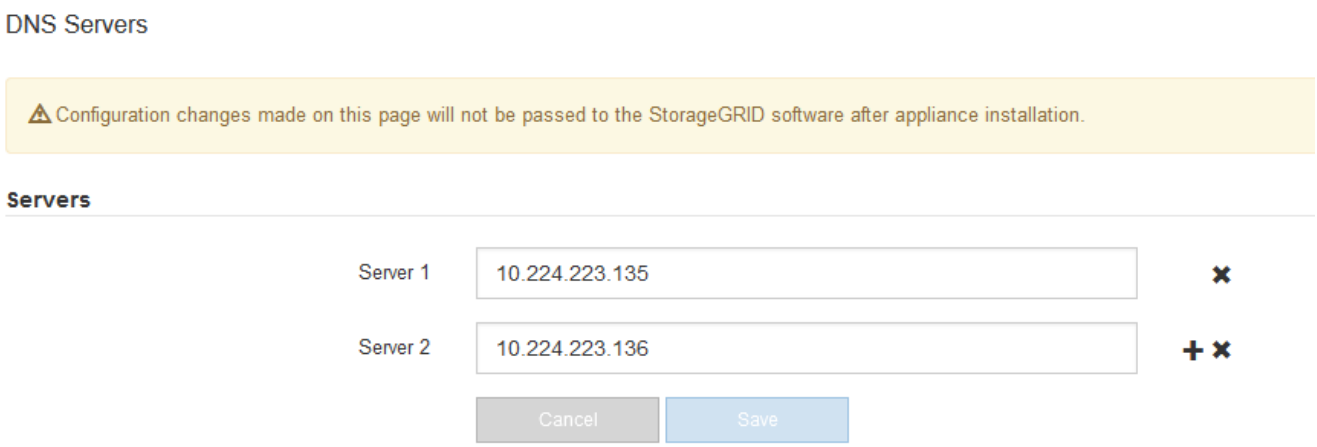
- Los cambios temporales en la configuración DNS sólo son necesarios para los dispositivos cifrados por nodo en los que el servidor KMS se define mediante un nombre de dominio completo, en lugar de una dirección IP, para el nombre de host.
- Cuando un dispositivo cifrado por nodo se conecta a un KMS mediante un nombre de dominio, debe conectarse a uno de los servidores DNS definidos para la cuadrícula. A continuación, uno de estos servidores DNS convierte el nombre de dominio en una dirección IP.
- Si el nodo no puede llegar a un servidor DNS para la cuadrícula, o si cambió la configuración de DNS para toda la cuadrícula cuando un nodo de dispositivo cifrado por nodo estaba sin conexión, el nodo no podrá conectarse al KMS. Los datos cifrados en el dispositivo no se pueden descifrar hasta que se resuelva el problema de DNS.

Para resolver un problema de DNS que impide la conexión de KMS, especifique la dirección IP de uno o más servidores DNS en el instalador de dispositivos de StorageGRID. Estas configuraciones temporales de DNS permiten que el dispositivo se conecte al KMS y descifre los datos en el nodo.

Por ejemplo, si el servidor DNS de la cuadrícula cambia mientras un nodo cifrado estaba desconectado, el nodo no podrá llegar al KMS cuando vuelva a conectarse, ya que sigue utilizando los valores DNS anteriores. La introducción de la nueva dirección IP del servidor DNS en el instalador de dispositivos de StorageGRID permite que una conexión KMS temporal descifre los datos del nodo.

Pasos

1. En el instalador de dispositivos StorageGRID, seleccione **Configurar redes** > **Configuración de DNS**.
2. Compruebe que los servidores DNS especificados sean correctos.



3. Si es necesario, cambie los servidores DNS.

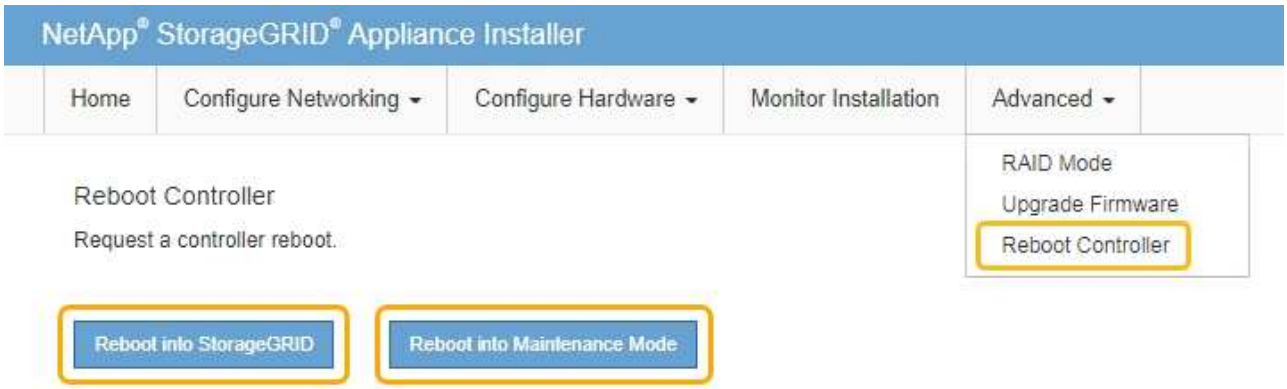
> Los cambios realizados en la configuración de DNS son temporales y se pierden al salir del modo de mantenimiento.

4. Cuando esté satisfecho con la configuración temporal de DNS, seleccione **Guardar**.

   El nodo utiliza la configuración del servidor DNS especificada en esta página para volver a conectarse al KMS, lo que permite descifrar los datos del nodo.

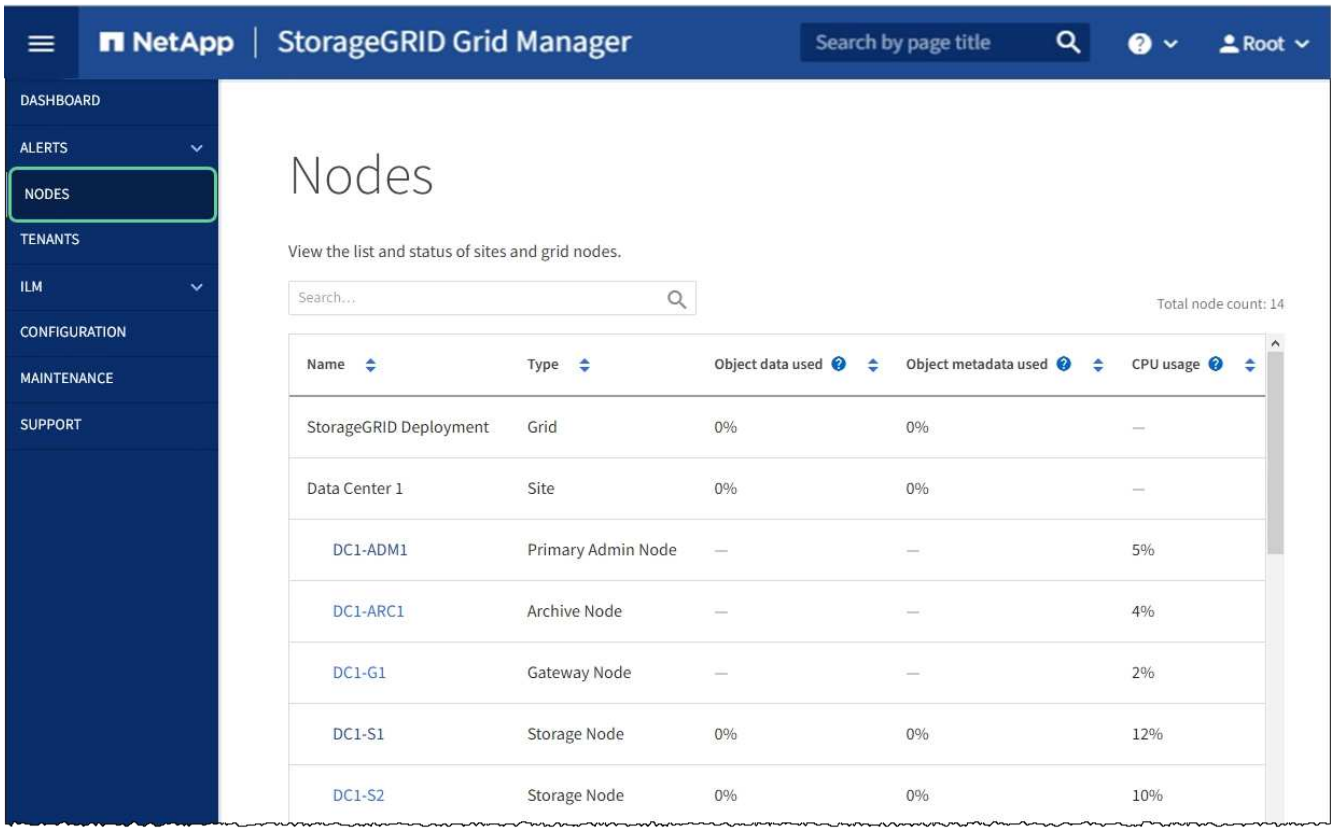
5. Tras descifrar los datos del nodo, reinicie el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



> Cuando el nodo se reinicia y se vuelve a unir a la cuadrícula, utiliza los servidores DNS de todo el sistema enumerados en Grid Manager. Después de volver a unirse a la cuadrícula, el dispositivo ya no utilizará los servidores DNS temporales especificados en el instalador de dispositivos StorageGRID mientras el dispositivo estaba en modo de mantenimiento.

El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Supervisar el cifrado de nodos en modo de mantenimiento (SG6000)

Si habilitó el cifrado de nodos para el dispositivo durante la instalación, puede supervisar el estado de cifrado del nodo de cada nodo de dispositivo, incluidos el estado del cifrado del nodo y detalles del servidor de gestión de claves (KMS).

Lo que necesitará

- El cifrado de nodos debe haber estado habilitado para el dispositivo durante la instalación. No se puede habilitar el cifrado de nodos después de que el dispositivo se haya instalado.
- Ya tienes puso el aparato en modo de mantenimiento.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Configurar hardware** > **cifrado de nodos**.

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption ☑

Save

Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate >

Client certificate >

Clear KMS Key

Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

La página cifrado de nodos incluye estas tres secciones:

- El estado de cifrado muestra si el cifrado de nodos está habilitado o deshabilitado para el dispositivo.
- Detalles del servidor de gestión de claves muestra información sobre el KMS que se utiliza para cifrar el dispositivo. Puede expandir las secciones de certificados de servidor y cliente para ver los detalles y el estado del certificado.
  - Para solucionar problemas con los propios certificados, como renovar certificados caducados, consulte la información sobre KMS en las instrucciones para administrar StorageGRID.
  - Si hay problemas inesperados al conectarse a los hosts KMS, compruebe que los servidores del sistema de nombres de dominio (DNS) son correctos y que la red del dispositivo está configurada correctamente.

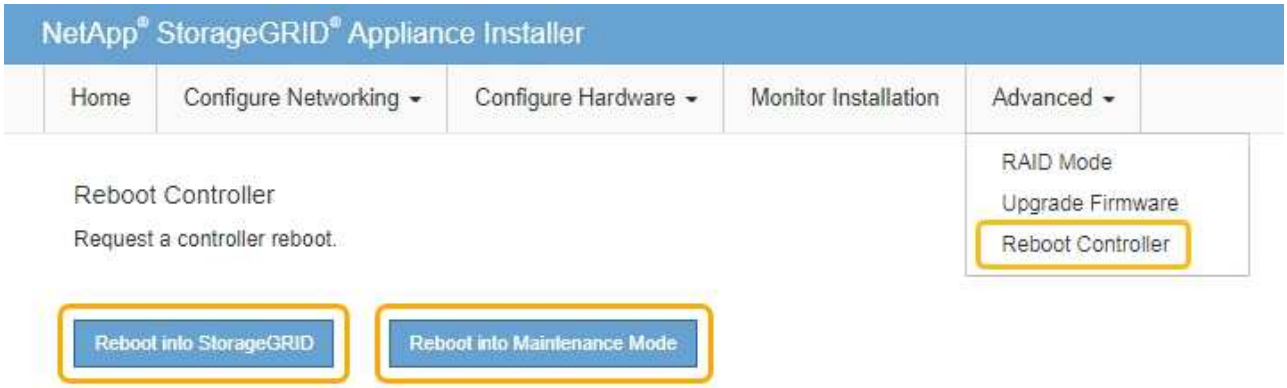
    Comprobar la configuración del servidor DNS

  - Si no puede resolver problemas de certificado, póngase en contacto con el soporte técnico.
- Clear KMS Key deshabilita el cifrado de nodos para el dispositivo, elimina la asociación entre el

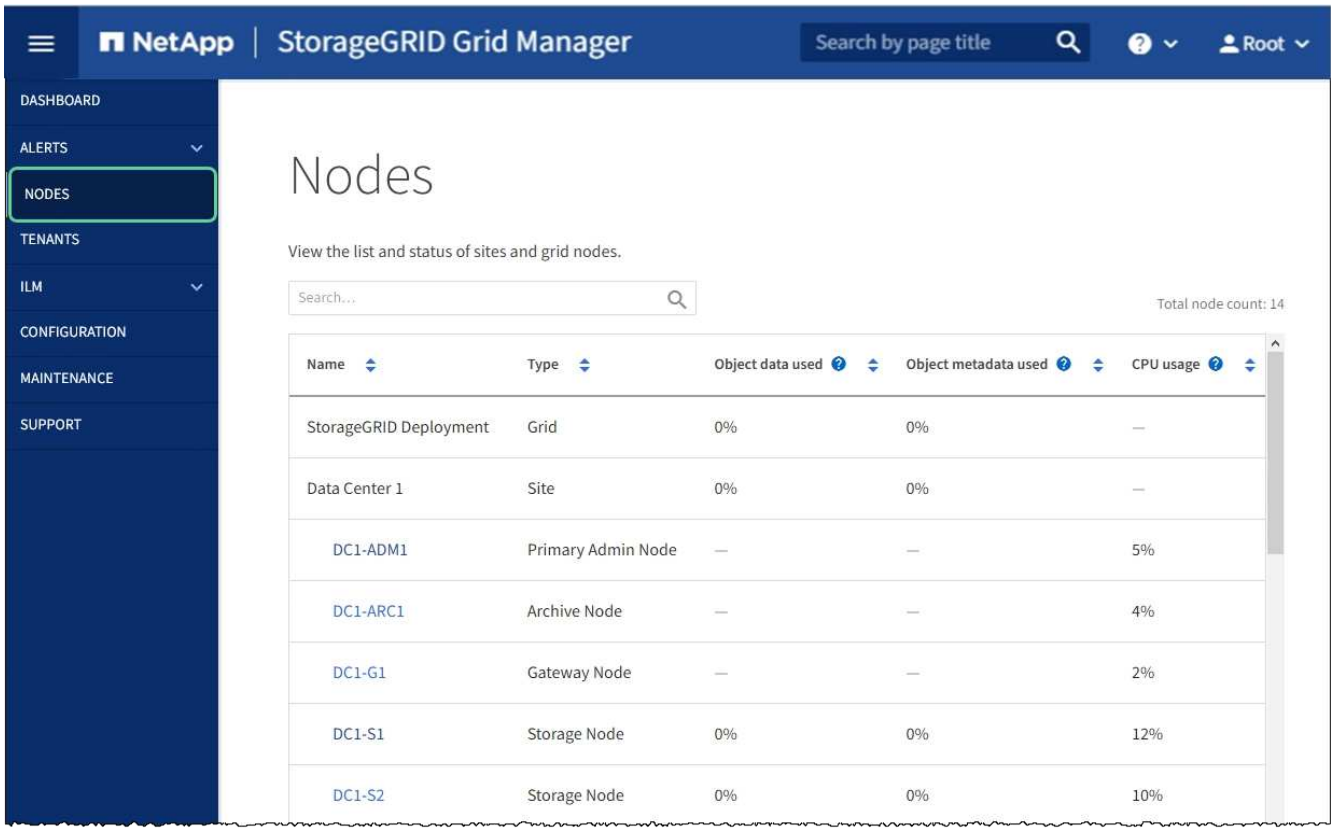
dispositivo y el servidor de gestión de claves configurado para el sitio StorageGRID y elimina todos los datos del dispositivo. Debe Borre la clave KMS Antes de poder instalar el dispositivo en otro sistema StorageGRID.

> Al borrar la configuración de KMS se eliminan los datos del dispositivo, lo que hace que no se pueda acceder a ellos de forma permanente. Estos datos no se pueden recuperar.

2. Cuando haya terminado de comprobar el estado de cifrado de nodo, reinicie el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:
   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Administre StorageGRID

Borrar configuración de servidor de gestión de claves

Al borrar la configuración del servidor de gestión de claves (KMS), se deshabilita el cifrado de nodos en el dispositivo. Tras borrar la configuración de KMS, los datos del dispositivo se eliminan de forma permanente y ya no se puede acceder a ellos. Estos datos no se pueden recuperar.

Lo que necesitará

Si necesita conservar datos en el dispositivo, debe realizar un procedimiento de retirada del nodo o clonar el nodo antes de borrar la configuración de KMS.

> Cuando se borra KMS, los datos del dispositivo se eliminan de forma permanente y ya no se puede acceder a ellos. Estos datos no se pueden recuperar.

Retire el nodo Para mover los datos que contiene a otros nodos en StorageGRID.

Acerca de esta tarea

Al borrar la configuración de KMS del dispositivo, se deshabilita el cifrado de nodos y se elimina la asociación entre el nodo del dispositivo y la configuración de KMS del sitio StorageGRID. Los datos del dispositivo se eliminan y el dispositivo se deja en estado previo a la instalación. Este proceso no se puede revertir.

Debe borrar la configuración de KMS:

- Antes de poder instalar el dispositivo en otro sistema StorageGRID, que no utiliza un KMS o que utiliza un

KMS diferente.

> No borre la configuración de KMS si piensa volver a instalar un nodo de dispositivo en un sistema StorageGRID que utilice la misma clave KMS.

- Antes de poder recuperar y volver a instalar un nodo en el que se perdió la configuración de KMS y la clave KMS no se puede recuperar.
- Antes de devolver cualquier aparato que se haya utilizado anteriormente en su centro.
- Después de retirar un dispositivo con el cifrado de nodos habilitado.

> Retire el dispositivo antes de borrar KMS para mover sus datos a otros nodos del sistema StorageGRID. La eliminación de KMS antes de retirar el dispositivo provocará la pérdida de datos y podría hacer que el dispositivo deje de funcionar.

Pasos

1. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.
   `https://Controller_IP:8443`

   `Controller_IP` Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Configurar hardware** > **cifrado de nodos**.

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption ☑

Save

Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate >

Client certificate >

Clear KMS Key

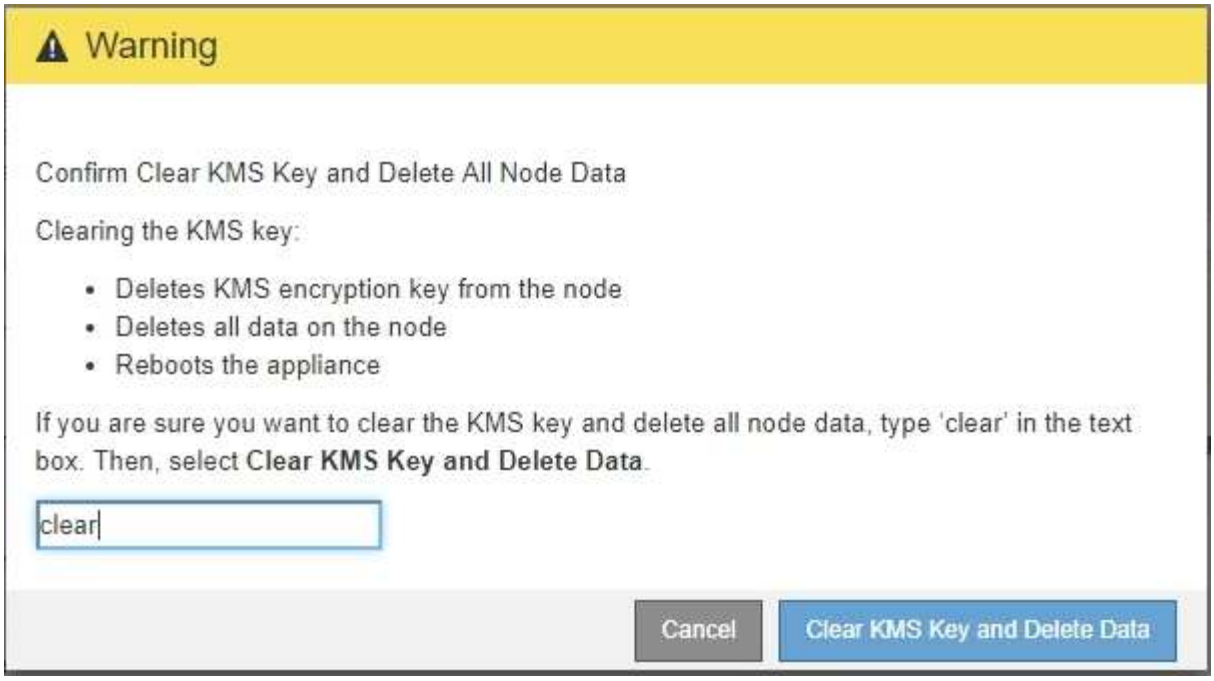
Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

> Si se borra la configuración de KMS, los datos del dispositivo se eliminarán permanentemente. Estos datos no se pueden recuperar.

3. En la parte inferior de la ventana, seleccione **Borrar clave KMS y Eliminar datos**.
4. Si está seguro de que desea borrar la configuración de KMS, escriba **`clear`** + y seleccione **Borrar clave KMS y Eliminar datos**.



La clave de cifrado KMS y todos los datos se eliminan del nodo y el dispositivo se reinicia. Esto puede tardar hasta 20 minutos.

5. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.
   `https://Controller_IP:8443`

   `Controller_IP` Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

6. Seleccione **Configurar hardware** > **cifrado de nodos**.
7. Compruebe que el cifrado de nodos está desactivado y que la información de claves y certificados de **Detalles del servidor de administración de claves** y el control **Borrar clave KMS y Eliminar datos** se eliminan de la ventana.

   El cifrado de nodos no se puede volver a habilitar en el dispositivo hasta que se vuelva a instalar en una cuadrícula.

Después de terminar

Una vez que el dispositivo se haya reiniciado y haya verificado que se ha borrado KMS y que el dispositivo está en estado previo a la instalación, puede quitar físicamente el dispositivo del sistema de StorageGRID. Consulte instrucciones para preparar el aparato para su reinstalación.

Información relacionada

Administre StorageGRID

Dispositivos de almacenamiento SG5700

Información general del dispositivo SG5700 de StorageGRID

El dispositivo SG5700 StorageGRID es una plataforma informática y de almacenamiento integrada que funciona como nodo de almacenamiento en un grid StorageGRID. El dispositivo se puede utilizar en un entorno de grid híbrido que combina los nodos de almacenamiento del dispositivo y los nodos de almacenamiento virtuales (basados en software).

El dispositivo de la serie SG5700 de StorageGRID proporciona las siguientes funciones:

- Integre los elementos de computación y almacenamiento para un nodo de almacenamiento de StorageGRID.
- Incluya el instalador de dispositivos StorageGRID para simplificar la puesta en marcha y la configuración del nodo de almacenamiento.
- Incluye System Manager de la serie E-Series SANtricity para la gestión y supervisión del hardware.
- Admite hasta cuatro conexiones de 10 GbE o 25 GbE a la red Grid y a la red cliente de StorageGRID.
- Admitir unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Cuando estas unidades se usan con la función Drive Security en SANtricity System Manager, se evita el acceso no autorizado a los datos.

El dispositivo SG5700 está disponible en cuatro modelos: SG5712 y SG5712X, así como SG5760 y SG5760X. No existen diferencias de especificación o funcionamiento entre el SG5712 y el SG5712X, excepto la ubicación de los puertos de interconexión de la controladora de almacenamiento. Del mismo modo, no hay especificaciones o diferencias funcionales entre el SG5760 y el SG5760X excepto en lo que respecta a la ubicación de los puertos de interconexión en la controladora de almacenamiento.

Los modelos incluyen los siguientes componentes:

Componente	SG5712	SG5712X	SG5760	SG5760X
Controladora de computación	Controladora E5700SG	Controladora E5700SG	Controladora E5700SG	Controladora E5700SG
Controladora de almacenamiento	Controladora E2800A	Controladora E2800B	Controladora E2800A	Controladora E2800B

Componente	SG5712	SG5712X	SG5760	SG5760X
Chasis	E-Series DE212C, un compartimento de dos unidades rack (2U)	E-Series DE212C, un compartimento de dos unidades rack (2U)	Compartimento DE460C E-Series, un compartimento de cuatro unidades de rack (4U)	Compartimento DE460C E-Series, un compartimento de cuatro unidades de rack (4U)
Unidades	12 unidades NL-SAS (3.5 pulgadas)	12 unidades NL-SAS (3.5 pulgadas)	60 unidades NL-SAS (3.5 pulgadas)	60 unidades NL-SAS (3.5 pulgadas)
Sistemas de alimentación y ventiladores redundantes	Dos contenedores de alimentación/ventilador	Dos contenedores de alimentación/ventilador	Dos contenedores de alimentación y dos contenedores de ventilador	Dos contenedores de alimentación y dos contenedores de ventilador

El almacenamiento bruto máximo disponible en el dispositivo StorageGRID es fijo, en función del número de unidades de cada compartimento. No se puede expandir el almacenamiento disponible si se añade una bandeja con unidades adicionales.

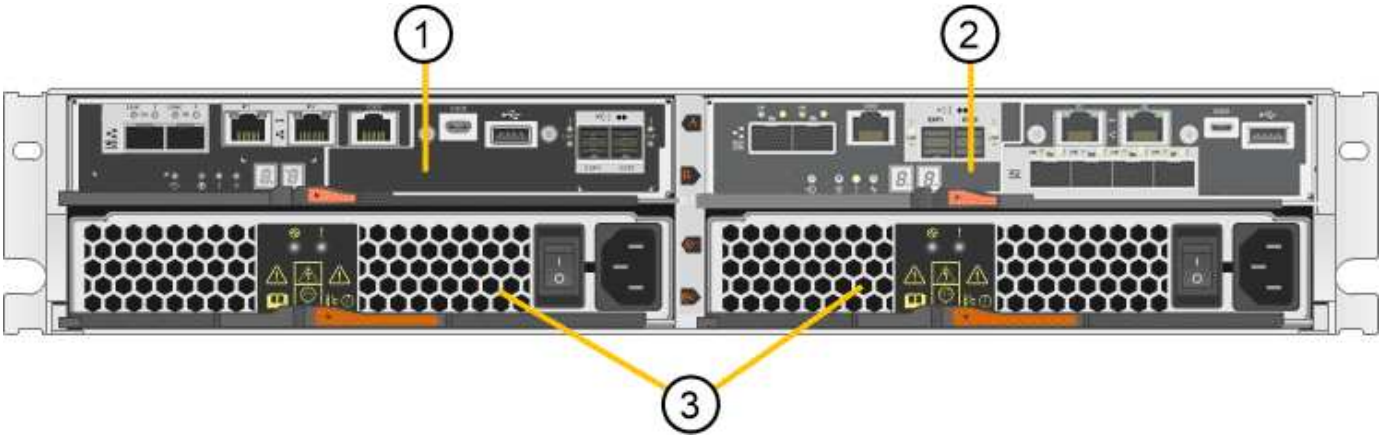
Modelos SG5712 y 5712X

Las cifras muestran el frente y la parte posterior del modelo SG5712 y SG5712X, un compartimento de 2U con 12 unidades.

Vista frontal y trasera SG5712

El SG5712 incluye dos controladoras y dos contenedores de alimentación/ventilador.

Componentes SG5712



Llamada	Descripción
1	Controladora E2800A (controladora de almacenamiento)
2	Controladora E5700SG (controladora de computación)
3	Contenedores de alimentación/ventilador

Vista frontal y trasera SG5712X

El SG5712X incluye dos controladoras y dos contenedores de alimentación/ventilador.

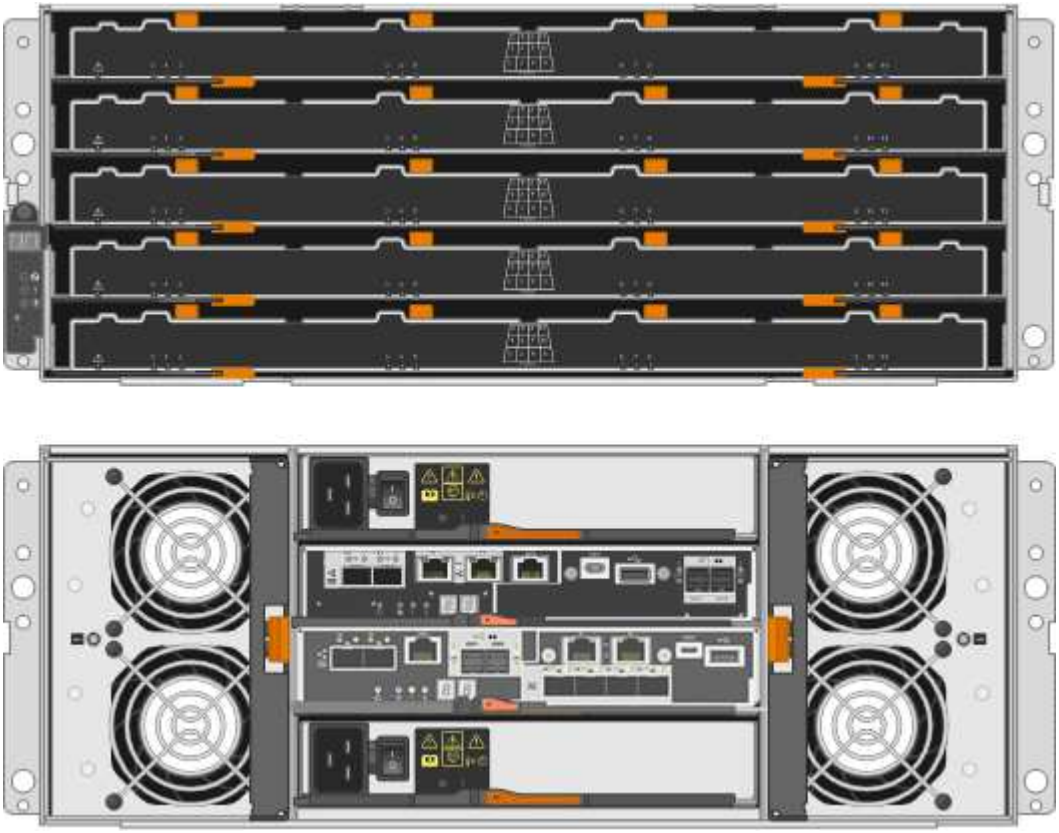
Componentes SG5712X

Llamada	Descripción
1	Controladora E2800B (controladora de almacenamiento)
2	Controladora E5700SG (controladora de computación)
3	Contenedores de alimentación/ventilador

Los modelos SG5760 y SG5760X

Las cifras muestran el frente y la parte posterior de los modelos SG5760 y SG5760X, un compartimento de 4U que tiene 60 unidades en 5 cajones de unidades.

Vista frontal y trasera SG5760

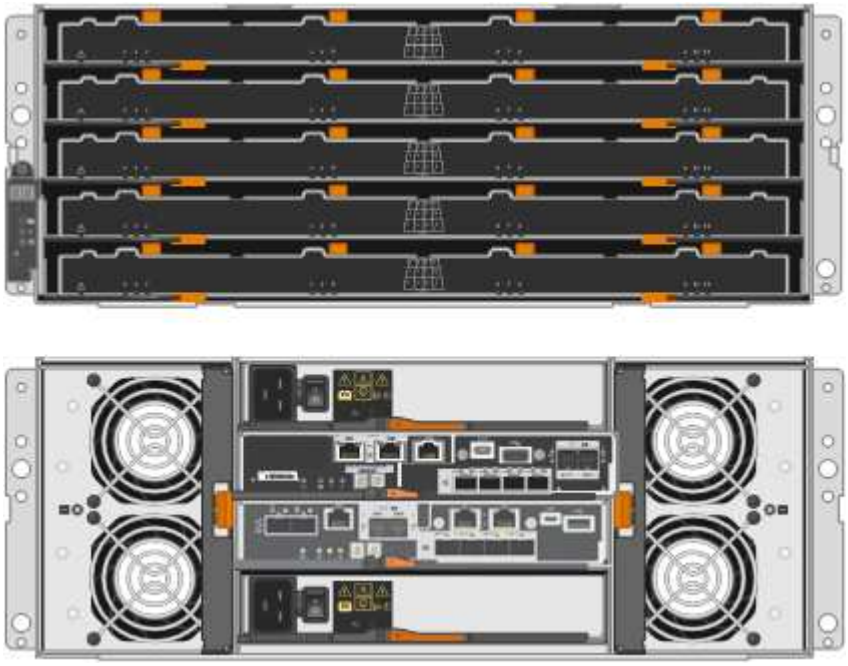


El SG5760 incluye dos controladoras, dos contenedores de ventilador y dos contenedores de alimentación.

Componentes SG5760

Llamada	Descripción
1	Controladora E2800A (controladora de almacenamiento)
2	Controladora E5700SG (controladora de computación)
3	Contenedor de ventilador (1 de 2)
4	Contenedor de alimentación (1 de 2)

Vista frontal y trasera de SG5760X



El SG5760S incluye dos controladoras, dos contenedores de ventilador y dos contenedores de alimentación.

Componentes SG5760X

Llamada	Descripción
1	Controladora E2800B (controladora de almacenamiento)
2	Controladora E5700SG (controladora de computación)
3	Contenedor de ventilador (1 de 2)

Llamada	Descripción
4	Contenedor de alimentación (1 de 2)

Información relacionada

"Sitio de documentación para sistemas E-Series y EF-Series de NetApp"

En el dispositivo StorageGRID 5700

Los modelos SG5712 y SG5712X de 12 unidades, así como los modelos SG5760 y SG5760X de 60 unidades del dispositivo StorageGRID, incluyen una controladora de computación E5700SG y una controladora de almacenamiento E2800 E-Series.

- SG5712 y SG5760 utilizan controladoras E2800A.
- SG5712X y SG5760X utilizan una controladora E2800B.

```
The E2800A and E2800B controllers are identical in specification and
function except for the location of the interconnect ports.
```

Debe revisar los diagramas para saber cuáles son las diferencias entre las controladoras.

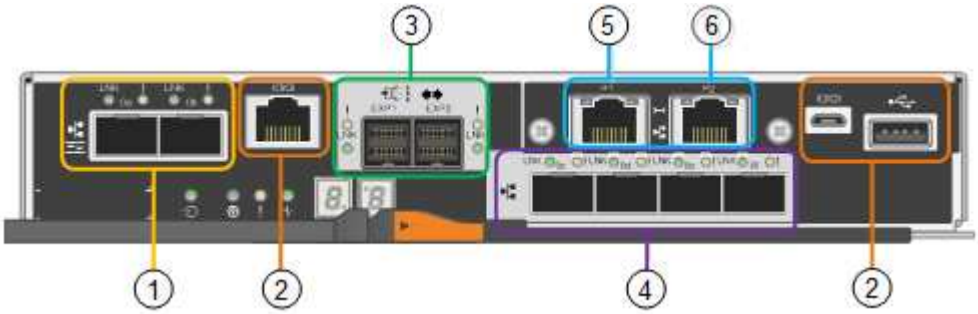
Controladora E5700SG

- Funciona como servidor de computación del dispositivo.
- Incluye el instalador de dispositivos StorageGRID.

> El software StorageGRID no está preinstalado en el dispositivo. A este software se accede desde el nodo de administración cuando se implementa el dispositivo.

- Se puede conectar a las tres redes StorageGRID, incluidas la red de cuadrícula, la red de administración y la red de cliente.
- Se conecta a la controladora E2800 y funciona como iniciador.

En esta figura se muestran los conectores de la parte posterior del controlador E5700SG.



	Puerto	Tipo	Uso
1	Puertos de interconexión 1 y 2	Fibre Channel (FC) de 16 GB/s, SFPA óptico	Conecte la controladora E5700SG a la controladora E2800.
2	Puertos de diagnóstico y soporte	• Puerto serie RJ-45 • Puerto serie micro USB • Puerto USB	Reservado para soporte técnico.
3	Puertos de expansión de unidades	SAS de 12 GB/s	No se utiliza. Los dispositivos StorageGRID no admiten bandejas de unidades de expansión.
4	Puertos de red 1-4	10-GbE o 25-GbE, según el tipo de transceptor SFP, la velocidad del switch y la velocidad de enlace configurada	Conéctese a la red de red y a la red de cliente para StorageGRID.
5	Puerto de gestión 1	Ethernet de 1 GB (RJ-45)	Conéctese a la red de administración para StorageGRID.
6	Puerto de gestión 2	Ethernet de 1 GB (RJ-45)	Opciones: • Bond con el puerto de gestión 1 para una conexión redundante con la red de administrador para StorageGRID. • Deje sin cables y disponible para acceso local temporal (IP 169.254.0.1). • Durante la instalación, utilice el puerto 2 para la configuración de IP si las direcciones IP asignadas por DHCP no están disponibles.

Controladora de almacenamiento serie E2800

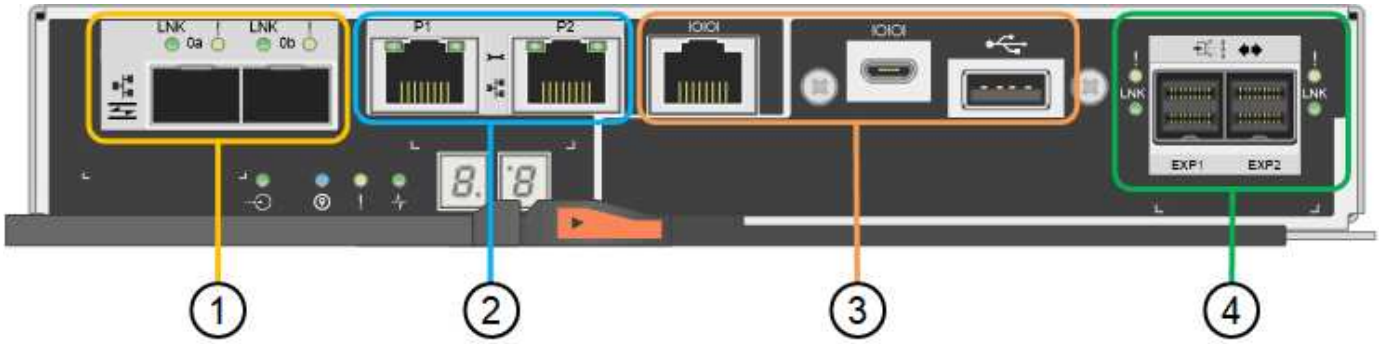
Existen dos versiones de la controladora de almacenamiento E2800 que se utilizan en los dispositivos SG5700: E2800A y E2800B. El E2800A no tiene HIC, y el E2800B tiene una HIC de cuatro puertos. Las dos versiones de controlador tienen especificaciones y funciones idénticas a excepción de la ubicación de los puertos de interconexión.

La controladora de almacenamiento de la serie E2800 tiene las siguientes especificaciones:

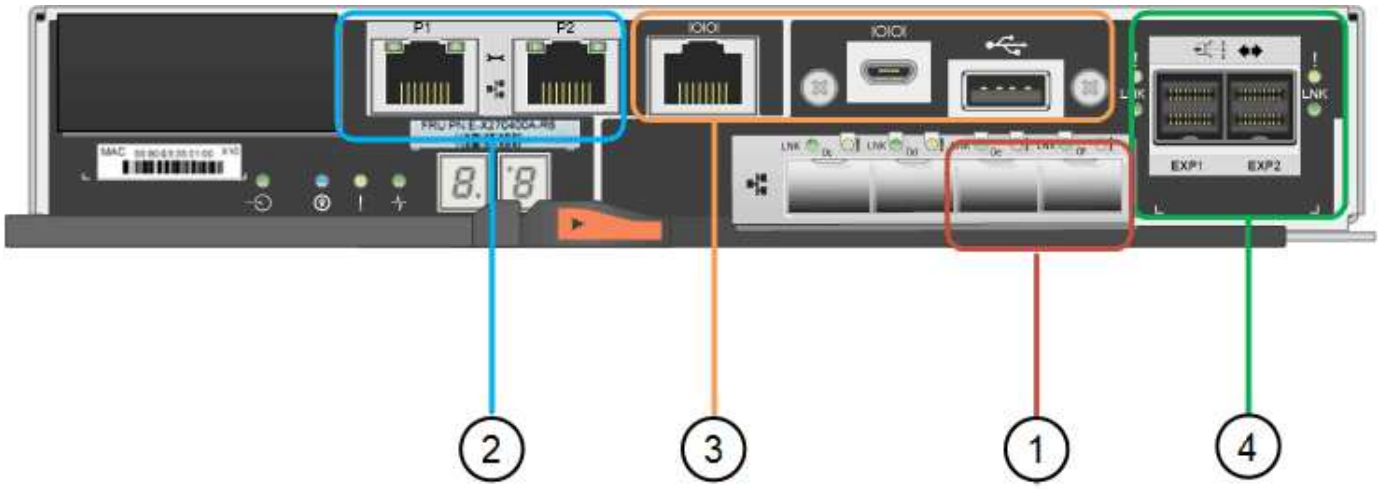
- Funciona como controladora de almacenamiento del dispositivo.
- Gestiona el almacenamiento de datos en las unidades.
- Funciona como controladora E-Series estándar en modo simple.
- Incluye software de sistema operativo SANtricity (firmware de la controladora).
- Incluye System Manager de SANtricity para supervisar el hardware del dispositivo y gestionar alertas, la función AutoSupport y la función Drive Security.
- Se conecta a la controladora E5700SG y funciona como objetivo.

Las siguientes figuras muestran los conectores en la parte posterior de las controladoras E2800A y E2800B.

Conectores en la parte posterior del E2800A



Conectores en la parte posterior del E2800B



	Puerto	Tipo	Uso
1	Puertos de interconexión 1 y 2	SFPA óptico FC de 16 GB/s	Conecte la controladora E2800 a la controladora E5700SG.

	Puerto	Tipo	Uso
2	Puertos de gestión 1 y 2	Ethernet de 1 GB (RJ-45)	• Opciones del puerto 1: ◦ Conéctese a una red de gestión para habilitar el acceso TCP/IP directo a System Manager de SANtricity ◦ Deje sin cables para guardar un puerto del switch y una dirección IP. Acceda a SANtricity System Manager usando las interfaces de usuario del instalador de Grid Manager o Storage Grid Appliance. **Nota**: Algunas funciones opcionales de SANtricity, como sincronización NTP para marcas de hora de registro precisas, no están disponibles cuando elige dejar el puerto 1 sin cable. **Nota**: Se requiere StorageGRID 11.5 o superior, y SANtricity 11.70 o superior, cuando salga del Puerto 1 sin cables. • El puerto 2 está reservado para uso del soporte técnico.
3	Puertos de diagnóstico y soporte	• Puerto serie RJ-45 • Puerto serie micro USB • Puerto USB	Reservado para uso del soporte técnico.

	Puerto	Tipo	Uso
4	Puertos de expansión de unidades.	SAS de 12 GB/s	No se utiliza.

Información general sobre la instalación y la implementación

Puede instalar uno o varios dispositivos StorageGRID cuando implemente StorageGRID por primera vez, o bien puede añadir nodos de almacenamiento del dispositivo más adelante como parte de una ampliación. Es posible que también se deba instalar un nodo de almacenamiento del dispositivo como parte de una operación de recuperación.

Añadir un dispositivo de almacenamiento StorageGRID a un sistema StorageGRID incluye cuatro pasos principales:

1. Preparación de la instalación:
    - Preparación del sitio de instalación
    - Desembalaje de las cajas y comprobación del contenido
    - Obtención de equipos y herramientas adicionales
    - Recopilación de direcciones IP e información de red
    - Opcional: Configurar un servidor de gestión de claves (KMS) externo si planea cifrar todos los datos del dispositivo. Consulte detalles sobre la gestión de claves externas en las instrucciones para administrar StorageGRID.
2. Instalar el hardware:
    - Registrar el hardware
    - Instalación del dispositivo en un armario o rack
    - Instalación de las unidades (solo SG5760)
    - Cableado del aparato
    - Conexión de los cables de alimentación y alimentación
    - Ver los códigos de estado de inicio
3. Configurar el hardware:
    - Acceder a SANtricity System Manager, configurar una dirección IP estática para el puerto de gestión 1 en la controladora E2800 y configurar los ajustes de SANtricity System Manager
    - Acceder al instalador de dispositivos de StorageGRID y configurar los ajustes de enlace e IP de red necesarios para conectarse a redes StorageGRID
    - Opcional: Habilitar el cifrado de nodos si tiene previsto utilizar un KMS externo para cifrar los datos del dispositivo.
    - Opcional: Cambiar el modo RAID.
4. Poner en marcha el dispositivo como nodo de almacenamiento:

Tarea	Instrucciones
Poner en marcha un nodo de almacenamiento del dispositivo en un nuevo sistema StorageGRID	Ponga en marcha el nodo de almacenamiento del dispositivo
Añadir un nodo de almacenamiento del dispositivo a un sistema StorageGRID existente	Instrucciones para ampliar un sistema StorageGRID
Poner en marcha un nodo de almacenamiento del dispositivo como parte de una operación de recuperación de nodo de almacenamiento	Instrucciones para recuperación y mantenimiento

Información relacionada

Preparación de la instalación (SG5700)

Instale el hardware

Configurar hardware (SG5700)

Instale VMware

Instale Red Hat Enterprise Linux o CentOS

Instalar Ubuntu o Debian

Servicios de aplicaciones SG100 y SG1000

Amplíe su grid

Recuperación y mantenimiento

Administre StorageGRID

Preparación de la instalación (SG5700)

Para preparar la instalación de un dispositivo StorageGRID es necesario preparar el sitio y obtener todo el hardware, cables y herramientas necesarios. También debe recopilar información sobre las direcciones IP y la red.

Información relacionada

Requisitos del navegador web

Preparación del sitio (SG5700)

Antes de instalar el dispositivo, debe asegurarse de que el sitio y el armario o rack que desee usar cumplan con las especificaciones de un dispositivo StorageGRID.

Pasos

1. Confirmar que el emplazamiento cumple los requisitos de temperatura, humedad, rango de altitud, flujo de aire, disipación de calor, cableado, alimentación y conexión a tierra. Si desea obtener más información, consulte Hardware Universe de NetApp.

2. Si está instalando el modelo SG5760, confirme que su ubicación proporciona alimentación de CA de 240 voltios.
3. Obtenga un armario o rack de 19 pulgadas (48.3 cm) para colocar bandejas de este tamaño (sin cables):

Modelo de dispositivo	Altura	Anchura	Profundidad	Peso máximo
SG5712 (12 unidades)	3.41 pda (8.68 cm)	17.6 pda (44.7 cm)	21.1 pda (53.6 cm)	63.9 lb (29.0 kg)
SG5760 (60 unidades)	6.87 pda (17.46 cm)	17.66 pda (44.86 cm)	38.25 pda (97.16 cm)	250 lb. (113 kg)

4. Instale los switches de red necesarios. Consulte la herramienta de la matriz de interoperabilidad de NetApp para obtener información de compatibilidad.

Información relacionada

"Hardware Universe de NetApp"

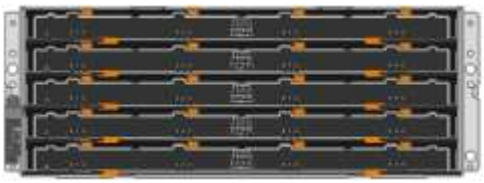
"Herramienta de matriz de interoperabilidad de NetApp"

Cajas de desempaquetado (SG5700)

Antes de instalar el aparato StorageGRID, desembale todas las cajas y compare el contenido con los artículos del recibo de embalaje.

- **SG5712 con 12 unidades instaladas**

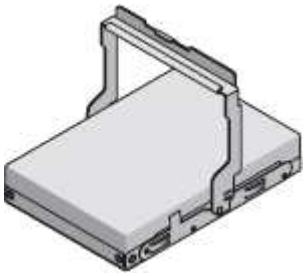
- **Dispositivo SG5760 sin unidades instaladas**



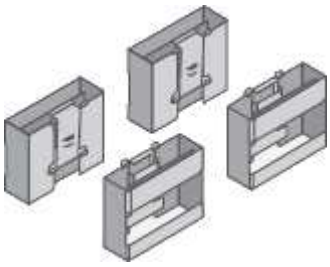
- **Bisel frontal para el aparato**

- **Kit de guías con instrucciones**

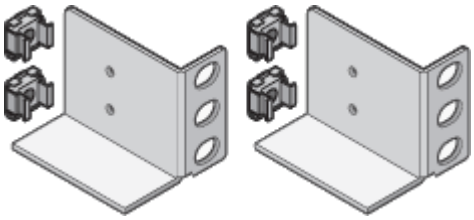
- **SG5760: Sesenta unidades**



- **SG5760: Identificadores**



- **SG5760: Soportes de fondo y tuercas de jaula para la instalación de bastidores de agujero cuadrado**



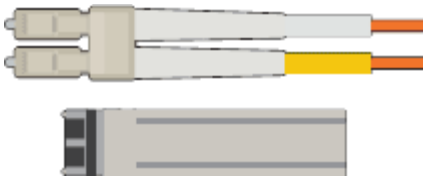
Cables y conectores

El envío del dispositivo StorageGRID incluye los siguientes cables y conectores:

- **Dos cables de alimentación para su país**

  Es posible que el armario tenga cables de alimentación especiales que utilice en lugar de los cables de alimentación que se suministran con el aparato.

- **Cables ópticos y transceptores SFP**



Dos cables ópticos para los puertos de interconexión de FC

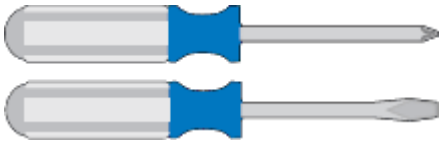
Ocho transceptores SFP+, compatible con los cuatro puertos FC interconnect de 16 GB/s y los cuatro puertos de red de 10 GbE

Obtener equipamiento y herramientas adicionales (SG5700)

Antes de instalar el aparato StorageGRID, confirme que dispone de todos los equipos y herramientas adicionales que necesita.

Necesitará el siguiente equipo adicional para instalar y configurar el hardware:

- **Destornilladores**

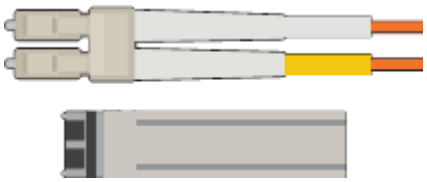


Phillips no 2 destornillador

Destornillador plano medio

- **Muñequera ESD**

- **Cables ópticos y transceptores SFP**



Cables ópticos para los puertos 10/25-GbE que tiene previsto utilizar

Opcional: Transceptores SFP28 si desea utilizar velocidad de enlace 25-GbE

- **Cables Ethernet**

- **Portátil de servicio**

Navegador web compatible

Cliente SSH, como PuTTY

Puerto Ethernet de 1 GB (RJ-45)

- **Herramientas opcionales**

Taladro eléctrico con punta Phillips

Linterna

Elevación mecanizada para SG5760

Revisar las conexiones de red del dispositivo (SG5700)

Antes de instalar el dispositivo StorageGRID, debe comprender qué redes se pueden conectar al dispositivo y cómo se utilizan los puertos de cada controladora.

Redes de dispositivos StorageGRID

Al implementar un dispositivo de StorageGRID como nodo de almacenamiento en un grid StorageGRID, puede conectarlo a las siguientes redes:

- **Red de Grid para StorageGRID**: 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. Se requiere la red de red.

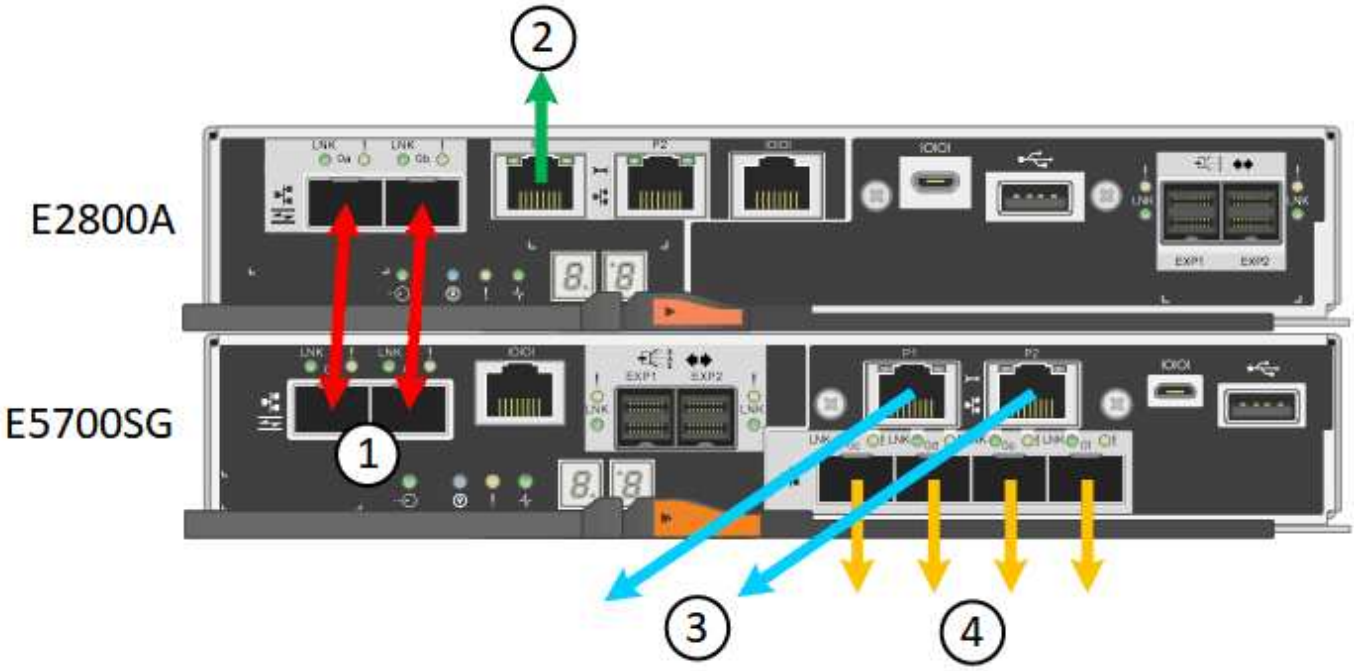
- **Red de administración para StorageGRID**: La Red de administración es una red cerrada que se utiliza para la administración y el mantenimiento del sistema. La red de administración suele ser una red privada y no es necesario que se pueda enrutar entre sitios. La red administrativa es opcional.
- **Red de clientes para StorageGRID:** la red de clientes es una red abierta que se utiliza para proporcionar acceso a las aplicaciones cliente, incluidos S3 y Swift. La red de cliente proporciona acceso de protocolo de cliente a la cuadrícula, de modo que la red de red de red pueda aislarse y protegerse. La red cliente es opcional.
- **Red de administración para el Administrador del sistema SANtricity** (opcional): Esta red proporciona acceso al Administrador del sistema SANtricity en la controladora E2800, lo que le permite supervisar y administrar los componentes de hardware del dispositivo. Esta red de gestión puede ser la misma que la Red de administración para StorageGRID, o bien puede ser una red de gestión independiente.

  Si la red opcional de SANtricity System Manager no está conectada, es posible que no pueda utilizar algunas funciones SANtricity.

Para obtener información detallada acerca de las redes StorageGRID, consulte *Grid primer*.

Conexiones de dispositivos StorageGRID

Al instalar un dispositivo StorageGRID, debe conectar las dos controladoras entre sí y a las redes necesarias. La figura muestra las dos controladoras del SG5760, con la controladora E2800 en la parte superior y la controladora E5700SG en la parte inferior. En SG5712, la controladora E2800 se encuentra a la izquierda de la controladora E5700SG.



	Puerto	Tipo de puerto	Función
1	Dos puertos de interconexión en cada controladora	SFP+ óptico FC de 16 GB/s	Conecte las dos controladoras entre sí.

	Puerto	Tipo de puerto	Función
2	Puerto de gestión 1 en la controladora E2800	1 GbE (RJ-45).	Se conecta a la red en la que se accede a System Manager de SANtricity. Es posible usar la red administrativa para StorageGRID o una red de gestión independiente.
2	Puerto de gestión 2 en la controladora E2800	1 GbE (RJ-45).	Reservado para soporte técnico.
3	Puerto de gestión 1 en la controladora E5700SG	1 GbE (RJ-45).	Conecta la controladora E5700SG a la red de administración para StorageGRID.
3	Puerto de gestión 2 en la controladora E5700SG	1 GbE (RJ-45).	• Se puede unir al puerto de administración 1 si desea una conexión redundante a la red de administración. • Puede dejarse sin cables y disponible para acceso local temporal (IP 169.254.0.1). • Durante la instalación, se puede utilizar para conectar la controladora E5700SG a un portátil de servicio si las direcciones IP asignadas por DHCP no están disponibles.
4	10 puertos 1-4 de 25 GbE en la controladora E5700SG	10-GbE o 25-GbE **Nota:** los transceptores SFP+ incluidos con el dispositivo admiten velocidades de enlace de 10 GbE. Si desea utilizar velocidades de enlace de 25-GbE para los cuatro puertos de red, debe proporcionar transceptores SFP28.	Conéctese a la red de red y a la red de cliente para StorageGRID. Consulte «'conexiones de puertos 10/25-GbE para el controlador E5700SG'».

Información relacionada

Reunir información de instalación (SG5700)

Dispositivo de cable (SG5700)

Modos de enlace de puerto para puertos de controladora E5700SG

Directrices sobre redes

Instale VMware

Instale Red Hat Enterprise Linux o CentOS

Instalar Ubuntu o Debian

Modos de enlace de puerto para puertos de controladora E5700SG

Al configurar enlaces de red para los puertos de la controladora E5700SG, puede utilizar la vinculación de puertos para los puertos 10/25-GbE que se conectan a la red de grid y la red de cliente opcional, y los puertos de gestión de 1-GbE que se conectan a la red de administración opcional. El enlace de puertos ayuda a proteger los datos proporcionando rutas redundantes entre las redes StorageGRID y el dispositivo.

Información relacionada

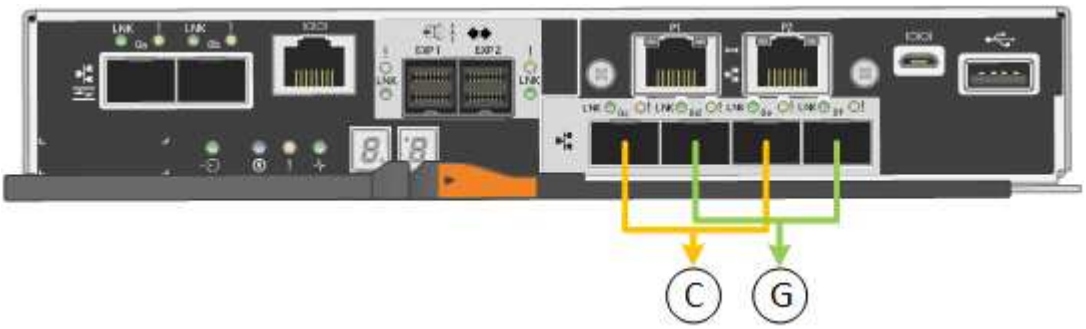
Configurar enlaces de red (SG5700)

Modos de enlace de red para puertos 10/25-GbE

Los puertos de red 10/25-GbE de la controladora E5700SG admiten el modo de enlace de puerto fijo o el modo de enlace de puerto agregado para las conexiones de red de Grid y de cliente.

Modo de enlace de puerto fijo

El modo fijo es la configuración predeterminada para los puertos de red de 10/25-GbE.



Llamada	Qué puertos están Unidos
C	Los puertos 1 y 3 se unen para la red cliente, si se utiliza esta red.

Llamada	Qué puertos están Unidos
G	Los puertos 2 y 4 están Unidos para la red de cuadrícula.

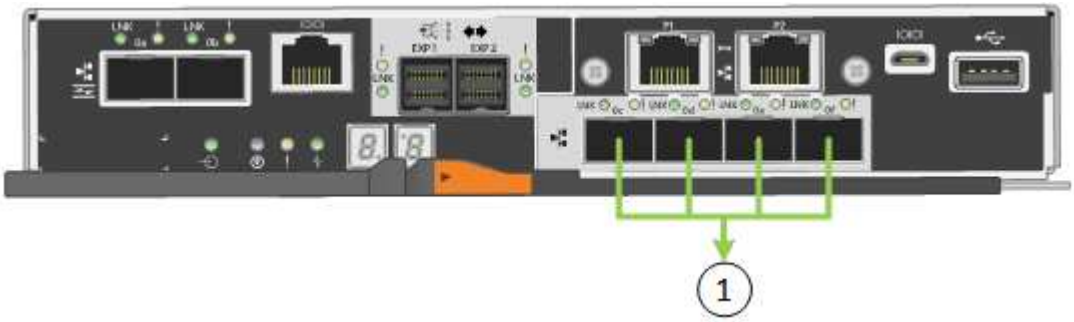
Cuando se utiliza el modo de enlace de puerto fijo, se puede utilizar uno de los dos modos de enlace de red: Active-Backup o el protocolo de control de agregación de enlaces (LACP).

- En el modo Active-Backup (predeterminado), sólo hay un puerto activo a la vez. Si se produce un error en el puerto activo, su puerto de backup proporciona automáticamente una conexión de conmutación por error. El puerto 4 proporciona una ruta de copia de seguridad para el puerto 2 (red de red de cuadrícula) y el puerto 3 proporciona una ruta de copia de seguridad para el puerto 1 (red de cliente).
- En el modo LACP, cada par de puertos forma un canal lógico entre la controladora y la red, lo que permite un mayor rendimiento. Si un puerto falla, el otro continúa proporcionando el canal. El rendimiento se reduce, pero la conectividad no se ve afectada.

> Si no necesita conexiones redundantes, sólo puede utilizar un puerto para cada red. Sin embargo, tenga en cuenta que se generará una alarma en el administrador de grid después de instalar StorageGRID, lo que indica que se ha desenchufado un cable. Puede reconocer esta alarma de forma segura para borrarla.

Modo de enlace de puerto agregado

El modo de enlace de puerto de agregado aumenta de forma significativa las mejoras en cada red StorageGRID y proporciona rutas de conmutación al nodo de respaldo adicionales.



Llamada	Qué puertos están Unidos
1	Todos los puertos conectados se agrupan en un único enlace LACP, lo que permite que todos los puertos se usen para el tráfico de red de grid y de red de cliente.

Si tiene pensado utilizar el modo de enlace de puerto agregado:

- Debe usar el modo de enlace de red LACP.
- Debe especificar una etiqueta de VLAN exclusiva para cada red. Esta etiqueta VLAN se añadirá a cada paquete de red para garantizar que el tráfico de red se dirija a la red correcta.
- Los puertos deben estar conectados a switches que sean compatibles con VLAN y LACP. Si varios switches participan en el enlace LACP, los switches deben ser compatibles con los grupos de agregación de enlaces de varios chasis (MLAG), o equivalentes.

- Debe comprender cómo configurar los switches para que utilicen VLAN, LACP y MLAG, o equivalente.

Si no desea usar los cuatro puertos 10/25-GbE, puede usar uno, dos o tres puertos. El uso de más de un puerto maximiza la posibilidad de que cierta conectividad de red permanezca disponible si falla uno de los puertos 10/25-GbE.

> Si decide utilizar menos de cuatro puertos, tenga en cuenta que puede activarse una alerta * de enlace de dispositivo de servicios* en Grid Manager después de instalar el nodo del dispositivo, lo que indica que se ha desenchufado un cable. Puede deshabilitar con seguridad esta regla de alerta para la alerta activada. En Grid Manager, seleccione **ALERTS** > **Reglas**, seleccione la regla y haga clic en **Editar regla**. A continuación, desactive la casilla de verificación **Activado**.

Modos de enlace de red para puertos de gestión de 1 GbE

Para los dos puertos de gestión de 1 GbE en la controladora E5700SG, puede elegir el modo de enlace de red independiente o el modo de enlace de red Active-Backup para conectarse a la red opcional Admin Network.

En modo independiente, solo el puerto de gestión 1 está conectado a la red del administrador. Este modo no proporciona una ruta de acceso redundante. El puerto de administración 2 no tiene cables y está disponible para las conexiones locales temporales (utilice la dirección IP 169.254.0.1)

En el modo Active-Backup, los puertos de gestión 1 y 2 están conectados a la red Admin. Solo hay un puerto activo a la vez. Si se produce un error en el puerto activo, su puerto de backup proporciona automáticamente una conexión de conmutación por error. La vinculación de estos dos puertos físicos en un puerto de gestión lógica proporciona una ruta redundante a la red de administración.

> Si necesita establecer una conexión local temporal con la controladora E5700SG cuando los puertos de gestión de 1-GbE están configurados para el modo Active-Backup, quite los cables de ambos puertos de gestión, conecte el cable temporal al puerto de gestión 2 y acceda al dispositivo con la dirección IP 169.254.0.1.

Reunir información de instalación (SG5700)

Al instalar y configurar el dispositivo StorageGRID, debe tomar decisiones y recopilar información acerca de los puertos del switch Ethernet, las direcciones IP y los modos de enlace de puerto y red.

Acerca de esta tarea

Puede utilizar las siguientes tablas para registrar la información necesaria para cada red que conecte al dispositivo. Estos valores son necesarios para instalar y configurar el hardware.

La información necesaria para conectarse a System Manager de SANtricity en la controladora E2800

Debe conectar la controladora E2800 a la red de gestión que usará para SANtricity System Manager.

Información necesaria	Su valor
El puerto del switch Ethernet se conectará al puerto de gestión 1	
Dirección MAC para el puerto de gestión 1 (impreso en una etiqueta cerca del puerto P1 para la controladora E2800A y 0a para la controladora E2800B)	
Dirección IP asignada por DHCP para el puerto de gestión 1, si está disponible después de encenderse **Nota:** Si la red que va a conectar al controlador E2800 incluye un servidor DHCP, el administrador de red puede utilizar la dirección MAC para determinar la dirección IP asignada por el servidor DHCP.	
Velocidad y modo doble **Nota:** debe asegurarse de que el conmutador Ethernet de la red de administración de SANtricity System Manager está establecido en Negotiate automático.	Debe ser: • Autonegociar (predeterminado)
Formato de dirección IP	Elija una opción: • IPv4 • IPv6
Dirección IP estática que planea usar para el dispositivo en la red de gestión	Para IPv4: • Dirección IPv4: • Máscara de subred: • Puerta de enlace: Para IPv6: • Dirección IPv6: • Dirección IP enrutable: • Dirección IP del enrutador de la controladora E2800:

Información necesaria para conectar el controlador E5700SG a la red de administración

La red de administración de StorageGRID es una red opcional que se utiliza para la administración y el mantenimiento del sistema. El dispositivo se conecta a la red de administrador mediante los puertos de gestión de 1-GbE en la controladora E5700SG.

Información necesaria	Su valor
Red de administrador habilitada	Elija una opción: • No • Sí (predeterminado)
Modo de enlace de red	Elija una opción: • Independiente • Copia de seguridad activa
Puerto del switch para el puerto 1	
Puerto del switch para el puerto 2 (únicamente modo de enlace de red Active-Backup)	
Dirección IP asignada por DHCP para el puerto de gestión 1, si está disponible después de encenderse **Nota:** Si la red Admin incluye un servidor DHCP, el controlador E5700SG muestra la dirección IP asignada por DHCP en su pantalla de siete segmentos después de que se inicie. También puede determinar la dirección IP asignada por DHCP utilizando la dirección MAC para buscar la IP asignada.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Dirección IP estática que piensa usar para el nodo de almacenamiento del dispositivo en la red de administración **Nota:** Si su red no tiene una puerta de enlace, especifique la misma dirección IPv4 estática para la puerta de enlace.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Subredes de red de administración (CIDR)	

La información necesaria para conectar y configurar puertos 10/25-GbE en la controladora E5700SG

Los cuatro puertos 10/25-GbE del controlador E5700SG se conectan a la red de grid y la red de cliente de StorageGRID.

> Consulte "conexiones de puerto 10/25-GbE para la controladora E5700SG" para obtener más información sobre las opciones de estos puertos.

Información necesaria	Su valor
Velocidad de enlace **Nota:** Si selecciona 25 GbE, debe instalar transceptores SPF28. No se admite la negociación automática, por lo que también debe configurar los puertos y los switches conectados para 25 GbE.	Elija una opción: • 10 GbE (predeterminado) • 25 GbE
Modo de enlace de puerto	Elija una opción: • Fijo (predeterminado) • Agregado
Puerto del switch para el puerto 1 (red cliente)	
Puerto del switch para el puerto 2 (red de cuadrícula)	
Puerto del switch para el puerto 3 (red cliente)	
Puerto del switch para el puerto 4 (red Grid)	

Información necesaria para conectar el controlador E5700SG a Grid Network

Grid Network para StorageGRID es una red necesaria que se utiliza para todo el tráfico interno de StorageGRID. El dispositivo se conecta a la red Grid mediante los puertos 10/25-GbE en la controladora E5700SG.

> Consulte "conexiones de puerto 10/25-GbE para la controladora E5700SG" para obtener más información sobre las opciones de estos puertos.

Información necesaria	Su valor
Modo de enlace de red	Elija una opción: • Active-Backup (predeterminado) • LACP (802.3ad)
Etiquetado VLAN habilitado	Elija una opción: • No (predeterminado) • Sí
Etiqueta de VLAN (si el etiquetado de VLAN está habilitado)	Introduzca un valor entre 0 y 4095:

Información necesaria	Su valor
Dirección IP asignada por DHCP para la red de cuadrícula, si está disponible después del encendido **Nota:** Si Grid Network incluye un servidor DHCP, el controlador E5700SG muestra la dirección IP asignada por DHCP para la Red de cuadrícula en su pantalla de siete segmentos después de que se inicie.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Dirección IP estática que tiene previsto usar para el nodo de almacenamiento del dispositivo en la red de grid **Nota:** Si su red no tiene una puerta de enlace, especifique la misma dirección IPv4 estática para la puerta de enlace.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Subredes de red de cuadrícula (CIDR) **Nota:** Si la red de cliente no está activada, la ruta predeterminada del controlador utilizará la puerta de enlace especificada aquí.	

Información necesaria para conectar el controlador E5700SG a la red cliente

La red de cliente para StorageGRID es una red opcional que se suele utilizar para proporcionar acceso al protocolo de cliente al grid. El dispositivo se conecta a la red cliente mediante los puertos 10/25-GbE en la controladora E5700SG.

> Consulte "conexiones de puerto 10/25-GbE para la controladora E5700SG" para obtener más información sobre las opciones de estos puertos.

Información necesaria	Su valor
Red de cliente habilitada	Elija una opción: • No (predeterminado) • Sí
Modo de enlace de red	Elija una opción: • Active-Backup (predeterminado) • LACP (802.3ad)

Información necesaria	Su valor
Etiquetado VLAN habilitado	Elija una opción: • No (predeterminado) • Sí
Etiqueta de VLAN (Si el etiquetado de VLAN está habilitado)	Introduzca un valor entre 0 y 4095:
Dirección IP asignada por DHCP para la red cliente, si está disponible después del encendido	• Dirección IPv4 (CIDR): • Puerta de enlace:
Dirección IP estática que tiene previsto usar para el nodo de almacenamiento del dispositivo en la red cliente **Nota:** Si la red de cliente está activada, la ruta predeterminada del controlador utilizará la puerta de enlace especificada aquí.	• Dirección IPv4 (CIDR): • Puerta de enlace:

Información relacionada

Revisar las conexiones de red del dispositivo (SG5700)

Modos de enlace de puerto para puertos de controladora E5700SG

Configurar hardware (SG5700)

Instalar el hardware (SG5700)

La instalación del hardware implica la instalación del dispositivo en un armario o rack, la conexión de los cables y la alimentación.

Registre el hardware

El registro del hardware del dispositivo proporciona ventajas de asistencia.

Pasos

1. Busque el número de serie del chasis.

   Puede encontrar el número en el recibo de embalaje, en el correo electrónico de confirmación o en el aparato después de desembalarlo.

2. Vaya al sitio de soporte de NetApp en "mysupport.netapp.com".
3. Determine si necesita registrar el hardware:

Si usted es un…	Siga estos pasos…
Cliente existente de NetApp	a. Inicie sesión con su nombre de usuario y contraseña. b. Seleccione **Productos** > **Mis productos**. c. Confirme que el nuevo número de serie aparece en la lista. d. De lo contrario, siga las instrucciones para nuevos clientes de NetApp.
Nuevo cliente de NetApp	a. Haga clic en **Registrar ahora** y cree una cuenta. b. Seleccione **Productos** > **Registrar productos**. c. Introduzca el número de serie del producto y los detalles solicitados. Una vez aprobado el registro, puede descargar el software necesario. El proceso de aprobación puede llevar hasta 24 horas.

Instale el dispositivo en armario o rack (SG5700)

Debe instalar rieles en su armario o rack y, a continuación, deslizar el dispositivo sobre los rieles. Si tiene un SG5760, debe instalar las unidades después de instalar el dispositivo.

Lo que necesitará

- Ha revisado el documento de avisos de seguridad que se incluye en la caja y comprende las precauciones para mover e instalar el hardware.
- Tiene las instrucciones incluidas en el kit de raíl.
- Dispone de las *instrucciones de instalación y configuración* del aparato.

Instale el hardware desde la parte inferior del rack, armario o rack hasta para evitar que el equipo vuelque.

El SG5712 pesa aproximadamente 29 kg (64 lb) cuando está totalmente cargado con unidades. Se requiere que dos personas o un ascensor mecanizado muevan de forma segura el SG5712.

El SG5760 pesa aproximadamente 60 kg (132 lb) sin unidades instaladas. Se requiere que cuatro personas o un ascensor mecanizado muevan de forma segura un SG5760 vacío.

Para evitar que se dañe el hardware, no mueva nunca un SG5760 si hay unidades instaladas. Debe quitar todas las unidades antes de mover la bandeja.

Pasos

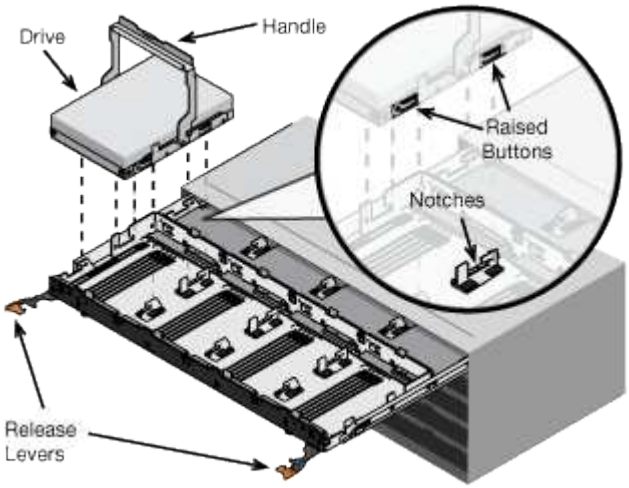
1. Siga con cuidado las instrucciones del kit de raíl para instalar los rieles en su armario o rack.

2. Si tiene un SG5760, siga estos pasos para preparar el traslado del aparato.
   a. Retire la caja de embalaje exterior. A continuación, pliegue las solapas de la caja interior.
   b. Si va a levantar el SG5760 manualmente, fije las cuatro asas a los lados del chasis.

      Retire estas asas mientras desliza el aparato sobre los rieles.
3. Consulte las *instrucciones de instalación y configuración* y deslice el aparato en el armario o bastidor.
4. Consulte las *instrucciones de instalación y configuración* y fije el aparato al armario o bastidor.

   Si tiene un SG5760, utilice los soportes posteriores para fijar el aparato a la parte posterior del rack o armario. Utilice las tuercas de jaula si el bastidor o el armario tiene orificios cuadrados.
5. Si tiene un SG5760, instale 12 unidades en cada uno de los cajones de 5 unidades.

   Debe instalar las 60 unidades para garantizar que su funcionamiento es correcto.
   a. Coloque la muñequera ESD y retire los accionamientos de su embalaje.
   b. Suelte las palancas del cajón de mando superior y deslice el cajón hacia fuera con las palancas.
   c. Levante el asa de la unidad a la posición vertical y alinee los botones de la unidad con las muescas del cajón.



   d. Al presionar suavemente en la parte superior de la unidad, gire la palanca de mando hacia abajo hasta que la unidad encaje en su lugar.
   e. Después de instalar los primeros 12 mandos, deslice el cajón hacia atrás presionando el centro y cerrando ambas palancas con cuidado.
   f. Repita estos pasos para los otros cuatro cajones.
6. Conecte el panel frontal.

Dispositivo de cable (serie SG5700)

Debe conectar las dos controladoras entre sí, conectar los puertos de gestión de cada controladora y conectar los puertos 10/25-GbE de la controladora E5700SG a la red de grid y la red de cliente opcional para StorageGRID.

Lo que necesitará

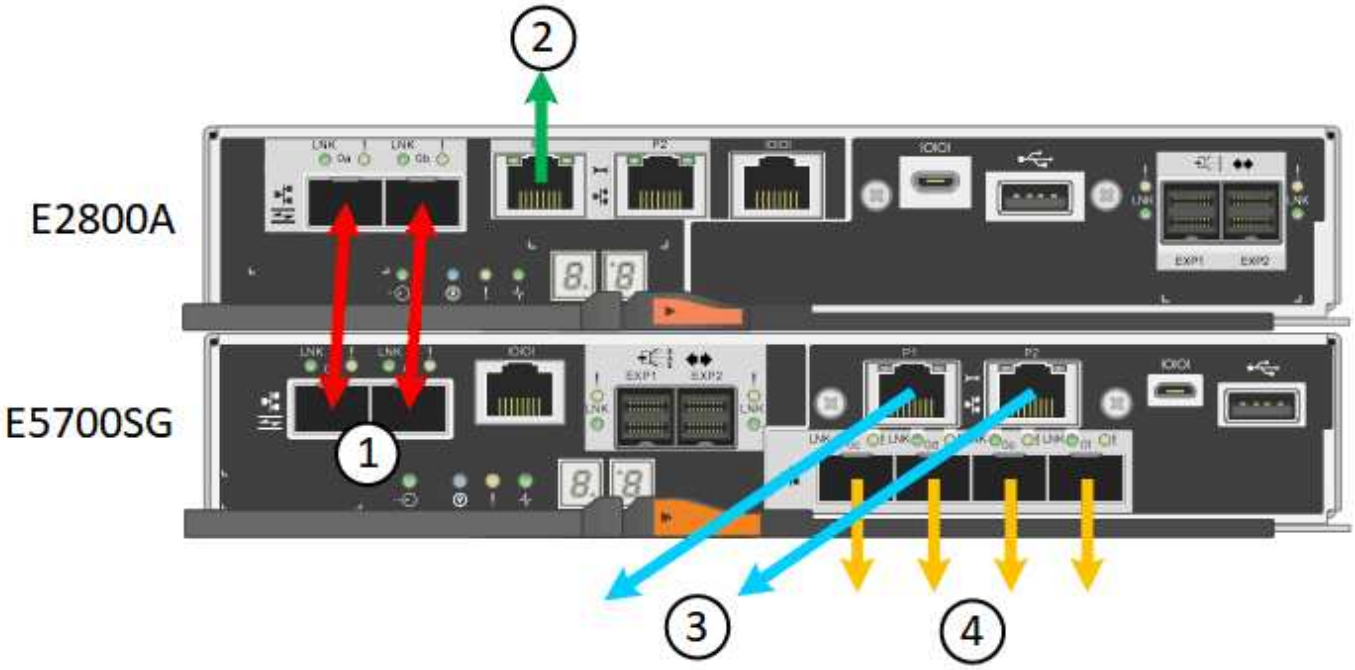
- Ha desembalado los siguientes elementos, que se incluyen con el aparato:
  - Dos cables de alimentación.
  - Dos cables ópticos para los puertos de interconexión de FC en las controladoras.
  - Ocho transceptores SFP+, que admiten FC de 10-GbE o 16 Gbps. Los transceptores pueden utilizarse con los dos puertos de interconexión de ambas controladoras y con los cuatro puertos de red 10/25-GbE de la controladora E5700SG, suponiendo que desee que los puertos de red utilicen una velocidad de enlace de 10-GbE.
- Ha obtenido los siguientes elementos, que no se incluyen con el aparato:
  - De uno a cuatro cables ópticos para los puertos 10/25-GbE que planea utilizar.
  - De uno a cuatro transceptores SFP28, si tiene previsto utilizar velocidad de enlace 25-GbE.
  - Cables Ethernet para conectar los puertos de gestión.

Riesgo de exposición a la radiación láser — no desmonte ni retire ninguna parte de un transceptor SFP. Puede que esté expuesto a la radiación láser.

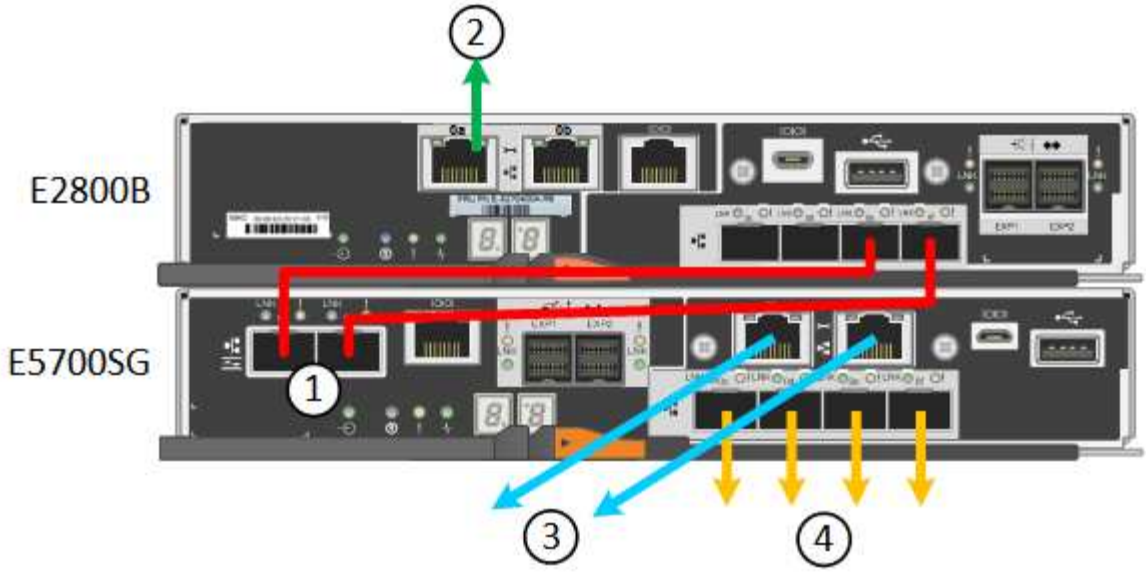
Acerca de esta tarea

Las figuras muestran las dos controladoras en SG5760 y SG5760X, con la controladora de almacenamiento de la serie E2800 en la parte superior y la controladora E5700SG en la parte inferior. En SG5712 y SG5712X, la controladora de almacenamiento de la serie E2800 se encuentra a la izquierda de la controladora E5700SG cuando se ve desde la parte posterior.

Conexiones SG5760



Conexiones SG5760X



	Puerto	Tipo de puerto	Función
1	Dos puertos de interconexión en cada controladora	SFP+ óptico FC de 16 GB/s	Conecte las dos controladoras entre sí.
2	Puerto de gestión 1 en la controladora serie E2800	1 GbE (RJ-45).	Se conecta a la red en la que se accede a System Manager de SANtricity. Es posible usar la red administrativa para StorageGRID o una red de gestión independiente.
2	Puerto de gestión 2 en la controladora serie E2800	1 GbE (RJ-45).	Reservado para soporte técnico.
3	Puerto de gestión 1 en la controladora E5700SG	1 GbE (RJ-45).	Conecta la controladora E5700SG a la red de administración para StorageGRID.

	Puerto	Tipo de puerto	Función
3	Puerto de gestión 2 en la controladora E5700SG	1 GbE (RJ-45).	• Se puede unir al puerto de administración 1 si desea una conexión redundante a la red de administración. • Puede dejarse sin cables y disponible para acceso local temporal (IP 169.254.0.1). • Durante la instalación, se puede utilizar para conectar la controladora E5700SG a un portátil de servicio si las direcciones IP asignadas por DHCP no están disponibles.
4	10 puertos 1-4 de 25 GbE en la controladora E5700SG	10-GbE o 25-GbE **Nota:** los transceptores SFP+ incluidos con el dispositivo admiten velocidades de enlace de 10 GbE. Si desea utilizar velocidades de enlace de 25-GbE para los cuatro puertos de red, debe proporcionar transceptores SFP28.	Conéctese a la red de red y a la red de cliente para StorageGRID. Consulte «'conexiones de puertos 10/25-GbE para el controlador E5700SG'».

Pasos

1. Conecte la controladora E2800 a la controladora E5700SG, utilizando dos cables ópticos y cuatro de los ocho transceptores SFP+.

Conectar este puerto…	A este puerto…
Puerto 1 de interconexión en la controladora E2800	Puerto de interconexión 1 en el controlador E5700SG
Puerto 2 de interconexión en la controladora E2800	Puerto de interconexión 2 en el controlador E5700SG

2. Si tiene pensado utilizar System Manager de SANtricity, conecte el puerto de gestión 1 (P1 en el E2800A y 0a en el E2800B) en la controladora E2800 (el puerto RJ-45 a la izquierda) a la red de gestión para SANtricity System Manager, mediante un cable Ethernet.

No utilice el puerto de gestión 2 (P2 en E2800A y 0b en E2800B) en la controladora E2800 (el puerto RJ-45 a la derecha). Este puerto está reservado para el soporte técnico.

3. Si tiene previsto utilizar la Red de administración para StorageGRID, conecte el puerto de administración 1 del controlador E5700SG (el puerto RJ-45 de la izquierda) a la Red de administración mediante un cable Ethernet.

   Si tiene pensado utilizar el modo de enlace de red de copia de seguridad activa para la red de administración, conecte el puerto de administración 2 en la controladora E5700SG (el puerto RJ-45 a la derecha) a la red de administración, utilizando un cable Ethernet.

4. Conecte los puertos 10/25-GbE de la controladora E5700SG a los switches de red correspondientes, mediante cables ópticos y transceptores SFP+ o SFP28.

   > Todos los puertos deben utilizar la misma velocidad de enlace. Instale transceptores SFP+ si tiene pensado utilizar velocidades de enlace 10-GbE. Instale transceptores SFP28 si tiene pensado utilizar velocidades de enlace 25-GbE.

   - Si piensa utilizar el modo de enlace de puerto fijo (predeterminado), conecte los puertos a la red de StorageGRID y a las redes de cliente, como se muestra en la tabla.

Puerto	Conecta a…
Puerto 1	Red de cliente (opcional)
Puerto 2	Red Grid
Puerto 3	Red de cliente (opcional)
Puerto 4	Red Grid

   - Si planea utilizar el modo de enlace de puerto agregado, conecte uno o varios puertos de red a uno o varios switches. Debe conectar al menos dos de los cuatro puertos para evitar tener un único punto de error. Si utiliza más de un switch para un único vínculo LACP, los switches deben ser compatibles con MLAG o equivalente.

Información relacionada

Acceda al instalador de dispositivos de StorageGRID

Modos de enlace de puerto para puertos de controladora E5700SG

Conectar los cables de alimentación y aplicar alimentación (SG5700)

Cuando encienda el dispositivo, ambos controladores se iniciarán.

Lo que necesitará

Ambos interruptores de alimentación del aparato deben estar apagados antes de conectar la alimentación.

> **Riesgo de descarga eléctrica** — antes de conectar los cables de alimentación, asegúrese de que los dos interruptores de alimentación del aparato están apagados.

Pasos

1. Confirme que los dos interruptores de alimentación del aparato están apagados.
2. Conecte los dos cables de alimentación al aparato.
3. Conecte los dos cables de alimentación a diferentes unidades de distribución de alimentación (PDU) en el armario o rack.
4. Encienda los dos interruptores de alimentación del aparato.
   - No apague los interruptores de alimentación durante el proceso de encendido.
   - Los ventiladores son muy ruidosos cuando se ponen en marcha por primera vez. El ruido fuerte durante el arranque es normal.
5. Una vez arrancados las controladoras, compruebe sus pantallas de siete segmentos.

Ver los códigos de estado de arranque SG5700

Las pantallas de siete segmentos de cada controlador muestran el estado y los códigos de error a medida que el dispositivo se enciende.

Acerca de esta tarea

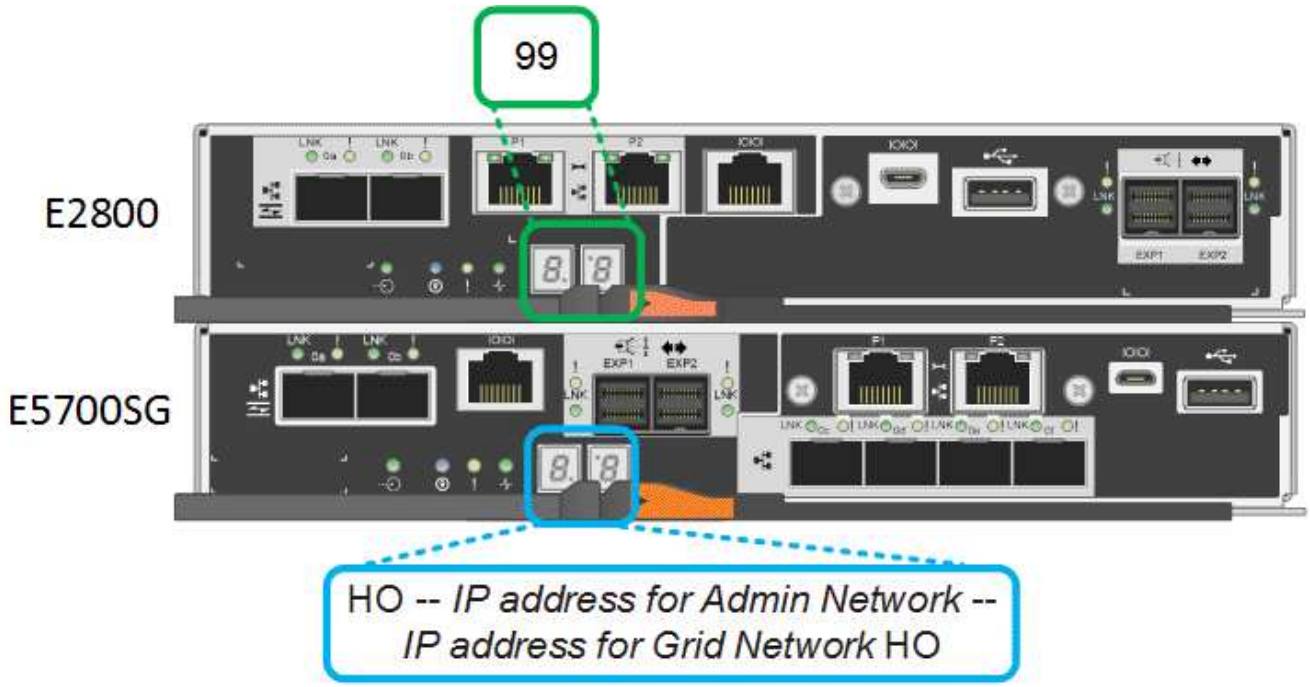
La controladora E2800 y la controladora E5700SG muestran diferentes Estados y códigos de error.

Para comprender qué significan estos códigos, consulte los siguientes recursos:

Controladora	Referencia
Controladora E2800	*E5700 y Guía de supervisión del sistema E2800* **Nota:** los códigos enumerados para el controlador E5700 E-Series no se aplican al controlador E5700SG del aparato.
Controladora E5700SG	"Indicadores de Estados en el controlador E5700SG"

Pasos

1. Durante el arranque, supervise el progreso visualizando los códigos que se muestran en las pantallas de siete segmentos.
   - La pantalla de siete segmentos del controlador E2800 muestra la secuencia de repetición **OS**, **SD**, ***blank*** para indicar que está realizando el procesamiento de comienzo del día.
   - La pantalla de siete segmentos del controlador E5700SG muestra una secuencia de códigos que termina con **AA** y **FF**.
2. Una vez arrancados las controladoras, confirme las pantallas de siete segmentos que muestran lo siguiente:



Controladora	Pantalla de siete segmentos
Controladora E2800	Muestra 99, que es el ID predeterminado de una bandeja de controladoras E-Series.
Controladora E5700SG	Muestra **HO**, seguido de una secuencia repetida de dos números. `HO -- IP address for Admin Network -- IP address for Grid Network HO` En la secuencia, el primer conjunto de números es la dirección IP asignada por DHCP para el puerto de gestión 1 de la controladora. Esta dirección se utiliza para conectar la controladora a la red del administrador para StorageGRID. El segundo conjunto de números es la dirección IP asignada por DHCP utilizada para conectar el dispositivo a la red de cuadrícula para StorageGRID. **Nota:** Si no se puede asignar una dirección IP mediante DHCP, se muestra 0.0.0.0.

3. Si las pantallas de siete segmentos muestran otros valores, consulte Solucionar problemas de instalación de hardware (SG5700) y confirme que ha completado los pasos de la instalación correctamente. Si no puede resolver el problema, póngase en contacto con el soporte técnico.

Información relacionada

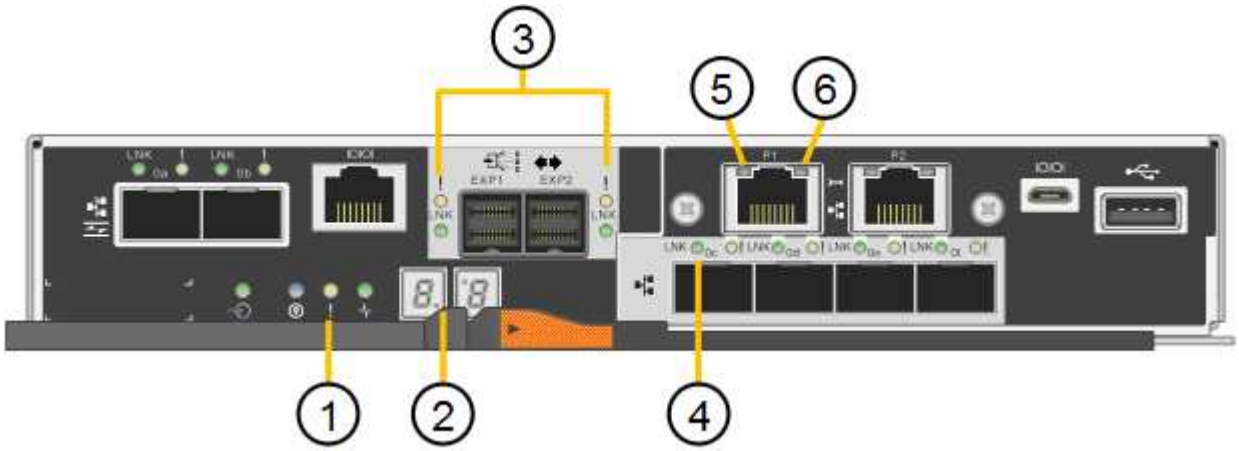
Indicadores de estado en el controlador E5700SG

"Guía de supervisión del sistema E5700 y E2800"

Indicadores de estado del controlador E5700SG

La pantalla de siete segmentos y los LED del controlador E5700SG muestran el estado y los códigos de error mientras el dispositivo se enciende y mientras el hardware se está inicializando. Estas pantallas se pueden utilizar para determinar el estado y la solución de errores.

Una vez iniciado el instalador de dispositivos StorageGRID, es necesario revisar periódicamente los indicadores de estado de la controladora E5700SG.



	Mostrar	Descripción
1	LED de atención	Ámbar: El controlador está defectuoso y requiere atención del operador, o no se ha encontrado la secuencia de comandos de instalación. OFF: La controladora funciona con normalidad.
2	Pantalla de siete segmentos	Muestra un código de diagnóstico Las secuencias de visualización de siete segmentos le permiten comprender los errores y el estado de funcionamiento del dispositivo.
3	Indicadores LED de atención del puerto de expansión	Ámbar: Estos LED siempre son ámbar (no se ha establecido ningún enlace) porque el aparato no utiliza los puertos de expansión.

	Mostrar	Descripción
4	Indicadores LED de estado del enlace de puerto de host	Verde: El enlace está activo. Desactivado: El enlace está inactivo.
5	LED de estado de conexión Ethernet	Verde: Se ha establecido un enlace. Desactivado: No se ha establecido ningún enlace.
6	Indicadores LED de actividad Ethernet	Verde: El enlace entre el puerto de gestión y el dispositivo al que está conectado (como un switch Ethernet) está activo. Desactivado: No hay ningún enlace entre la controladora y el dispositivo conectado. Verde parpadeante: Hay actividad Ethernet.

códigos generales de arranque

Durante el arranque o después de un reinicio duro del aparato, ocurre lo siguiente:

1. La visualización de siete segmentos en el controlador E5700SG muestra una secuencia general de códigos que no es específica para la controladora. La secuencia general termina con los códigos AA y FF.
2. Aparecen códigos de arranque específicos del controlador E5700SG.

códigos de arranque del controlador E5700SG

Durante un arranque normal del dispositivo, la pantalla de siete segmentos del controlador E5700SG muestra los siguientes códigos en el orden indicado:

Codificación	Lo que indica
HOLA	Se ha iniciado la secuencia de comandos de inicio maestra.
PP	El sistema comprueba si es necesario actualizar la FPGA.
HP	El sistema comprueba si el firmware de la controladora de 10/25-GbE debe actualizarse.

Codificación	Lo que indica
RB	El sistema se reinicia después de aplicar las actualizaciones de firmware.
P F	Se completaron las comprobaciones de actualización del firmware del subsistema de hardware. Se están iniciando los servicios de comunicación entre controladoras.
ÉL	El sistema está esperando conectividad con la controladora E2800 y sincronizando con el sistema operativo SANtricity. **Nota:** Si este procedimiento de arranque no avanza más allá de esta fase, compruebe las conexiones entre los dos controladores.
HC	El sistema comprueba si hay datos de instalación de StorageGRID existentes.
HO	El instalador de dispositivos de StorageGRID se está ejecutando.
HA	StorageGRID está ejecutando.

códigos de error de la controladora E5700SG

Estos códigos representan condiciones de error que pueden mostrarse en el controlador E5700SG a medida que el dispositivo se arranca. se muestran códigos hexadecimales adicionales de dos dígitos si se producen errores específicos de hardware de bajo nivel. Si alguno de estos códigos persiste durante más de un segundo o dos, o si no puede resolver el error siguiendo uno de los procedimientos de solución de problemas prescritos, póngase en contacto con el soporte técnico.

Codificación	Lo que indica
22	No se ha encontrado ningún registro de arranque maestro en ningún dispositivo de arranque.
23	El disco flash interno no está conectado.
2A, 2B	Bus atascado, no se pueden leer los datos del SPD del DIMM.
40	DIMM no válidos.
41	DIMM no válidos.
42	Error en la prueba de memoria.

Codificación	Lo que indica
51	Fallo de lectura del SPD.
92 a 96	Inicialización del bus PCI.
A0 a A3	Inicialización de la unidad SATA.
AB	Código de inicio alternativo.
AE	So de arranque.
EA	El entrenamiento de DDR4 falló.
E8	No hay memoria instalada.
UE	No se ha encontrado la secuencia de comandos de instalación.
EP	Se produjo un error en la instalación o la comunicación con la controladora E2800.

Información relacionada

Solucionar problemas de instalación de hardware (SG5700)

"Soporte de NetApp"

Configurar hardware (SG5700)

Tras aplicar la alimentación al dispositivo, debe configurar System Manager de SANtricity, que es el software que utilizará para supervisar el hardware. También debe configurar las conexiones de red que utilizará StorageGRID.

Configurar conexiones StorageGRID (SG5700)

Para poder implementar un dispositivo StorageGRID como nodo de almacenamiento en un grid StorageGRID, debe configurar las conexiones entre el dispositivo y las redes que tiene pensado utilizar. Puede configurar las redes examinando el instalador de dispositivos StorageGRID, que está incluido en la controladora E5700SG (la controladora de computación del dispositivo).

Pasos

- Acceda al instalador de dispositivos de StorageGRID
- Comprobar y actualizar la versión de StorageGRID Appliance Installer
- Configurar enlaces de red (SG5700)
- Establezca la configuración de IP

- Compruebe las conexiones de red
- Verifique las conexiones de red a nivel de puerto

Acceda al instalador de dispositivos de StorageGRID

Debe acceder al instalador de dispositivos de StorageGRID para configurar las conexiones entre el dispositivo y las tres redes StorageGRID: La red de grid, la red de administrador (opcional) y la red de cliente (opcional).

Lo que necesitará

- Está utilizando un navegador web compatible.
- El dispositivo está conectado a todas las redes StorageGRID que tiene previsto utilizar.
- Conoce la dirección IP, la puerta de enlace y la subred del dispositivo en estas redes.
- Configuró los switches de red que planea utilizar.

Acerca de esta tarea

Cuando acceda por primera vez al instalador de dispositivos de StorageGRID, puede utilizar la dirección IP asignada por DHCP para la red de administración (suponiendo que el dispositivo esté conectado a la red de administración) o la dirección IP asignada por DHCP para la red de grid. Se recomienda usar la dirección IP para la red de administración. De lo contrario, si accede al instalador de dispositivos de StorageGRID con la dirección DHCP de la red de grid, puede perder la conexión con el instalador de dispositivos de StorageGRID al cambiar la configuración de los enlaces y al introducir una IP estática.

Pasos

1. Obtenga la dirección DHCP del dispositivo en la red de administración (si está conectada) o en la red de red (si la red de administración no está conectada).

   Puede realizar una de las siguientes acciones:

   - Observe la pantalla de siete segmentos en la controladora E5700SG. Si los puertos 1 y 10/25-GbE 2 y 4 de la controladora E5700SG están conectados a redes con servidores DHCP, la controladora intenta obtener direcciones IP asignadas de forma dinámica cuando se enciende en el compartimento. Una vez que el controlador ha completado el proceso de encendido, su pantalla de siete segmentos muestra **HO**, seguido de una secuencia repetida de dos números.

     ```
     HO -- IP address for Admin Network -- IP address for Grid Network HO
     ```

     En la secuencia:

     - El primer conjunto de números es la dirección DHCP para el nodo de almacenamiento del dispositivo en la red de administración, si está conectado. Esta dirección IP se asigna al puerto de gestión 1 en la controladora E5700SG.
     - El segundo conjunto de números es la dirección DHCP del nodo de almacenamiento del dispositivo en la red de grid. Esta dirección IP se asigna a los puertos 10/25-GbE 2 y 4 cuando se enciende por primera vez el aparato.

       Si no se pudo asignar una dirección IP con DHCP, se muestra 0.0.0.0.

   - Proporcione la dirección MAC para el puerto de gestión 1 al administrador de red, para que puedan

buscar la dirección DHCP para este puerto en la red de administración. La dirección MAC está impresa en una etiqueta del controlador E5700SG, junto al puerto.

2. Si pudo obtener alguna de las direcciones DHCP:

   a. Abra un explorador Web en el portátil de servicios.

   b. Introduzca esta URL para el instalador del dispositivo StorageGRID:
   https://*E5700SG_Controller_IP*:8443

   Para *E5700SG_Controller_IP*, Utilice la dirección DHCP del controlador (utilice la dirección IP de la red de administración si la tiene).

   c. Si se le solicita una alerta de seguridad, vea e instale el certificado con el asistente de instalación del explorador.

   La alerta no aparecerá la próxima vez que acceda a esta URL.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID. La información y los mensajes que se muestran cuando accede por primera vez a esta página dependen de cómo el dispositivo está conectado actualmente a redes StorageGRID. Pueden aparecer mensajes de error que se resolverán en pasos posteriores.

NetApp® StorageGRID® Appliance Installer

Home | Configure Networking | Configure Hardware | Monitor Installation | Advanced

Home

The installation is ready to be started. Review the settings below, and then click Start Installation.

This Node

Node type: Storage

Node name: MM-2-108-SGA-lab25

Cancel Save

Primary Admin Node connection

Enable Admin Node discovery: ☐

Primary Admin Node IP: 172.16.1.178

Connection state: Connection to 172.16.1.178 ready

Cancel Save

Installation

Current state: Ready to start installation of MM-2-108-SGA-lab25 into grid with Admin Node 172.16.1.178 running StorageGRID 11.2.0, using StorageGRID software downloaded from the Admin Node.

Start Installation

3. Si la controladora E5700SG no pudo adquirir una dirección IP mediante DHCP:

   a. Conecte el portátil de servicio al puerto de gestión 2 de la controladora E5700SG mediante un cable Ethernet.

b. Abra un explorador Web en el portátil de servicios.

c. Introduzca esta URL para el instalador del dispositivo StorageGRID:
`https://169.254.0.1:8443`

Aparece la página de inicio del instalador de dispositivos de StorageGRID. La información y los mensajes que se muestran al acceder por primera vez a esta página dependen de cómo esté conectado el dispositivo actualmente.

> Si no puede acceder a la página de inicio a través de una conexión local de enlace, configure la dirección IP del portátil de servicio como `169.254.0.2`y vuelva a intentarlo.

4. Revise los mensajes que se muestran en la página Inicio y configure la configuración del vínculo y la configuración IP, según sea necesario.

Información relacionada

Requisitos del navegador web

Comprobar y actualizar la versión de StorageGRID Appliance Installer

La versión de instalador del dispositivo StorageGRID en el dispositivo debe coincidir con la versión de software instalada en el sistema StorageGRID para garantizar que todas las funciones de StorageGRID sean compatibles.

Lo que necesitará

Ha accedido al instalador de dispositivos de StorageGRID.

Acerca de esta tarea

Los dispositivos StorageGRID vienen de fábrica preinstalados con el instalador de dispositivos StorageGRID. Si va a añadir un dispositivo a un sistema StorageGRID actualizado recientemente, es posible que deba actualizar manualmente el instalador de dispositivos StorageGRID antes de instalar el dispositivo como un nodo nuevo.

El instalador de dispositivos de StorageGRID se actualiza automáticamente cuando se actualiza a una nueva versión de StorageGRID. No es necesario actualizar el instalador de dispositivos StorageGRID en los nodos del dispositivo instalados. Este procedimiento sólo es necesario cuando se instala un dispositivo que contiene una versión anterior del instalador de dispositivos de StorageGRID.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Actualizar firmware**.
2. Compare la versión actual del firmware con la versión de software instalada en el sistema StorageGRID. (En la parte superior de Grid Manager, seleccione el icono de ayuda y seleccione **Acerca de**).

   El segundo dígito de las dos versiones debe coincidir. Por ejemplo, si el sistema StorageGRID está ejecutando la versión 11.**6**.*x*.*y*, la versión del instalador de dispositivos StorageGRID debe ser 3.**6**.*z*.

3. Si el dispositivo tiene una versión de nivel inferior del instalador de dispositivos de StorageGRID, vaya a. "Descargas de NetApp: Dispositivo de StorageGRID".

   Inicie sesión con el nombre de usuario y la contraseña de su cuenta de NetApp.

4. Descargue la versión adecuada del archivo **Soporte para dispositivos StorageGRID** y el archivo de suma de comprobación correspondiente.

El archivo de soporte para dispositivos StorageGRID es un `.zip` archivo que contiene las versiones de firmware actuales y anteriores para todos los modelos de dispositivos StorageGRID, en subdirectorios para cada tipo de controlador.

Después de descargar el archivo de soporte para dispositivos StorageGRID, extraiga el `.zip` archive y consulte el archivo README para obtener información importante sobre la instalación del instalador de dispositivos StorageGRID.

5. Siga las instrucciones de la página actualización del firmware del instalador del dispositivo StorageGRID para realizar estos pasos:
   a. Cargue el archivo de soporte (imagen de firmware) apropiado para el tipo de controladora y el archivo de suma de comprobación.
   b. Actualice la partición inactiva.
   c. Reiniciar e intercambiar particiones.
   d. Actualice la segunda partición (inactiva).

Información relacionada

Acceda al instalador de dispositivos de StorageGRID

Configurar enlaces de red (SG5700)

Puede configurar los enlaces de red para los puertos utilizados para conectar el dispositivo a la red de grid, la red de cliente y la red de administración. Puede establecer la velocidad de enlace, así como los modos de enlace de red y puerto.

Lo que necesitará

Si tiene pensado utilizar la velocidad de enlace de 25-GbE para los puertos de 10/25-GbE:

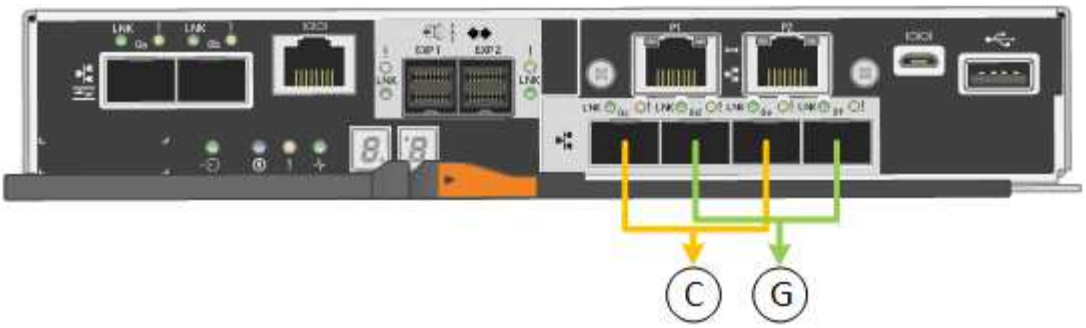
- Ha instalado transceptores SFP28 en los puertos que tiene previsto utilizar.
- Ya ha conectado los puertos a switches que admiten estas funciones.
- Comprende cómo configurar los switches para que utilicen esta mayor velocidad.

Si planea utilizar el modo de enlace de puerto agregado, el modo de enlace de red LACP o el etiquetado de VLAN para los puertos 10/25-GbE:

- Conectó los puertos del dispositivo a los switches que pueden ser compatibles con VLAN y LACP.
- Si varios switches participan en el enlace LACP, los switches admiten grupos de agregación de enlaces de varios chasis (MLAG) o equivalente.
- Comprende cómo configurar los switches para que utilicen VLAN, LACP y MLAG o equivalente.
- Conoce la etiqueta de VLAN única que se utilizará para cada red. Esta etiqueta VLAN se añadirá a cada paquete de red para garantizar que el tráfico de red se dirija a la red correcta.
- Si planea utilizar el modo Active-Backup para la red administrativa, habrá conectados cables Ethernet a ambos puertos de gestión de la controladora.

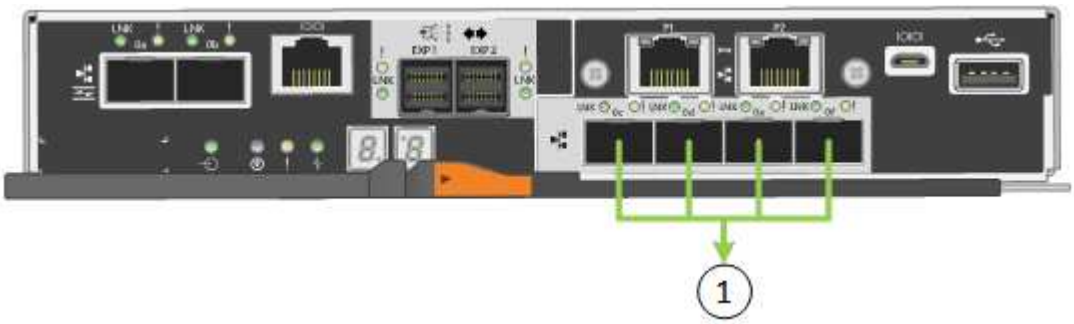
Acerca de esta tarea

Esta figura muestra cómo los cuatro puertos 10/25-GbE se bonifican en modo de enlace de puerto fijo (configuración predeterminada).



Llamada	Qué puertos están Unidos
C	Los puertos 1 y 3 se unen para la red cliente, si se utiliza esta red.
G	Los puertos 2 y 4 están Unidos para la red de cuadrícula.

Esta figura muestra cómo los cuatro puertos 10/25-GbE están Unidos en modo de enlace de puerto agregado.



Llamada	Qué puertos están Unidos
1	Los cuatro puertos se agrupan en un enlace LACP único, lo que permite que se usen todos los puertos para el tráfico de red de grid y de red de cliente.

La tabla resume las opciones para configurar los cuatro puertos 10/25-GbE. La configuración predeterminada se muestra en negrita. Sólo tiene que configurar los ajustes en la página Configuración de vínculos si desea utilizar un valor no predeterminado.

- **Modo de enlace de puerto fijo (predeterminado)**

Modo de enlace de red	Red de cliente desactivada (predeterminada)	Red de cliente habilitada
Active-Backup (predeterminado)	• Los puertos 2 y 4 utilizan un vínculo de copia de seguridad activa para la red Grid. • Los puertos 1 y 3 no se usan. • Una etiqueta de VLAN es opcional.	• Los puertos 2 y 4 utilizan un vínculo de copia de seguridad activa para la red Grid. • Los puertos 1 y 3 utilizan un vínculo de backup activo para la red cliente. • Es posible especificar etiquetas de VLAN para ambas redes.
LACP (802.3ad)	• Los puertos 2 y 4 utilizan un enlace LACP para la red de grid. • Los puertos 1 y 3 no se usan. • Una etiqueta de VLAN es opcional.	• Los puertos 2 y 4 utilizan un enlace LACP para la red de grid. • Los puertos 1 y 3 utilizan un enlace LACP para la red de cliente. • Es posible especificar etiquetas de VLAN para ambas redes.

- **Modo de enlace de puerto agregado**

Modo de enlace de red	Red de cliente desactivada (predeterminada)	Red de cliente habilitada
Solo LACP (802.3ad)	• Los puertos 1-4 utilizan un enlace LACP único para la red de grid. • Una única etiqueta VLAN identifica los paquetes de red Grid.	• Los puertos 1-4 utilizan un enlace LACP único para la red de grid y la red de cliente. • Dos etiquetas VLAN permiten que los paquetes de red de cuadrícula se separen de los paquetes de red de cliente.

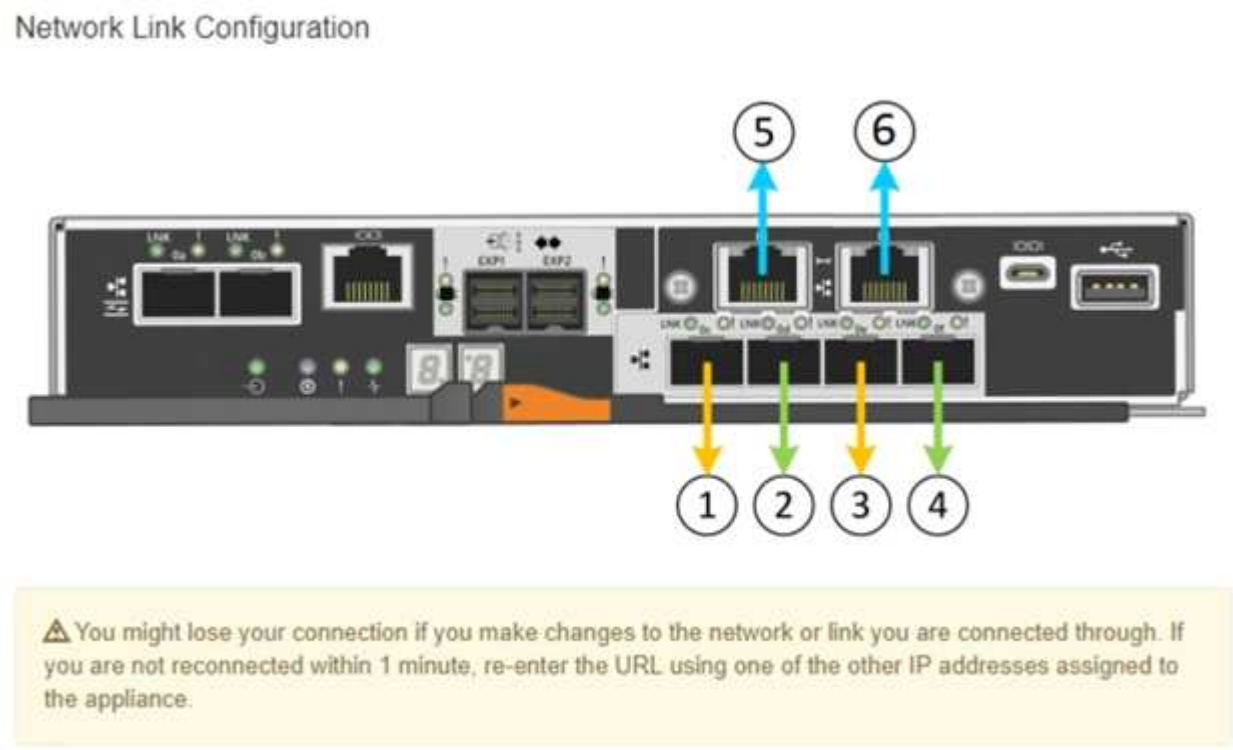
Consulte la información acerca de las conexiones de puertos 10/25-GbE para la controladora E5700SG para obtener más información acerca de los modos de enlace de puerto y enlace de red.

En esta figura, se muestra cómo los dos puertos de gestión de 1-GbE de la controladora E5700SG están Unidos en el modo de enlace de red Active-Backup para la red Admin.

Pasos

1. En la barra de menús del instalador del dispositivo StorageGRID, haga clic en **Configurar redes** > **Configuración de vínculo**.

   La página Network Link Configuration muestra un diagrama del dispositivo con los puertos de red y administración numerados.



   La tabla Estado del enlace muestra el estado de los vínculos (arriba/abajo) y la velocidad (1/10/25/40/100 Gbps) de los puertos numerados.

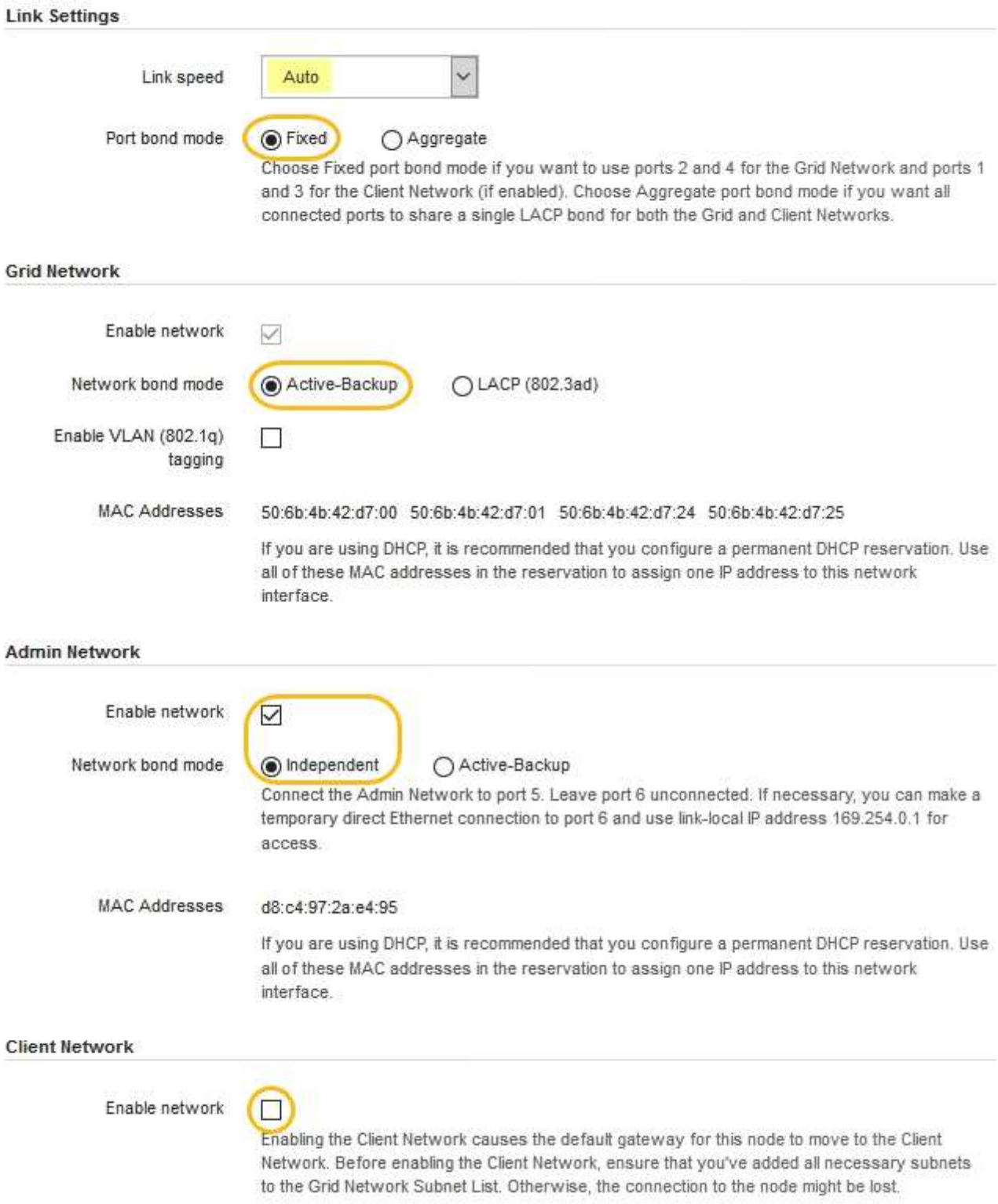
Link Status

Link	State	Speed (Gbps)
1	Up	25
2	Up	25
3	Up	25
4	Up	25
5	Up	1
6	Up	1

   La primera vez que acceda a esta página:

   - **Velocidad de enlace** se ajusta a **10 GbE**.

- **El modo de enlace de puerto** está establecido en **fijo**.
- **El modo de enlace de red** para la red Grid se establece en **Active-Backup**.
- La **Red de administración** está activada y el modo de enlace de red se establece en **independiente**.
- La **Red cliente** está desactivada.



2. Si planea utilizar la velocidad de enlace de 25 GbE para los puertos de 10/25 GbE, seleccione **25GbE** en la lista desplegable velocidad de enlace.

Los switches de red que utiliza para la red de cuadrícula y la red de cliente también deben ser compatibles y configurados para esta velocidad. Los transceptores SFP28 deben estar instalados en los puertos.

3. Habilite o deshabilite las redes StorageGRID que tiene previsto utilizar.

   Se requiere la red de red. No se puede deshabilitar esta red.

   a. Si el dispositivo no está conectado a la red de administración, anule la selección de la casilla de verificación **Activar red** para la red de administración.

      Admin Network

      Enable network ☐

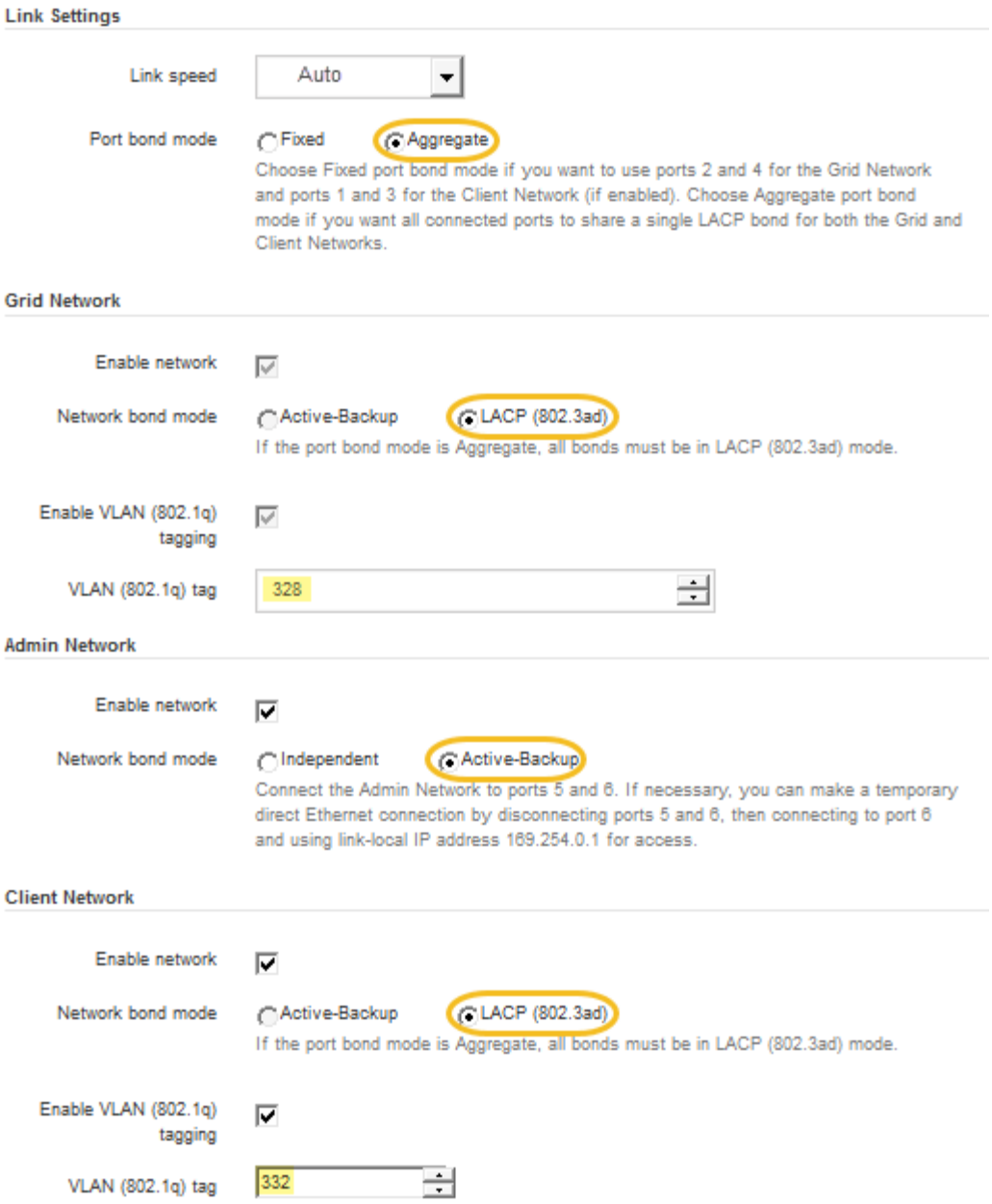
   b. Si el dispositivo está conectado a la red cliente, seleccione la casilla de verificación **Activar red** de la red cliente.

      Ahora se muestran los ajustes de red de clientes para los puertos de 10/25-GbE.

4. Consulte la tabla y configure el modo de enlace de puerto y el modo de enlace de red.

   El ejemplo muestra:

   - **Agregado** y **LACP** seleccionados para las redes Grid y Client. Debe especificar una etiqueta de VLAN exclusiva para cada red. Puede seleccionar valores entre 0 y 4095.
   - **Active-Backup** seleccionado para la red de administración.



5. Cuando esté satisfecho con sus selecciones, haga clic en **Guardar**.

> Puede perder la conexión si ha realizado cambios en la red o el enlace que está conectado a través de. Si no vuelve a conectarse en un minuto, vuelva a introducir la URL del instalador de dispositivos StorageGRID utilizando una de las otras direcciones IP asignadas al dispositivo:
> **`https://E5700SG_Controller_IP:8443`**

Información relacionada

Modos de enlace de puerto para puertos de controladora E5700SG

Establezca la configuración de IP

El instalador de dispositivos StorageGRID se utiliza para configurar las direcciones IP y la información de enrutamiento utilizadas para el nodo de almacenamiento del dispositivo

en las redes de cliente, administrador y grid de StorageGRID.

Acerca de esta tarea

Debe asignar una IP estática al dispositivo en cada red conectada o asignar una concesión permanente a la dirección del servidor DHCP.

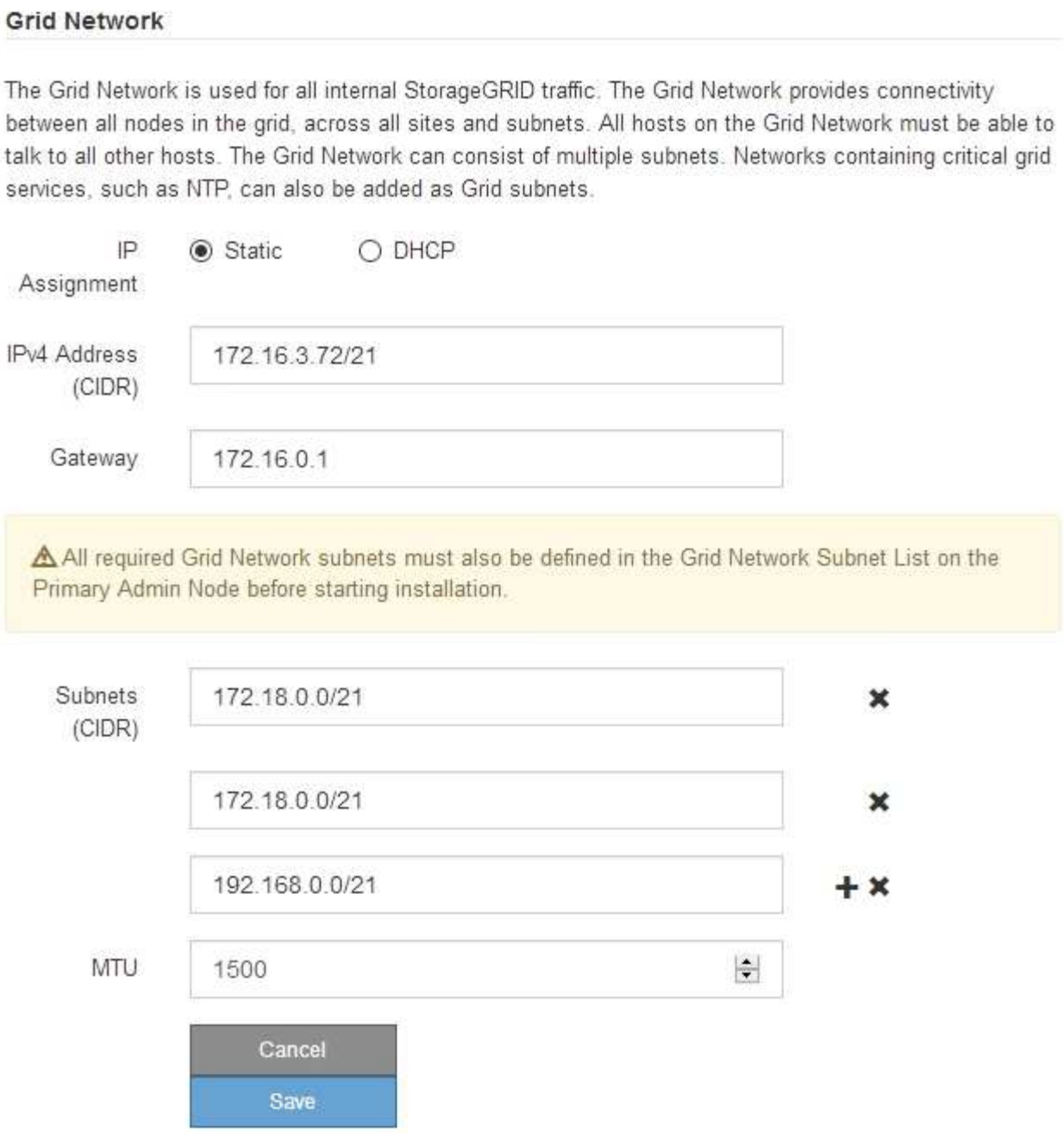
Si desea cambiar la configuración del enlace, consulte las instrucciones para cambiar la configuración del enlace de la controladora E5700SG.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Configurar redes** > **Configuración IP**.

   Aparece la página Configuración de IP.

2. Para configurar Grid Network, seleccione **Static** o **DHCP** en la sección **Grid Network** de la página.



3. Si ha seleccionado **estático**, siga estos pasos para configurar la red de cuadrícula:
   a. Introduzca la dirección IPv4 estática utilizando la notación CIDR.
   b. Introduzca la puerta de enlace.

      Si la red no tiene una puerta de enlace, vuelva a introducir la misma dirección IPv4 estática.

   c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

      > 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. Los valores de MTU no tienen que ser iguales para todos los tipos de red.

d. Haga clic en **Guardar**.

   Al cambiar la dirección IP, la pasarela y la lista de subredes también pueden cambiar.

   Si pierde la conexión con el instalador de dispositivos StorageGRID, vuelva a introducir la URL con la nueva dirección IP estática que acaba de asignar. Por ejemplo, **`https://services_appliance_IP:8443`**

e. Confirme que la lista de subredes de red es correcta.

   Si tiene 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. Estas subredes de red de cuadrícula también deben definirse en la Lista de subredes de red de cuadrícula del nodo de administración principal al iniciar la instalación de StorageGRID.

   > La ruta predeterminada no aparece en la lista. Si la red de cliente no está activada, la ruta predeterminada utilizará la puerta de enlace de red de cuadrícula.

   - Para agregar una subred, haga clic en el icono de inserción ➕ a la derecha de la última entrada.
   - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

f. Haga clic en **Guardar**.

4. Si ha seleccionado **DHCP**, siga estos pasos para configurar Grid Network:

a. Después de seleccionar el botón de opción **DHCP**, haga clic en **Guardar**.

   Los campos **Dirección IPv4**, **Puerta de enlace** y **subredes** se rellenan automáticamente. Si el servidor DHCP está configurado para asignar un valor MTU, el campo **MTU** se rellena con ese valor y el campo pasa a ser de sólo lectura.

   El navegador web se redirige automáticamente a la nueva dirección IP para el instalador de dispositivos StorageGRID.

b. Confirme que la lista de subredes de red es correcta.

   Si tiene 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. Estas subredes de red de cuadrícula también deben definirse en la Lista de subredes de red de cuadrícula del nodo de administración principal al iniciar la instalación de StorageGRID.

   > La ruta predeterminada no aparece en la lista. Si la red de cliente no está activada, la ruta predeterminada utilizará la puerta de enlace de red de cuadrícula.

   - Para agregar una subred, haga clic en el icono de inserción ➕ a la derecha de la última entrada.
   - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes,

como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

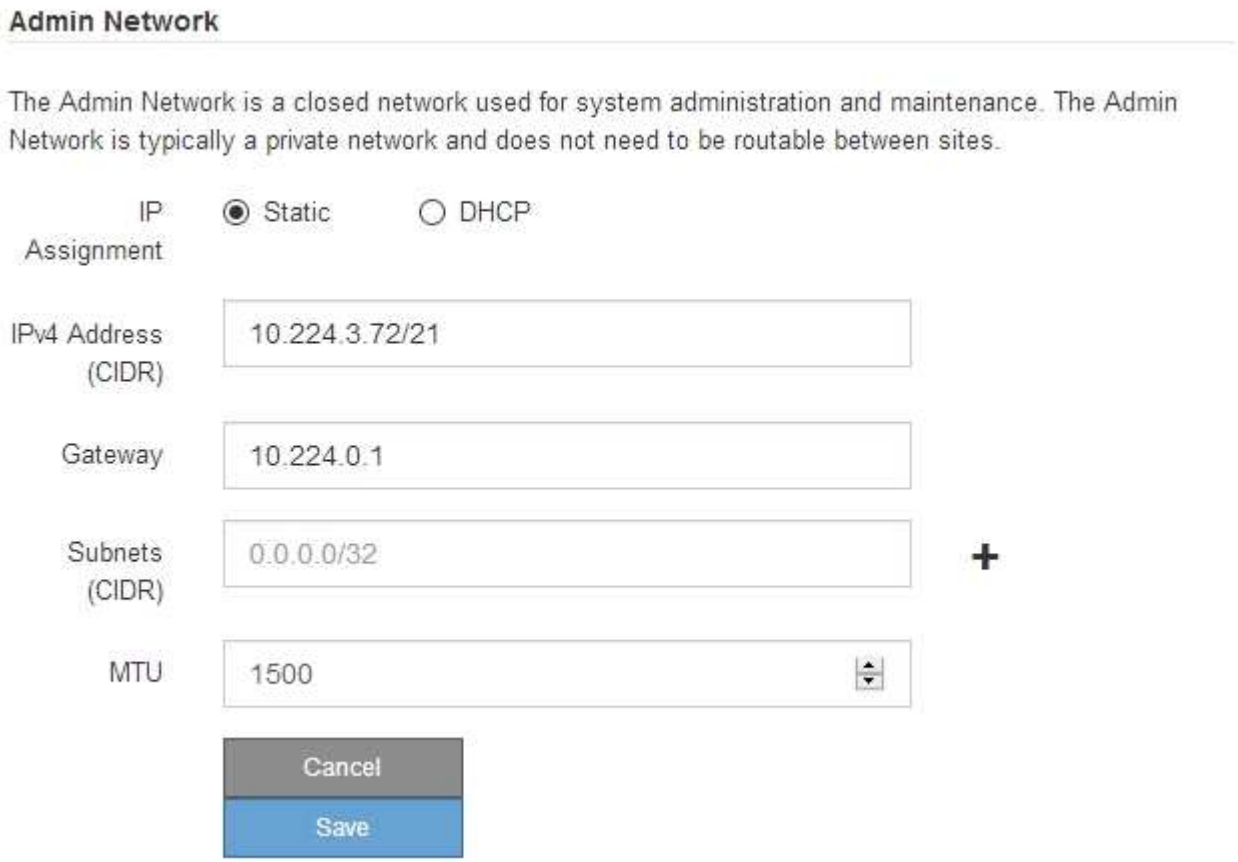
> El valor de MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, pueden ocurrir problemas de rendimiento de red o pérdida de paquetes.

> 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. Los valores de MTU no tienen que ser iguales para todos los tipos de red.

a. Haga clic en **Guardar**.

5. Para configurar la Red de administración, seleccione **estático** o **DHCP** en la sección Red de administración de la página.

> Para configurar la Red de administración, debe activar la Red de administración en la página Configuración de vínculos.



6. Si ha seleccionado **estático**, siga estos pasos para configurar la red de administración:

   a. Introduzca la dirección IPv4 estática, mediante la notación CIDR, para el puerto de gestión 1 del dispositivo.

      El puerto de gestión 1 está a la izquierda de los dos puertos RJ45 de 1-GbE del extremo derecho del dispositivo.

b. Introduzca la puerta de enlace.

   Si la red no tiene una puerta de enlace, vuelva a introducir la misma dirección IPv4 estática.

c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

   > 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.

d. Haga clic en **Guardar**.

   Al cambiar la dirección IP, la pasarela y la lista de subredes también pueden cambiar.

   Si pierde la conexión con el instalador de dispositivos StorageGRID, vuelva a introducir la URL con la nueva dirección IP estática que acaba de asignar. Por ejemplo, `https://services_appliance:8443`

e. Confirme que la lista de subredes de la red administrativa es correcta.

   Debe verificar que se pueda acceder a todas las subredes mediante la puerta de enlace que ha proporcionado.

   > No se puede realizar la ruta predeterminada para utilizar la puerta de enlace de red de administración.

   - Para agregar una subred, haga clic en el icono de inserción + a la derecha de la última entrada.
   - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

f. Haga clic en **Guardar**.

7. Si ha seleccionado **DHCP**, siga estos pasos para configurar la red de administración:

   a. Después de seleccionar el botón de opción **DHCP**, haga clic en **Guardar**.

      Los campos **Dirección IPv4**, **Puerta de enlace** y **subredes** se rellenan automáticamente. Si el servidor DHCP está configurado para asignar un valor MTU, el campo **MTU** se rellena con ese valor y el campo pasa a ser de sólo lectura.

      El navegador web se redirige automáticamente a la nueva dirección IP para el instalador de dispositivos StorageGRID.

   b. Confirme que la lista de subredes de la red administrativa es correcta.

      Debe verificar que se pueda acceder a todas las subredes mediante la puerta de enlace que ha proporcionado.

      > No se puede realizar la ruta predeterminada para utilizar la puerta de enlace de red de administración.

      - Para agregar una subred, haga clic en el icono de inserción + a la derecha de la última entrada.
      - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

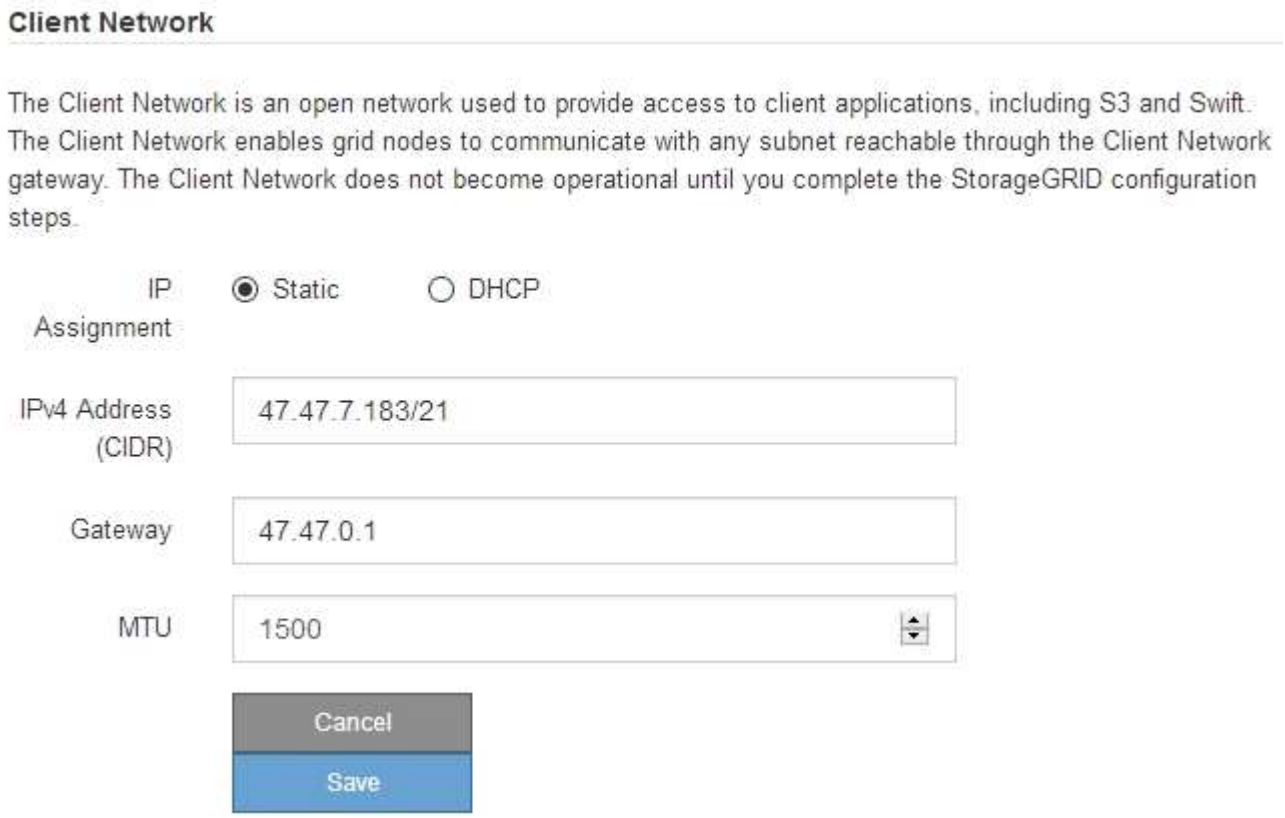
c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

> 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.

d. Haga clic en **Guardar**.

8. Para configurar la red de cliente, seleccione **Static** o **DHCP** en la sección **Client Network** de la página.

> Para configurar la red de cliente, debe activar la red de cliente en la página Configuración de vínculos.



9. Si ha seleccionado **estático**, siga estos pasos para configurar la red de cliente:

a. Introduzca la dirección IPv4 estática utilizando la notación CIDR.

b. Haga clic en **Guardar**.

c. Confirme que la dirección IP de la puerta de enlace de red de cliente es correcta.

> Si la red de cliente está activada, se muestra la ruta predeterminada. La ruta predeterminada utiliza la puerta de enlace de red de cliente y no se puede mover a otra interfaz mientras la red de cliente está activada.

d. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

> 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.

e. Haga clic en **Guardar**.

10. Si ha seleccionado **DHCP**, siga estos pasos para configurar la red de cliente:

    a. Después de seleccionar el botón de opción **DHCP**, haga clic en **Guardar**.

    Los campos **Dirección IPv4** y **Puerta de enlace** se rellenan automáticamente. Si el servidor DHCP está configurado para asignar un valor MTU, el campo **MTU** se rellena con ese valor y el campo pasa a ser de sólo lectura.

    El navegador web se redirige automáticamente a la nueva dirección IP para el instalador de dispositivos StorageGRID.

    a. Confirme que la puerta de enlace es correcta.

    > Si la red de cliente está activada, se muestra la ruta predeterminada. La ruta predeterminada utiliza la puerta de enlace de red de cliente y no se puede mover a otra interfaz mientras la red de cliente está activada.

    b. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

    > 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.

Información relacionada

Cambie la configuración del enlace de la controladora E5700SG

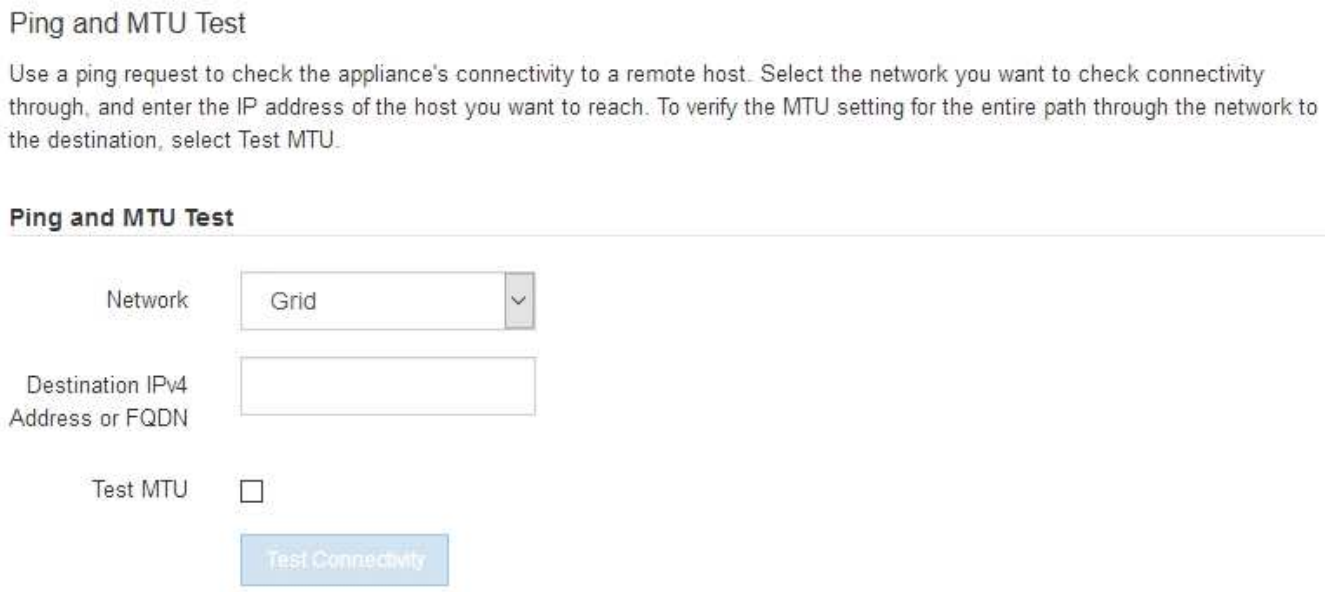
Compruebe las conexiones de red

Debe confirmar que puede acceder a las redes StorageGRID que está utilizando desde el dispositivo. Para validar el enrutamiento mediante puertas de enlace de red, debe probar la conectividad entre el instalador de dispositivos de StorageGRID y las direcciones IP en subredes diferentes. También puede verificar la configuración de MTU.

Pasos

1. En la barra de menús del instalador del dispositivo StorageGRID, haga clic en **Configurar redes** > **Ping y prueba de MTU**.

   Aparece la página pruebas de ping y MTU.



2. En el cuadro desplegable **Red**, seleccione la red que desea probar: Grid, Admin o Client.
3. Introduzca la dirección IPv4 o el nombre de dominio completo (FQDN) correspondiente a un host en esa red.

   Por ejemplo, puede hacer ping a la puerta de enlace de la red o al nodo de administración principal.

4. Opcionalmente, active la casilla de verificación **probar MTU** para comprobar la configuración de MTU para toda la ruta de acceso a través de la red hasta el destino.

   Por ejemplo, puede probar la ruta entre el nodo del dispositivo y un nodo en un sitio diferente.

5. Haga clic en **probar conectividad**.

   Si la conexión de red es válida, aparece el mensaje "Ping test pased", con la salida del comando ping en la lista.

Ping and MTU Test

Use a ping request to check the appliance's connectivity to a remote host. Select the network you want to check connectivity through, and enter the IP address of the host you want to reach. To verify the MTU setting for the entire path through the network to the destination, select Test MTU.

Ping and MTU Test

Network: Grid

Destination IPv4 Address or FQDN: 10.96.104.223

Test MTU: ☑

Test Connectivity

Ping test passed

Ping command output

```
PING 10.96.104.223 (10.96.104.223) 1472(1500) bytes of data.
1480 bytes from 10.96.104.223: icmp_seq=1 ttl=64 time=0.318 ms

--- 10.96.104.223 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.318/0.318/0.318/0.000 ms

Found MTU 1500 for 10.96.104.223 via br0
```

Información relacionada

Configurar enlaces de red (SG5700)

Cambie la configuración de MTU

Verifique las conexiones de red a nivel de puerto

Para garantizar que los firewalls no obstruyan el acceso entre el instalador del dispositivo StorageGRID y otros nodos, confirme que el instalador del dispositivo StorageGRID puede conectarse a un puerto TCP o a un conjunto de puertos en la dirección IP o el rango de direcciones especificados.

Acerca de esta tarea

Con la lista de puertos que se incluye en el instalador de dispositivos de StorageGRID, puede probar la conectividad entre el dispositivo y los demás nodos de la red de grid.

Además, puede probar la conectividad en las redes de administración y cliente y en los puertos UDP, como los que se utilizan para servidores NFS o DNS externos. Para obtener una lista de estos puertos, consulte la referencia de puertos en las directrices de red de StorageGRID.

Los puertos de red de red enumerados en la tabla de conectividad de puertos sólo son válidos para StorageGRID versión 11.6.0. Para verificar qué puertos son correctos para cada tipo de nodo, siempre debe consultar las directrices de red para su versión de StorageGRID.

Pasos

1. En el instalador del dispositivo StorageGRID, haga clic en **Configurar red** > **Prueba de conectividad de puerto (nmap)**.

   Aparece la página Prueba de conectividad de puerto.

   La tabla de conectividad de puertos enumera los tipos de nodos que requieren conectividad TCP en la red de cuadrícula. Para cada tipo de nodo, la tabla enumera los puertos de red de cuadrícula a los que el dispositivo debe acceder.

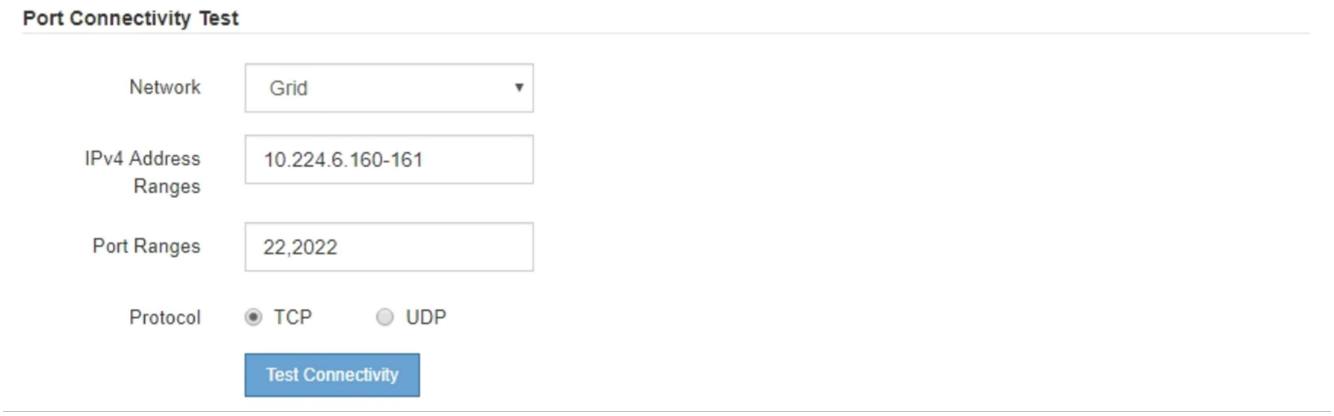
   Puede probar la conectividad entre los puertos del dispositivo que aparecen en la tabla y los demás nodos de la red de grid.

2. En el menú desplegable **Red**, seleccione la red que desea probar: **Grid**, **Admin** o **Cliente**.
3. Especifique un rango de direcciones IPv4 para los hosts en esa red.

   Por ejemplo, es posible que desee sondear la puerta de enlace en la red o en el nodo de administración principal.

   Especifique un rango utilizando un guión, como se muestra en el ejemplo.

4. Introduzca un número de puerto TCP, una lista de puertos separados por comas o un intervalo de puertos.



5. Haga clic en **probar conectividad**.

   - Si las conexiones de red a nivel de puerto seleccionadas son válidas, el mensaje "'Prueba de conectividad de puerto superada'" aparece en un banner verde. El resultado del comando nmap se muestra debajo del banner.

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- Si se realiza una conexión de red a nivel de puerto al host remoto, pero el host no escucha en uno o más de los puertos seleccionados, el mensaje "'error de prueba de conectividad de puerto'" aparece en un banner amarillo. El resultado del comando nmap se muestra debajo del banner.

  Cualquier puerto remoto al que no esté escuchando el host tiene un estado de "'cerrado'". Por ejemplo, puede ver este banner amarillo cuando el nodo al que intenta conectarse está en estado preinstalado y el servicio NMS de StorageGRID aún no se está ejecutando en ese nodo.

Port connectivity test failed
Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
1504/tcp closed evb-elm
1505/tcp open   funkproxy
1506/tcp open   utcd
1508/tcp open   diagmond
7443/tcp open   oracleas-https
9999/tcp open   abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- Si no se puede establecer una conexión de red a nivel de puerto para uno o más puertos seleccionados, el mensaje "'Port Connectivity test failed'" aparece en un banner rojo. El resultado del comando nmap se muestra debajo del banner.

  El banner rojo indica que se ha realizado un intento de conexión TCP a un puerto en el host remoto, pero no se ha devuelto nada al remitente. Cuando no se devuelve ninguna respuesta, el puerto tiene un estado de "filtrado" y es probable que sea bloqueado por un firewall.

  ⓘ También se enumeran los puertos con «'cerrado'».

Port connectivity test failed
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT     STATE    SERVICE
22/tcp   open     ssh
79/tcp   filtered finger
80/tcp   open     http
443/tcp  open     https
1504/tcp closed   evb-elm
1505/tcp open     funkproxy
1506/tcp open     utcd
1508/tcp open     diagmond
7443/tcp open     oracleas-https
9999/tcp open     abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

Información relacionada

Directrices sobre redes

Acceder y configurar System Manager de SANtricity (SG5700)

Puede usar System Manager de SANtricity para supervisar el estado de las controladoras de almacenamiento, los discos de almacenamiento y otros componentes de hardware en la bandeja de controladoras de almacenamiento. También puede configurar un proxy para AutoSupport E-Series que permite enviar mensajes de AutoSupport desde el dispositivo sin utilizar el puerto de gestión.

Configuración y acceso a System Manager de SANtricity

Es posible que tenga que acceder a System Manager de SANtricity en la controladora de almacenamiento para supervisar el hardware de la bandeja de controladoras de almacenamiento o configurar AutoSupport de E-Series.

Lo que necesitará

- Está utilizando un navegador web compatible.
- Para acceder a SANtricity System Manager a través de Grid Manager, debe tener instalado StorageGRID, y debe tener el permiso de administrador de dispositivo de almacenamiento o de acceso raíz.
- Para acceder a System Manager de SANtricity mediante el instalador de dispositivos de StorageGRID, debe tener el nombre de usuario y la contraseña de administrador de SANtricity System Manager.
- Para acceder a SANtricity System Manager directamente mediante un explorador web, debe tener el nombre de usuario y la contraseña de administrador de SANtricity System Manager.

> Debe tener el firmware 8.70 (11.70) de SANtricity o superior para acceder a System Manager de SANtricity mediante Grid Manager o el instalador de dispositivos de StorageGRID. Puede comprobar su versión de firmware mediante el instalador del dispositivo StorageGRID y seleccionando **Ayuda** > **Acerca de**.

> Acceder a SANtricity System Manager desde Grid Manager o desde el instalador de dispositivos generalmente se realiza solo para supervisar el hardware y configurar E-Series AutoSupport. Muchas funciones y operaciones en SANtricity System Manager, como la actualización de firmware, no se aplican a la supervisión del dispositivo StorageGRID. Para evitar problemas, siga siempre las instrucciones de instalación y mantenimiento del hardware del dispositivo.

Acerca de esta tarea

Existen tres formas de acceder a System Manager de SANtricity, en función de la fase del proceso de instalación y configuración en la que se encuentre:

- Si el dispositivo aún no se ha puesto en marcha como nodo en su sistema StorageGRID, debe usar la pestaña Avanzada del instalador de dispositivos de StorageGRID.

  > Una vez que el nodo se pone en marcha, ya no podrá utilizar el instalador de dispositivos de StorageGRID para acceder a System Manager de SANtricity.

- Si el dispositivo se ha implementado como nodo en el sistema StorageGRID, use la pestaña SANtricity System Manager de la página Nodes de Grid Manager.
- Si no puede utilizar el instalador de dispositivos de StorageGRID o Grid Manager, puede acceder a SANtricity System Manager directamente mediante un explorador web conectado al puerto de gestión.

Este procedimiento incluye los pasos para su acceso inicial a System Manager de SANtricity. Si ya ha configurado SANtricity System Manager, vaya a la Configure las alertas de hardware paso.

> Utilizar Grid Manager o el instalador de dispositivos de StorageGRID le permite acceder a SANtricity System Manager sin necesidad de configurar ni conectar el puerto de gestión del dispositivo.

Utilice System Manager de SANtricity para supervisar lo siguiente:

- Datos de rendimiento como el rendimiento en cabinas de almacenamiento, la latencia de I/o, el uso de CPU y el rendimiento
- Estado de los componentes de hardware
- Entre las funciones de soporte se incluyen la visualización de datos de diagnóstico

Puede usar System Manager de SANtricity para configurar las siguientes opciones:

- Alertas por correo electrónico, alertas SNMP o alertas de syslog para los componentes de la bandeja de controladoras de almacenamiento
- Configuración de AutoSupport de E-Series para los componentes de la bandeja de la controladora de almacenamiento.

  Para obtener más información sobre AutoSupport de E-Series, consulte el centro de documentación de E-Series.

  "Sitio de documentación para sistemas E-Series y EF-Series de NetApp"

- Claves Drive Security, que se necesitan para desbloquear unidades seguras (este paso es necesario si la función Drive Security está habilitada)
- Contraseña de administrador para acceder a System Manager de SANtricity

Pasos

1. Utilice el instalador del dispositivo StorageGRID y seleccione **Avanzado** > **Administrador del sistema SANtricity**

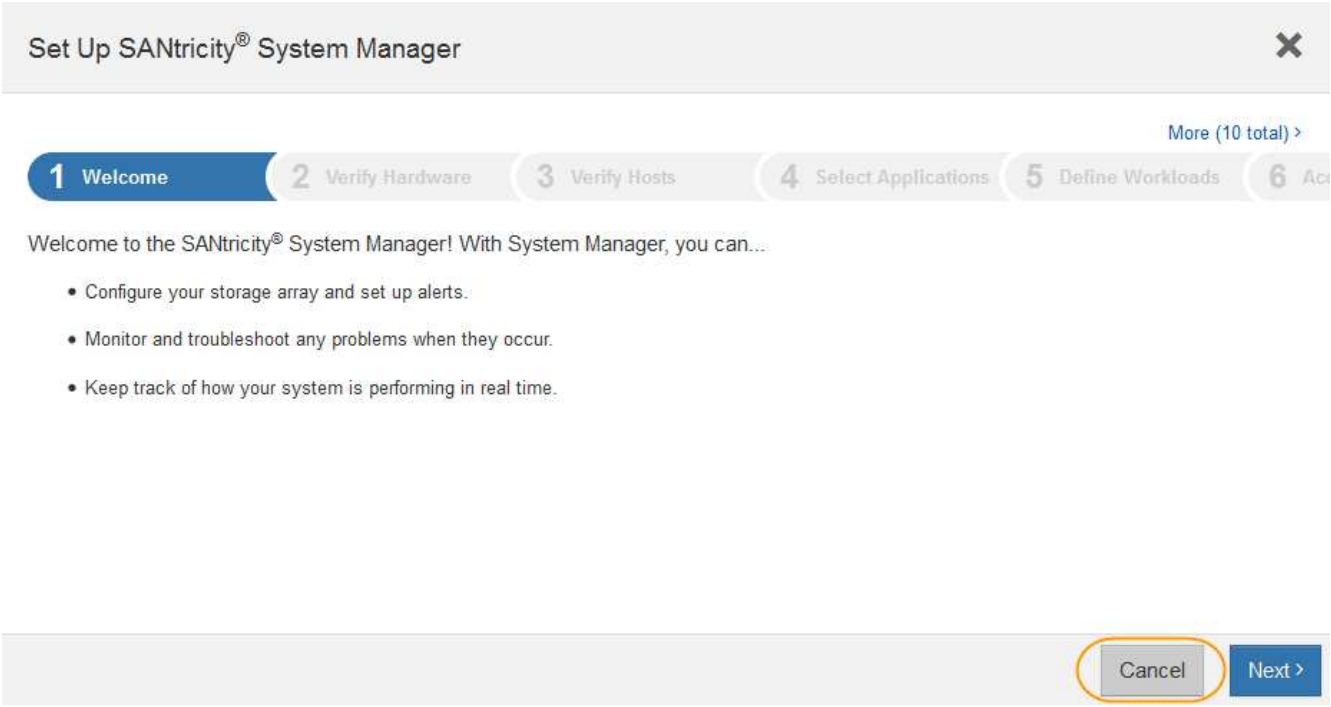
> Si el instalador de dispositivos StorageGRID no está disponible o no aparece la página de inicio de sesión, debe utilizar la dirección IP de la controladora de almacenamiento. Acceda a SANtricity System Manager; para ello, vaya a la dirección IP de la controladora de almacenamiento:
> `https://Storage_Controller_IP`

Aparece la página de inicio de sesión de SANtricity System Manager.

2. Defina o introduzca la contraseña del administrador.

> SANtricity System Manager utiliza una única contraseña de administrador que comparten todos los usuarios.

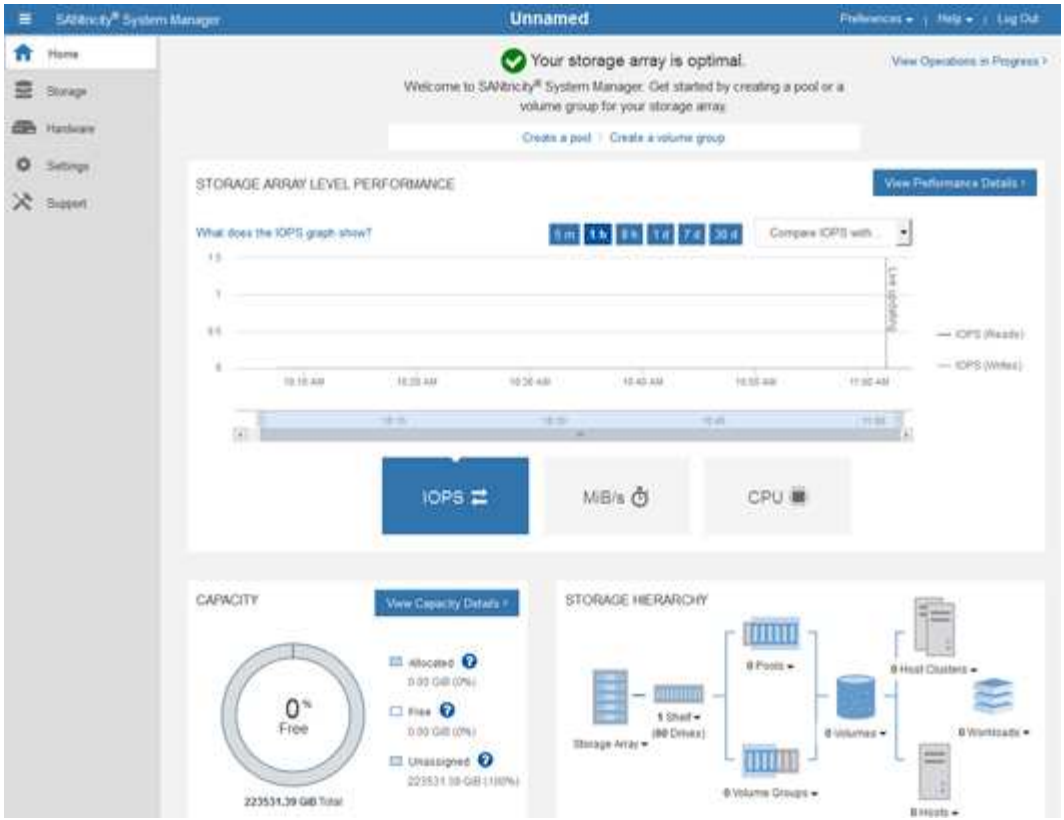
Se mostrará el asistente de configuración.



3. Seleccione **Cancelar** para cerrar el asistente.

> No complete el asistente de configuración de un dispositivo StorageGRID.

Se mostrará la página de inicio de SANtricity System Manager.



4. Configurar alertas de hardware.
   a. Seleccione **Ayuda** para acceder a la ayuda en línea del Administrador del sistema de SANtricity.
   b. Utilice la sección **Configuración** > **Alertas** de la ayuda en línea para obtener información sobre las alertas.
   c. Siga las instrucciones de configuración para configurar alertas por correo electrónico, alertas SNMP o alertas syslog.
5. Gestione AutoSupport para los componentes de la bandeja de controladoras de almacenamiento.
   a. Seleccione **Ayuda** para acceder a la ayuda en línea del Administrador del sistema de SANtricity.
   b. Utilice la sección **SUPPORT** > **Support Center** de la ayuda en línea para obtener más información sobre la función AutoSupport.
   c. Siga las instrucciones «¿Cómo?» para gestionar AutoSupport.

      Si desea obtener instrucciones específicas sobre la configuración de un proxy StorageGRID para enviar mensajes de AutoSupport E-Series sin usar el puerto de gestión, vaya a las instrucciones para administrar StorageGRID y busque "Configuración del proxy para AutoSupport de E-Series".

Administre StorageGRID

6. Si la función Drive Security está habilitada para el dispositivo, cree y gestione la clave de seguridad.
   a. Seleccione **Ayuda** para acceder a la ayuda en línea del Administrador del sistema de SANtricity.
   b. Utilice la sección **Configuración** > **sistema** > **Gestión de claves de seguridad** de la ayuda en línea para obtener información sobre Drive Security.
   c. Siga las instrucciones de «Cómo» para crear y gestionar la clave de seguridad.
7. Si lo desea, puede cambiar la contraseña del administrador.

a. Seleccione **Ayuda** para acceder a la ayuda en línea del Administrador del sistema de SANtricity.

b. Utilice la sección **Inicio** > **Administración de matrices de almacenamiento** de la ayuda en línea para obtener información sobre la contraseña de administrador.

c. Siga las instrucciones "Cómo" para cambiar la contraseña.

Revisar el estado del hardware en System Manager de SANtricity

Puede usar System Manager de SANtricity para supervisar y gestionar componentes de hardware individuales de la bandeja de controladoras de almacenamiento y para revisar la información medioambiental y los diagnósticos de hardware, como la temperatura de los componentes, así como los problemas relacionados con las unidades.

Lo que necesitará

- Está utilizando un navegador web compatible.
- Para acceder a System Manager de SANtricity a través de Grid Manager, debe contar con permisos de administrador de dispositivos de almacenamiento o de acceso raíz.
- Para acceder a System Manager de SANtricity mediante el instalador de dispositivos de StorageGRID, debe tener el nombre de usuario y la contraseña de administrador de SANtricity System Manager.
- Para acceder a SANtricity System Manager directamente mediante un explorador web, debe tener el nombre de usuario y la contraseña de administrador de SANtricity System Manager.

> Debe tener el firmware 8.70 (11.70) de SANtricity o superior para acceder a System Manager de SANtricity mediante Grid Manager o el instalador de dispositivos de StorageGRID.

> Acceder a SANtricity System Manager desde Grid Manager o desde el instalador de dispositivos generalmente se realiza solo para supervisar el hardware y configurar E-Series AutoSupport. Muchas funciones y operaciones en SANtricity System Manager, como la actualización de firmware, no se aplican a la supervisión del dispositivo StorageGRID. Para evitar problemas, siga siempre las instrucciones de instalación y mantenimiento del hardware del dispositivo.

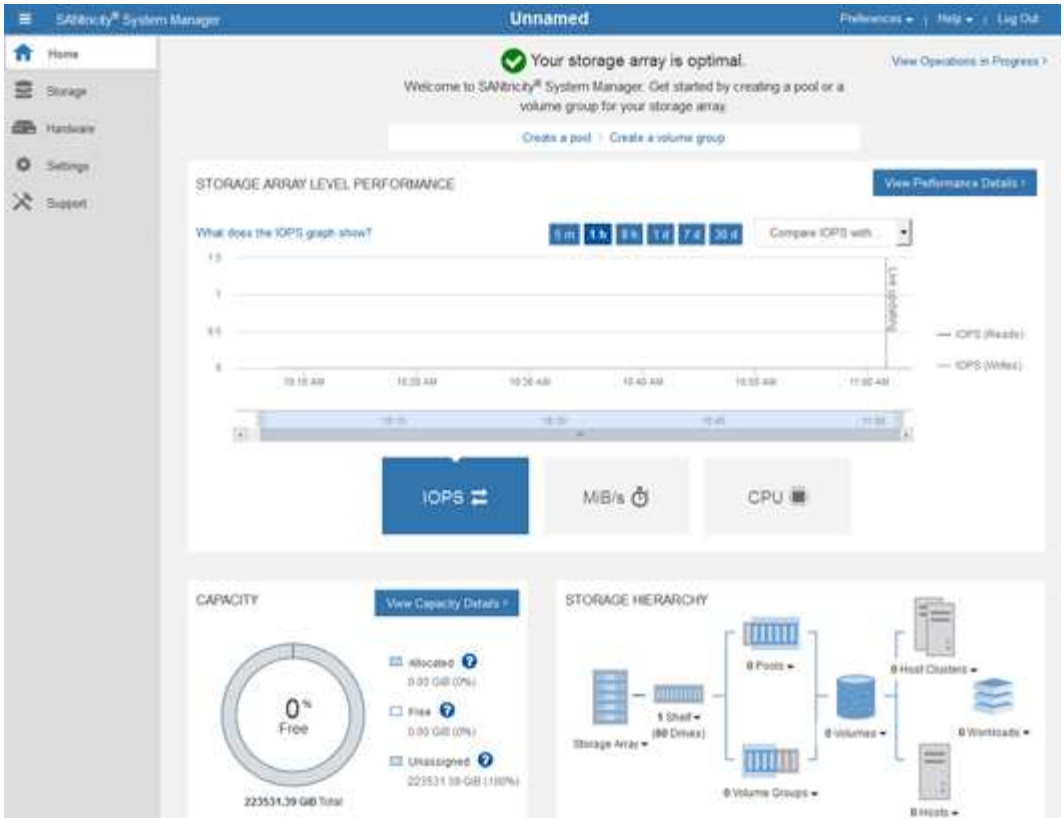
Pasos

1. Acceda a SANtricity System Manager.

   Configuración y acceso a System Manager de SANtricity

2. Introduzca el nombre de usuario y la contraseña del administrador si es necesario.
3. Haga clic en **Cancelar** para cerrar el asistente de configuración y mostrar la página de inicio del Administrador del sistema de SANtricity.

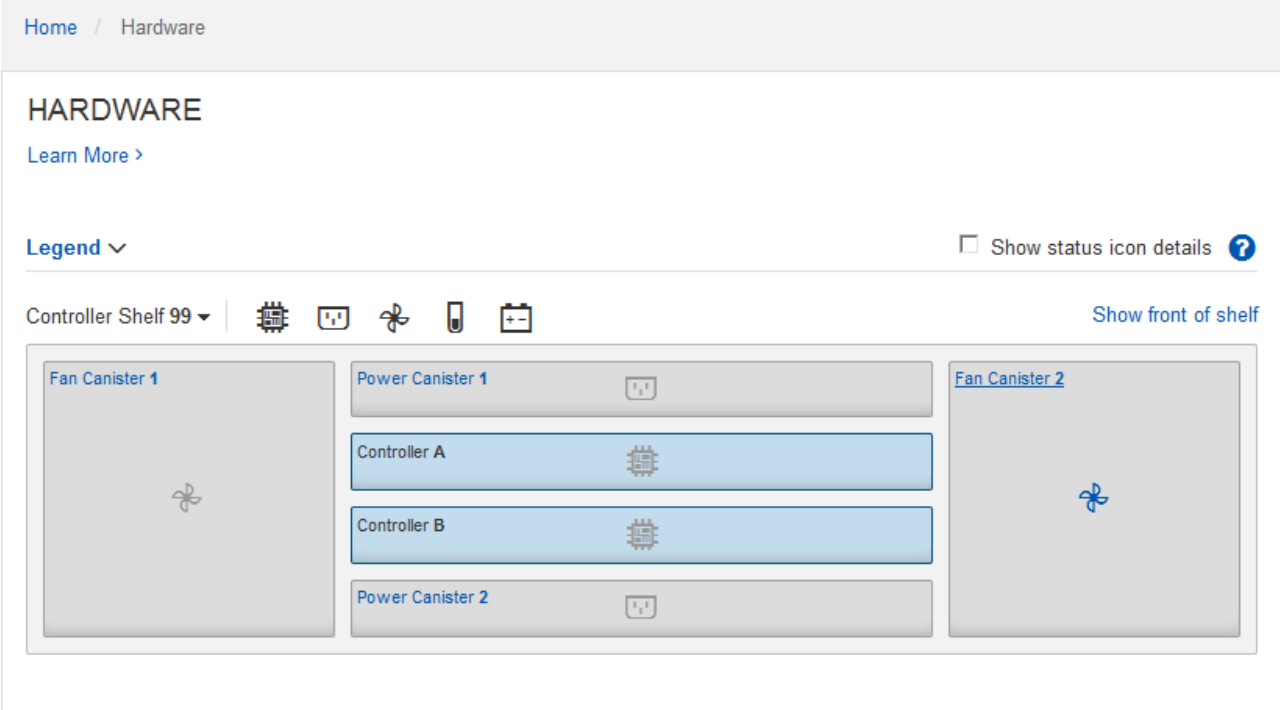
   Se mostrará la página de inicio de SANtricity System Manager. En SANtricity System Manager, la bandeja de controladoras se denomina cabina de almacenamiento.



4. Revise la información mostrada para el hardware del dispositivo y confirme que todos los componentes de hardware tienen un estado óptimo.

   a. Haga clic en la ficha **hardware**.

   b. Haga clic en **Mostrar parte posterior de la bandeja**.



Desde la parte posterior de la bandeja, puede ver ambas controladoras de almacenamiento, la batería de cada controladora de almacenamiento, los dos contenedores de alimentación, los dos compartimentos de

ventiladores y las bandejas de expansión (si los hubiera). También puede ver las temperaturas de los componentes.

a. Para ver los ajustes de cada controlador de almacenamiento, seleccione el controlador y seleccione **Ver ajustes** en el menú contextual.
b. Para ver la configuración de otros componentes de la parte posterior de la bandeja, seleccione el componente que desea ver.
c. Haga clic en **Mostrar frente de la bandeja** y seleccione el componente que desea ver.

   Desde el frente de la bandeja, es posible ver las unidades y los cajones de unidades de la bandeja de controladoras de almacenamiento o las bandejas de expansión (si las hubiera).

Si el estado de cualquier componente es necesita atención, siga los pasos de Recovery Guru para resolver el problema o póngase en contacto con el soporte técnico.

Establezca las direcciones IP para las controladoras de almacenamiento mediante el instalador de dispositivos de StorageGRID

El puerto de gestión 1 de cada controladora de almacenamiento conecta el dispositivo a la red de gestión para SANtricity System Manager. Si no puede acceder a SANtricity System Manager desde el instalador de dispositivos StorageGRID, debe configurar una dirección IP estática para cada controladora de almacenamiento a fin de garantizar que no se pierda la conexión de gestión con el hardware y el firmware de la controladora en la bandeja de controladoras.

Lo que necesitará

- Está utilizando cualquier cliente de gestión que pueda conectarse a la red de administración de StorageGRID o que tenga un portátil de servicio.
- El cliente o el portátil de servicio tienen un navegador web compatible.

Acerca de esta tarea

Las direcciones asignadas por DHCP pueden cambiar en cualquier momento. Asigne direcciones IP estáticas a las controladoras para garantizar una accesibilidad constante.

> Siga este procedimiento sólo si no tiene acceso al Administrador del sistema SANtricity desde el instalador del dispositivo StorageGRID (**Avanzado** > **Administrador del sistema SANtricity**) o el Administrador de grid (**NODOS** > **Administrador del sistema SANtricity**).

Pasos

1. Desde el cliente, introduzca la URL del instalador de dispositivos de StorageGRID:
   `https://`*`Appliance_Controller_IP`*`:8443`

   Para *`Appliance_Controller_IP`*, Utilice la dirección IP del dispositivo en cualquier red StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Configurar hardware** > **Configuración de red del controlador de almacenamiento**.

   Aparece la página Storage Controller Network Configuration.

3. En función de la configuración de la red, seleccione **habilitado** para IPv4, IPv6 o ambos.
4. Anote la dirección IPv4 que se muestra automáticamente.

   DHCP es el método predeterminado para asignar una dirección IP al puerto de gestión de la controladora de almacenamiento.

   > Puede que los valores de DHCP deban tardar varios minutos en aparecer.

5. De manera opcional, configurar una dirección IP estática para el puerto de gestión de la controladora de almacenamiento.

   > Debe asignar una IP estática al puerto de gestión o una concesión permanente para la dirección en el servidor DHCP.

   a. Seleccione **estático**.
   b. Introduzca la dirección IPv4 mediante la notación CIDR.
   c. Introduzca la pasarela predeterminada.

   d. Haga clic en **Guardar**.

      Puede que los cambios se apliquen en unos minutos.

   Cuando se conecta a SANtricity System Manager, utilizará la nueva dirección IP estática como la URL: `https://Storage_Controller_IP`

Opcional: Habilite el cifrado de nodos

Si habilita el cifrado de nodos, los discos del dispositivo pueden protegerse mediante el cifrado del servidor de gestión de claves seguro (KMS) contra la pérdida física o la eliminación del sitio. Debe seleccionar y habilitar el cifrado de nodos durante la instalación del dispositivo y no puede anular la selección del cifrado de nodos una vez que se inicia el proceso de cifrado KMS.

Lo que necesitará

Revise la información sobre KMS en las instrucciones para administrar StorageGRID.

Acerca de esta tarea

Un dispositivo con el cifrado de nodos habilitado se conecta al servidor de gestión de claves (KMS) externo que está configurado para el sitio StorageGRID. Cada KMS (o clúster KMS) administra las claves de cifrado de todos los nodos de dispositivos del sitio. Estas claves cifran y descifran los datos de cada disco de un dispositivo que tiene habilitado el cifrado de nodos.

Se puede configurar un KMS en Grid Manager antes o después de instalar el dispositivo en StorageGRID. Consulte la información sobre la configuración de KMS y del dispositivo en las instrucciones para administrar StorageGRID para obtener más detalles.

- Si se configura un KMS antes de instalar el dispositivo, el cifrado controlado por KMS comienza cuando se habilita el cifrado de nodos en el dispositivo y se lo agrega a un sitio StorageGRID donde se configura KMS.
- Si no se configura un KMS antes de instalar el dispositivo, el cifrado controlado por KMS se lleva a cabo en cada dispositivo que tenga activado el cifrado de nodos en cuanto se configure un KMS y esté disponible para el sitio que contiene el nodo del dispositivo.

> Los datos que existen antes de conectarse al KMS en un dispositivo con el cifrado de nodos habilitado se cifran con una clave temporal que no es segura. El dispositivo no está protegido de la retirada o robo hasta que la clave se configure en un valor proporcionado por el KMS.

Sin la clave KMS necesaria para descifrar el disco, los datos del dispositivo no se pueden recuperar y se pierden de forma efectiva. Este es el caso siempre que la clave de descifrado no se pueda recuperar del KMS. La clave se vuelve inaccesible si elimina la configuración de KMS, caduca una clave KMS, se pierde la conexión con el KMS o se elimina el dispositivo del sistema StorageGRID donde están instaladas sus claves KMS.

Pasos

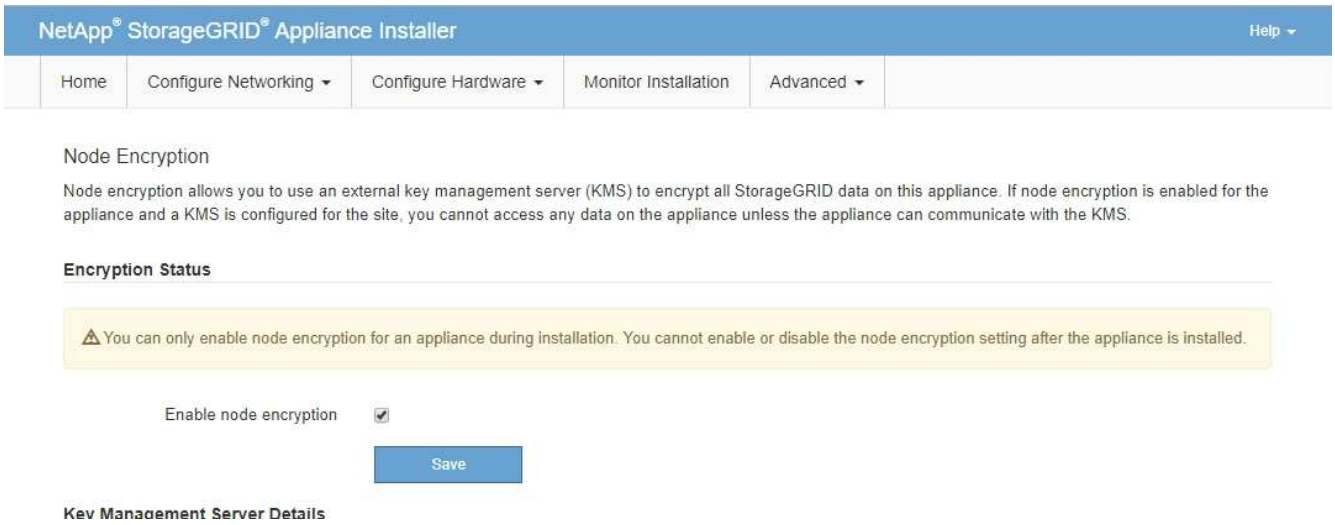
1. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.
   `https://`*`Controller_IP`*`:8443`

   `Controller_IP` Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

   > Una vez que el dispositivo se ha cifrado con una clave KMS, los discos del dispositivo no se pueden descifrar sin utilizar la misma clave KMS.

2. Seleccione **Configurar hardware** > **cifrado de nodos**.



3. Seleccione **Activar cifrado de nodo**.

   Antes de instalar el dispositivo, puede anular la selección **Activar cifrado de nodo** sin riesgo de pérdida de datos. Cuando se inicia la instalación el nodo del dispositivo, accede a las claves de cifrado de KMS en el sistema StorageGRID y comienza el cifrado de disco. No se puede deshabilitar el cifrado de nodos después de haber instalado el dispositivo.

   > Después de agregar un dispositivo que tiene habilitado el cifrado de nodos a un sitio StorageGRID que tiene un KMS, no puede detener el uso del cifrado KMS para el nodo.

4. Seleccione **Guardar**.
5. Ponga en marcha el dispositivo como nodo en su sistema StorageGRID.

   El cifrado controlado POR KMS se inicia cuando el dispositivo accede a las claves KMS configuradas para el sitio StorageGRID. El instalador muestra mensajes de progreso durante el proceso de cifrado KMS, que puede tardar unos minutos en función del número de volúmenes de disco del dispositivo.

   > Los dispositivos se configuran inicialmente con una clave de cifrado no KMS aleatoria asignada a cada volumen de disco. Los discos se cifran con esta clave de cifrado temporal, que no es segura, hasta que el dispositivo con cifrado de nodos habilitado acceda a las claves KMS configuradas para el sitio StorageGRID.

Después de terminar

Puede ver el estado de cifrado de nodo, los detalles de KMS y los certificados en uso cuando el nodo del dispositivo está en modo de mantenimiento.

Información relacionada

Administre StorageGRID

Supervisar el cifrado de nodo en modo de mantenimiento (SG5700)

Opcional: Cambiar el modo RAID (solo SG5760)

Si tiene un SG5760 con 60 unidades, puede cambiar a otro modo RAID para adaptarse a sus requisitos de almacenamiento y recuperación. Solo puede cambiar el modo antes de implementar el nodo de almacenamiento del dispositivo StorageGRID.

Lo que necesitará

- Tiene un SG5760. Si tiene un SG5712, debe usar el modo DDP.
- Está utilizando cualquier cliente que pueda conectarse a StorageGRID.
- El cliente tiene un navegador web compatible.

Acerca de esta tarea

Antes de implementar el dispositivo SG5760 como nodo de almacenamiento, puede seleccionar una de las siguientes opciones de configuración de volúmenes:

- **DDP**: Este modo utiliza dos unidades de paridad por cada ocho unidades de datos. Éste es el modo predeterminado y recomendado para todos los dispositivos. En comparación con RAID6, los DDP ofrecen mejor rendimiento del sistema, reducen los tiempos de recompilación después de fallos de unidad y facilitan la gestión. Además, DDP ofrece protección contra pérdida de cajón en dispositivos de 60 unidades.
- **DDP16**: Este modo utiliza dos unidades de paridad por cada 16 unidades de datos, lo que da como resultado una mayor eficiencia de almacenamiento en comparación con DDP. En comparación con RAID6, DDP16 ofrece un mejor rendimiento del sistema, menores tiempos de recompilación después de fallos de unidad, facilidad de gestión y una eficiencia de almacenamiento similar. Para utilizar el modo DDP16, la configuración debe contener al menos 20 unidades. DDP16 no ofrece protección contra pérdida de cajón.
- **RAID6**: Este modo utiliza dos unidades de paridad por cada 16 o más unidades de datos. Para utilizar el modo RAID 6, la configuración debe contener al menos 20 unidades. Aunque RAID6 puede aumentar la eficiencia de almacenamiento del dispositivo en comparación con DDP, no es recomendable para la mayoría de entornos StorageGRID.

> Si alguno de los volúmenes ya está configurado o si StorageGRID se instaló anteriormente, al cambiar el modo RAID se quitan y se reemplazan los volúmenes. Se perderán todos los datos de estos volúmenes.

Pasos

1. Con el portátil de servicio, abra un explorador web y acceda al instalador de dispositivos de StorageGRID: **`https://E5700SG_Controller_IP:8443`**

   Donde *`E5700SG_Controller_IP`* Es cualquiera de las direcciones IP de la controladora E5700SG.

2. Seleccione **Avanzado** > **modo RAID**.
3. En la página **Configurar el modo RAID**, seleccione el modo RAID deseado en la lista desplegable modo.
4. Haga clic en **Guardar**.

Información relacionada

"Sitio de documentación para sistemas E-Series y EF-Series de NetApp"

Opcional: Reasignar puertos de red para el dispositivo

Es posible que deba reasignar los puertos internos del nodo de almacenamiento del dispositivo a diferentes puertos externos. Por ejemplo, es posible que tenga que reasignar puertos debido a un problema de firewall.

Lo que necesitará

- Ya ha accedido anteriormente al instalador de dispositivos de StorageGRID.

- No ha configurado y no planea configurar los extremos del equilibrador de carga.

> Si se reasigna algún puerto, no se pueden utilizar los mismos puertos para configurar los puntos finales del equilibrador de carga. Si desea configurar puntos finales del equilibrador de carga y ya tiene puertos reasignados, siga los pasos de Eliminar reasignaciones de puertos.

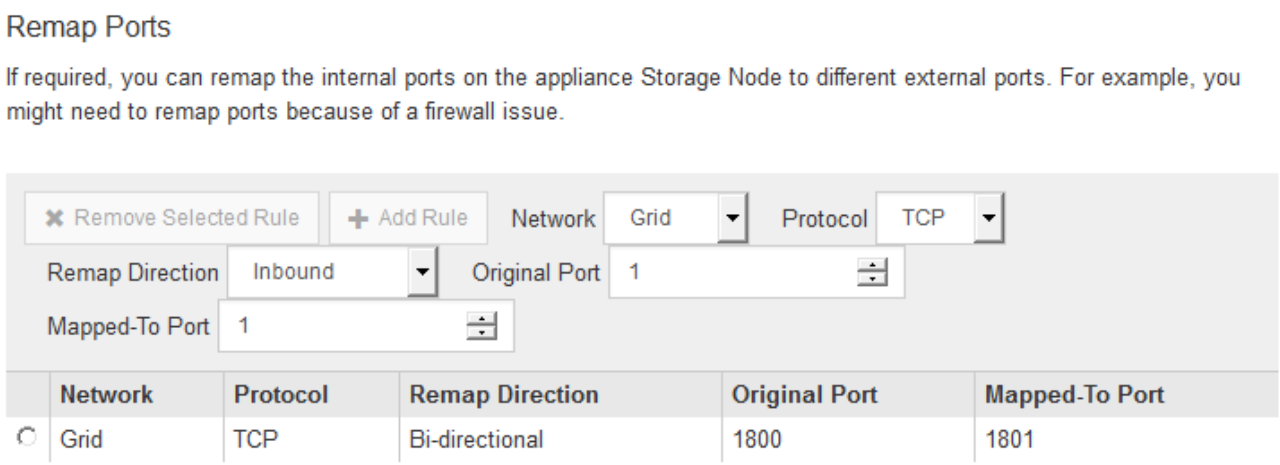
Pasos

1. En la barra de menús del instalador del dispositivo StorageGRID, haga clic en **Configurar redes** > **puertos de reasignación**.

   Aparecerá la página Remap Port.

2. En el cuadro desplegable **Red**, seleccione la red para el puerto que desea reasignar: Grid, Admin o Client.
3. En el cuadro desplegable **Protocolo**, seleccione el protocolo IP: TCP o UDP.
4. En el cuadro desplegable **Dirección de salida**, seleccione la dirección de tráfico que desea reasignar para este puerto: Entrante, saliente o bidireccional.
5. Para **Puerto original**, introduzca el número del puerto que desea reasignar.
6. En **Puerto asignado a**, introduzca el número del puerto que desea utilizar en su lugar.
7. Haga clic en **Agregar regla**.

   La nueva asignación de puertos se agrega a la tabla y la reasignación tiene efecto inmediatamente.



8. Para eliminar una asignación de puertos, seleccione el botón de opción de la regla que desea quitar y haga clic en **Eliminar regla seleccionada**.

Ponga en marcha el nodo de almacenamiento del dispositivo

Después de instalar y configurar el dispositivo de almacenamiento, puede ponerlo en marcha como un nodo de almacenamiento en un sistema StorageGRID. Al poner en marcha un dispositivo como nodo de almacenamiento, utiliza el instalador de dispositivos de StorageGRID que se incluye en el dispositivo.

Lo que necesitará

- Si va a clonar un nodo de dispositivo, continúe durante el proceso de recuperación y mantenimiento.

  Recuperación y mantenimiento

- El dispositivo se ha instalado en un rack o armario, conectado a las redes y encendido.
- Se han configurado los enlaces de red, las direcciones IP y la reasignación de puertos (si fuera necesario) para el dispositivo con el instalador de dispositivos de StorageGRID.
- Conoce una de las direcciones IP asignadas a la controladora de computación del dispositivo. Puede usar la dirección IP para cualquier red StorageGRID conectada.
- Se puso en marcha el nodo de administración principal del sistema 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.
- Tiene un portátil de servicio con un navegador web compatible.

Acerca de esta tarea

Cada dispositivo de almacenamiento funciona como un único nodo de almacenamiento. Cualquier dispositivo puede conectarse a la red de grid, a la red de administración y a la red de cliente

Para implementar un nodo de almacenamiento de dispositivos en un sistema StorageGRID, debe acceder al instalador de dispositivos StorageGRID y realizar los siguientes pasos:

- Debe especificar o confirmar la dirección IP del nodo de administrador principal y el nombre del nodo de almacenamiento.
- Se inicia la puesta en marcha y se espera a medida que se hayan configurado los volúmenes y se haya instalado el software.
- Cuando la instalación se detiene paso a paso a través de las tareas de instalación del dispositivo, se reanuda la instalación iniciando sesión en el Administrador de grid, aprobando todos los nodos de cuadrícula y completando los procesos de instalación e implementación de StorageGRID.

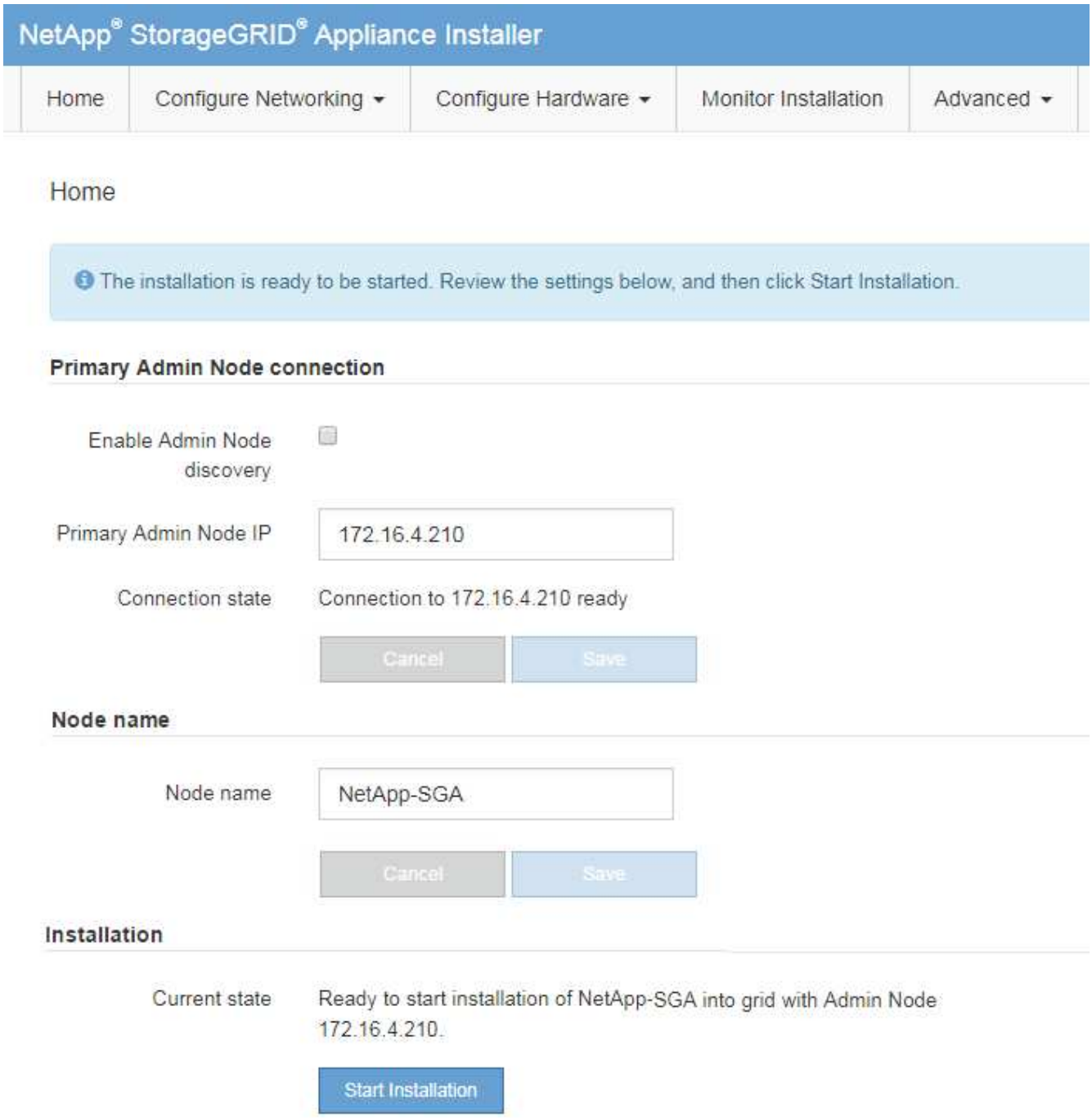
> Si necesita implementar varios nodos de dispositivos a la vez, puede automatizar el proceso de instalación mediante el `configure-sga.py` Script de instalación del dispositivo.

- Si va a realizar una operación de expansión o recuperación, siga las instrucciones correspondientes:
  - Para añadir un nodo de almacenamiento del dispositivo a un sistema StorageGRID existente, consulte las instrucciones para ampliar un sistema StorageGRID.
  - Para poner en marcha un nodo de almacenamiento del dispositivo como parte de una operación de recuperación, consulte las instrucciones de recuperación y mantenimiento.

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 **Conexión del 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. Anule la selección de la casilla de verificación **Activar descubrimiento de nodo de administración**. 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.
Detección automática de todos los nodos principales de administración conectados	a. Active la casilla de verificación **Activar descubrimiento de nodos de administración**. 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 haga clic en **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 **instalación**, confirme que el estado actual es "Listo para iniciar la instalación de `node name` En el grid con el nodo de administrador principal `admin_ip` " Y que el botón **Iniciar instalación** 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 instalación y mantenimiento del aparato.

   > Si va a poner en marcha el dispositivo Storage Node como destino de clonado de nodos, detenga el proceso de puesta en marcha aquí y continúe con el procedimiento de clonado de nodos en recuperación y mantenimiento.

   Recuperación y mantenimiento

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**.

7. Si el grid incluye varios nodos de almacenamiento de dispositivos, repita estos pasos para cada dispositivo.

> Si necesita implementar varios nodos de almacenamiento para dispositivos a la vez, puede automatizar el proceso de instalación mediante el `configure-sga.py` Script de instalación del dispositivo.

Información relacionada

Amplíe su grid

Recuperación y mantenimiento

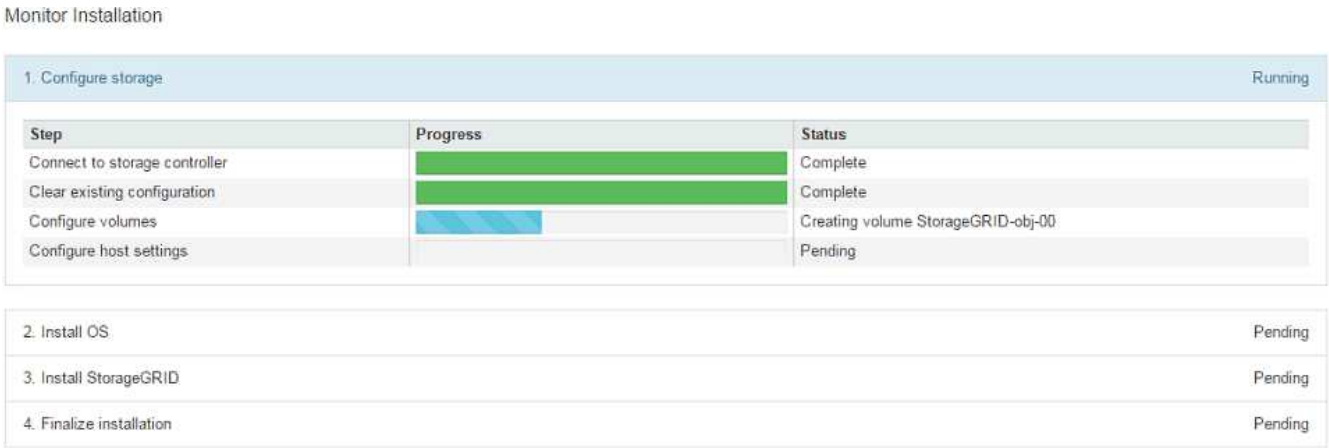
Supervise la instalación de dispositivos de almacenamiento

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**.

   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.

> El instalador garantiza que no se vuelvan a ejecutar las tareas completadas en una instalación anterior. 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 de "Shided."

2. Revise el progreso de las dos primeras etapas de instalación.

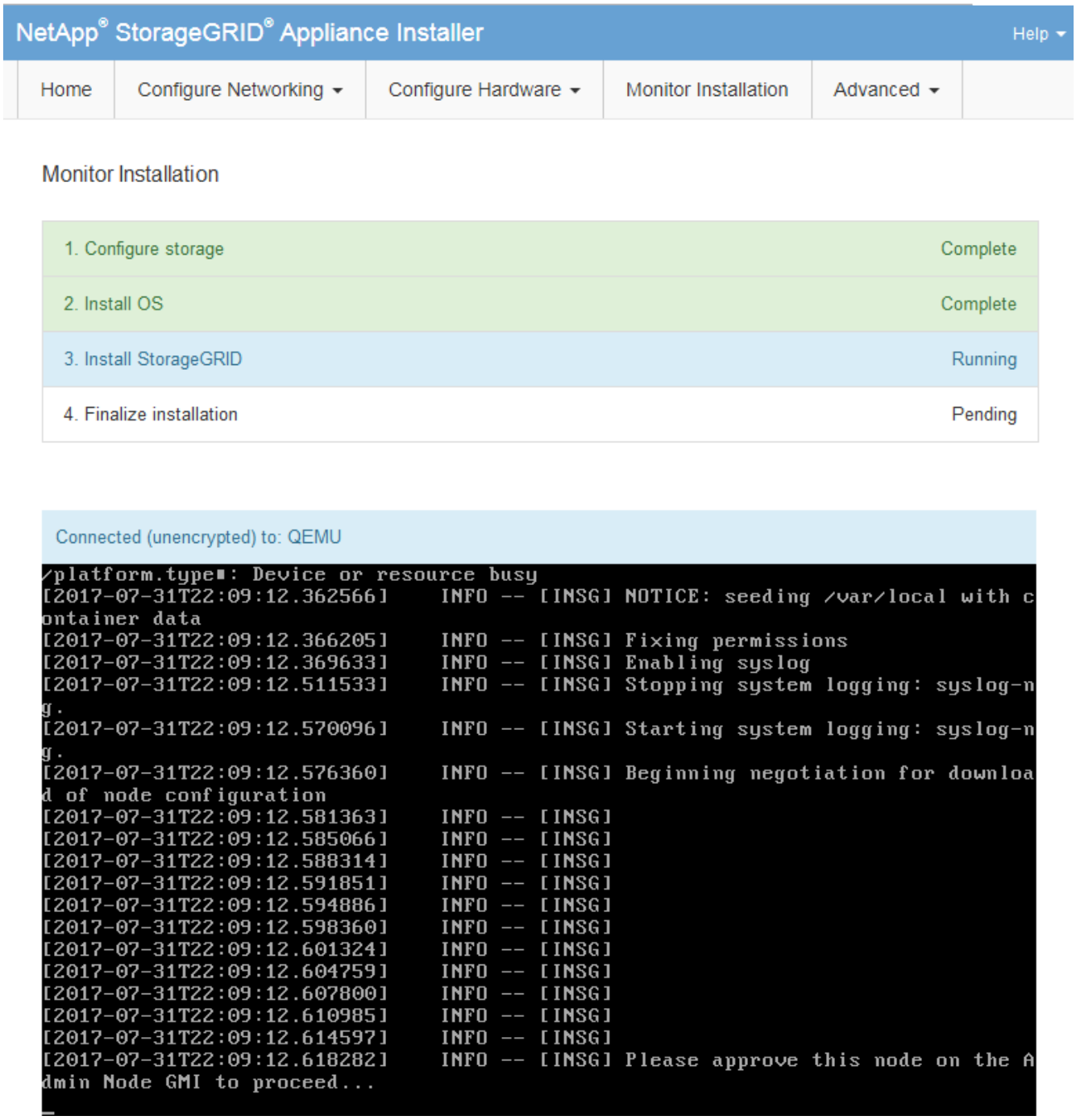
   1. Configurar almacenamiento

   Durante esta fase, el instalador se conecta al controlador de almacenamiento, borra cualquier configuración existente, se comunica con el software 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, solicitándole que apruebe este nodo en el nodo de administración mediante el Administrador de grid. Vaya al paso siguiente.



4. Vaya a Grid Manager del nodo Primary Admin, apruebe el nodo de almacenamiento pendiente y complete el proceso de instalación de StorageGRID.

   Al hacer clic en **instalar** desde Grid Manager, se completa la fase 3 y comienza la fase 4, **Finalizar instalación**. Cuando finaliza la etapa 4, se reinicia la controladora.

Automatizar la instalación y configuración del dispositivo (SG5700)

Puede automatizar la instalación y configuración de sus dispositivos y la configuración de todo el sistema StorageGRID.

Acerca de esta tarea

Automatizar la instalación y la configuración puede ser útil para poner en marcha varias instancias de StorageGRID o una instancia de StorageGRID grande y compleja.

Para automatizar la instalación y configuración, utilice una o varias de las siguientes opciones:

- Cree un archivo JSON que especifique las opciones de configuración para los dispositivos. Cargue el archivo JSON con el instalador de dispositivos StorageGRID.

  Puede usar el mismo archivo para configurar más de un dispositivo.

- Utilice la StorageGRID`configure-sga.py` Script Python para automatizar la configuración de sus dispositivos.
- Utilice scripts Python adicionales para configurar otros componentes de todo el sistema StorageGRID (la "cuadrícula").

Puede utilizar directamente los scripts Python de automatización de StorageGRID o bien puede usarlos como ejemplos de cómo utilizar la API DE REST de instalación de StorageGRID en las herramientas de puesta en marcha de grid y de configuración que desarrolla usted mismo. Consulte la información acerca de Descarga y extracción de los archivos de instalación de StorageGRID En las instrucciones de recuperación y mantenimiento.

Automatice la configuración del dispositivo con StorageGRID Appliance Installer

Puede automatizar la configuración de un dispositivo mediante un archivo JSON que contiene la información de configuración. El archivo se carga con el instalador de dispositivos de StorageGRID.

Lo que necesitará

- El dispositivo debe tener el firmware más reciente compatible con StorageGRID 11.5 o superior.
- Debe estar conectado al instalador de dispositivos de StorageGRID en el dispositivo que esté configurando mediante un navegador web compatible.

Acerca de esta tarea

Puede automatizar las tareas de configuración de los dispositivos, como la configuración de las siguientes opciones:

- Redes de grid, red de administración y direcciones IP de red de cliente
- Interfaz BMC
- Enlaces de red
  - Modo de enlace de puerto
  - Modo de enlace de red
  - Velocidad de enlace

La configuración del dispositivo con un archivo JSON cargado suele ser más eficaz que realizar la configuración manualmente mediante múltiples páginas en el instalador del dispositivo StorageGRID, especialmente si tiene que configurar muchos nodos. Debe aplicar el archivo de configuración para cada nodo de uno en uno.

> Los usuarios con experiencia que deseen automatizar tanto la instalación como la configuración de sus dispositivos pueden utilizar el `configure-sga.py` guión. +Automatice la instalación y configuración de los nodos de los dispositivos con un script configure-sga.py

Pasos

1. Genere el archivo JSON mediante uno de los siguientes métodos:
   - Aplicación ConfigBuilder

     "ConfigBuilder.netapp.com"

   - La `configure-sga.py` script de configuración del dispositivo. Puede descargar la secuencia de comandos desde el instalador del dispositivo StorageGRID (**Ayuda** > **secuencia de comandos de configuración del dispositivo**). Consulte las instrucciones sobre cómo automatizar la configuración mediante el script configure-sga.py.

     Automatice la instalación y configuración de los nodos de los dispositivos con un script configure-sga.py

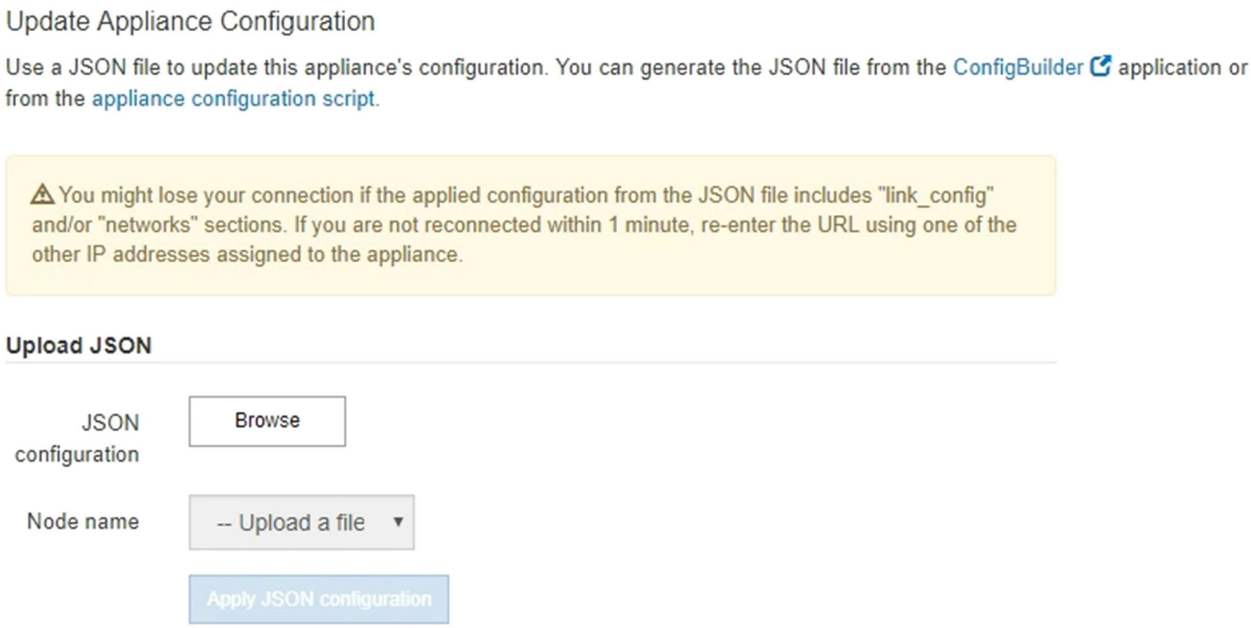
     Los nombres de nodos en el archivo JSON deben seguir estos requisitos:

     - Debe ser un nombre de host válido que contenga al menos 1 y no más de 32 caracteres
     - Puede usar letras, números y guiones
     - No se puede iniciar o finalizar con un guión
     - No se pueden o sólo contienen números

     > Asegúrese de que los nombres de nodo (los nombres de nivel superior) del archivo JSON son únicos o de que no pueda configurar más de un nodo mediante el archivo JSON.

2. Seleccione **Avanzado** > **Actualizar configuración del dispositivo**.

   Aparece la página Actualizar configuración del dispositivo.



3. Seleccione el archivo JSON con la configuración que desea cargar.

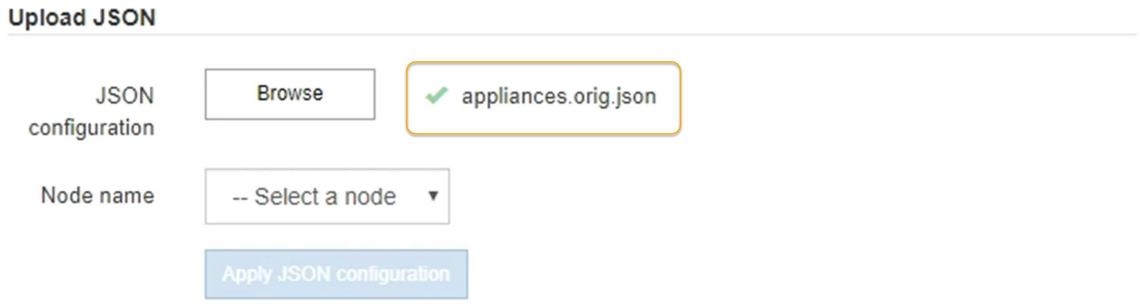
   a. Seleccione **examinar**.

   b. Localice y seleccione el archivo.

   c. Seleccione **Abrir**.

   El archivo se carga y se valida. Una vez completado el proceso de validación, se muestra el nombre del archivo junto a una Marca de verificación verde.

   > Es posible que pierda la conexión con el dispositivo si la configuración del archivo JSON incluye secciones de "link_config", "Networks" o ambas. Si no vuelve a conectarse en 1 minuto, vuelva a introducir la URL del dispositivo utilizando una de las otras direcciones IP asignadas al dispositivo.

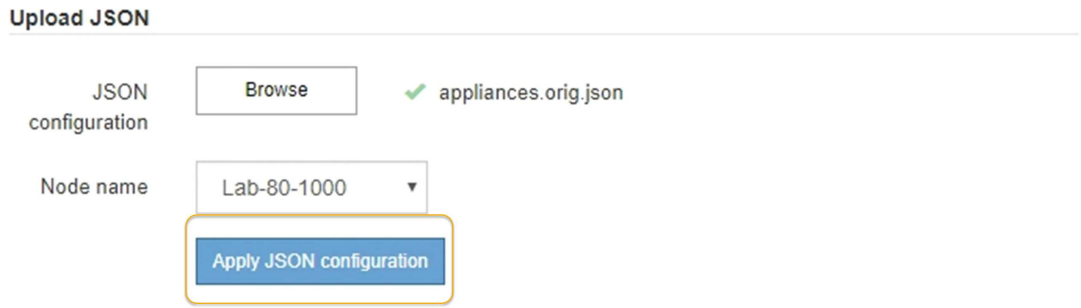


   La lista desplegable **Nombre de nodo** se rellena con los nombres de nodo de nivel superior definidos en el archivo JSON.

Si el archivo no es válido, el nombre del archivo se muestra en rojo y se muestra un mensaje de error en un banner amarillo. El archivo no válido no se ha aplicado al dispositivo. Puede utilizar ConfigBuilder para asegurarse de tener un archivo JSON válido.

4. Seleccione un nodo de la lista de la lista desplegable **Nombre de nodo**.

   El botón **aplicar configuración JSON** está activado.



5. Seleccione **aplicar configuración JSON**.

   La configuración se aplica al nodo seleccionado.

Automatice la instalación y configuración de los nodos de los dispositivos con un script configure-sga.py

Puede utilizar el `configure-sga.py` Script para automatizar muchas de las tareas de instalación y configuración para los nodos del dispositivo StorageGRID, incluida la instalación y configuración de un nodo de administración principal. Esta secuencia de comandos puede ser útil si tiene un gran número de dispositivos que configurar. También puede usar el script para generar un archivo JSON que contenga información de configuración del dispositivo.

Acerca de esta tarea

- 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 nodo de administración principal mediante el instalador de dispositivos de StorageGRID.
- Si está instalando el nodo de administrador principal, conoce su dirección IP.
- Si va a instalar y configurar otros nodos, el nodo de administrador principal se ha implementado y conoce su dirección IP.
- Para todos los nodos que no sean el nodo de administración principal, todas las subredes de red de cuadrícula que aparecen en la página Configuración de IP del instalador de dispositivos StorageGRID se han definido en la lista de subredes de redes de cuadrícula del nodo de administración principal.
- Ha descargado el `configure-sga.py` archivo. El archivo se incluye en el archivo de instalación o puede acceder a él haciendo clic en **Ayuda** > **secuencia de comandos de instalación del dispositivo** en el instalador del dispositivo StorageGRID.

Este procedimiento es para usuarios avanzados con cierta experiencia usando interfaces de línea de comandos. También puede usar el instalador de dispositivos de StorageGRID para automatizar la configuración. +Automatice la configuración del dispositivo con StorageGRID Appliance Installer

Pasos

1. Inicie sesión en el equipo Linux que está utilizando para ejecutar el script Python.
2. Para obtener ayuda general sobre la sintaxis de la secuencia de comandos y ver una lista de los parámetros disponibles, introduzca lo siguiente:

   ```
   configure-sga.py --help
   ```

   La `configure-sga.py` el script utiliza cinco subcomandos:

   - `advanced` Para interacciones avanzadas con dispositivos StorageGRID, incluida la configuración del BMC y la creación de un archivo JSON con la configuración actual del dispositivo
   - `configure` Para configurar los parámetros de modo RAID, nombre del nodo y red
   - `install` Para iniciar una instalación de StorageGRID
   - `monitor` Para supervisar una instalación de StorageGRID
   - `reboot` para reiniciar el dispositivo

   Si introduce un argumento de subcomando (avanzado, configure, instale, monitor o reboot) seguido del `--help` opción usted obtendrá un texto de ayuda diferente que proporciona más detalles sobre las opciones disponibles dentro de ese subcomando:
   `configure-sga.py` *`subcommand`* `--help`

3. Para confirmar la configuración actual del nodo del dispositivo, introduzca lo siguiente donde *`SGA-install-ip`* Es cualquiera de las direcciones IP del nodo del dispositivo:
   `configure-sga.py configure` *`SGA-INSTALL-IP`*

   Los resultados muestran información de IP actual del dispositivo, incluida la dirección IP del nodo de administración principal e información sobre las redes de administración, grid y cliente.

   ```
   Connecting to +https://10.224.2.30:8443+ (Checking version and
   connectivity.)
   2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
   2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
   200
   2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
   Received 200
   2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
   200
   2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
   2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
   200
   ```

```
StorageGRID Appliance
  Name:        LAB-SGA-2-30
  Node type:   storage

StorageGRID primary Admin Node
  IP:        172.16.1.170
  State:     unknown
  Message:   Initializing...
  Version:   Unknown

Network Link Configuration
  Link Status
        Link      State      Speed (Gbps)
        ----      -----      -----
        1         Up         10
        2         Up         10
        3         Up         10
        4         Up         10
        5         Up         1
        6         Down       N/A

  Link Settings
      Port bond mode:      FIXED
      Link speed:          10GBE

      Grid Network:        ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

      Admin Network:       ENABLED
          Bonding mode:    no-bond
          MAC Addresses:   00:80:e5:29:70:f4

      Client Network:      ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

Grid Network
  CIDR:      172.16.2.30/21 (Static)
  MAC:       00:A0:98:59:8E:8A
  Gateway:   172.16.0.1
  Subnets:   172.17.0.0/21
             172.18.0.0/21
             192.168.0.0/21
```

```
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

#################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#################################################################
```

4. Si necesita cambiar alguno de los valores de la configuración actual, utilice `configure` subcomando para actualizarlos. Por ejemplo, si desea cambiar la dirección IP que utiliza el dispositivo para conectarse al nodo de administración principal `172.16.2.99`, introduzca lo siguiente:
   `configure-sga.py configure --admin-ip 172.16.2.99` *`SGA-INSTALL-IP`*
5. Si desea realizar un backup de la configuración del dispositivo en un archivo JSON, utilice `advanced` y.. `backup-file` subcomandos. Por ejemplo, si desea realizar una copia de seguridad de la configuración de un dispositivo con dirección IP *`SGA-INSTALL-IP`* a un archivo llamado `appliance-SG1000.json`, introduzca lo siguiente:
   `configure-sga.py advanced --backup-file appliance-SG1000.json` *`SGA-INSTALL-IP`*

   El archivo JSON que contiene la información de configuración se escribe en el mismo directorio desde el que se ejecutó la secuencia de comandos.

   > Compruebe que el nombre del nodo de nivel superior del archivo JSON generado coincida con el nombre del dispositivo. No haga ningún cambio en este archivo a menos que sea un usuario con experiencia y que tenga una profunda comprensión de las API de StorageGRID.

6. Cuando esté satisfecho con la configuración del dispositivo, utilice `install` y.. `monitor` subcomandos para instalar el dispositivo:
   `configure-sga.py install --monitor` *`SGA-INSTALL-IP`*
7. Si desea reiniciar el dispositivo, introduzca lo siguiente:
   `configure-sga.py reboot` *`SGA-INSTALL-IP`*

Automatice la configuración de StorageGRID

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

Lo que necesitará

- 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
```

Después de terminar

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 ha especificado que se deben generar contraseñas aleatorias, debe extraer 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 general sobre la instalación de API de REST

StorageGRID proporciona dos API REST para realizar tareas de instalación: La API de instalación de StorageGRID y la API del instalador de dispositivos de StorageGRID.

Ambas API utilizan 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 (notación de objetos JavaScript).

> 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 configura inicialmente el sistema StorageGRID y en el caso de que deba realizar una recuperación de nodo de administrador principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de API, vaya a la página web de instalación del nodo de administración principal y seleccione **Ayuda** > **Documentación de 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.
- **Sites** — Operaciones de configuración a nivel de sitio. Puede crear, ver, eliminar y modificar un sitio.

API del instalador de dispositivos de StorageGRID

Se puede acceder a la API del instalador de dispositivos de StorageGRID a través de HTTPS desde `Controller_IP:8443`.

Para acceder a la documentación de la API, vaya al instalador del dispositivo StorageGRID en el dispositivo y seleccione **Ayuda** > **Documentación de la API** en la barra de menús.

La API del instalador de dispositivos de StorageGRID incluye las siguientes secciones:

- **Clone** — Operaciones para configurar y controlar la clonación de nodos.
- **Cifrado** — Operaciones para administrar el cifrado y ver el estado del cifrado.
- **Configuración del hardware** — Operaciones para configurar los ajustes del sistema en el hardware conectado.
- **Instalación** — Operaciones para iniciar la instalación del aparato y para supervisar el estado de instalación.
- **Redes** — Operaciones relacionadas con la configuración de red de Grid, Admin y Cliente para un dispositivo StorageGRID y los ajustes de puerto de dispositivo.
- **Setup** — Operaciones para ayudar con la instalación inicial del dispositivo incluyendo solicitudes para obtener información sobre el sistema y actualizar el IP principal del nodo de administración.
- **SOPORTE** — Operaciones para reiniciar el controlador y obtener registros.
- **Upgrade** — Operaciones relacionadas con la actualización del firmware del dispositivo.
- **Uploadsg** — Operaciones para cargar archivos de instalación de StorageGRID.

Solucionar problemas de instalación de hardware (SG5700)

Si encuentra problemas durante la instalación, es posible que le sea útil revisar información sobre la solución de problemas relacionados con la configuración del hardware y los problemas de conectividad.

La configuración del hardware parece que se bloquea (SG5700)

Es posible que el instalador de dispositivos StorageGRID no esté disponible si los errores de hardware o de cableado impiden que la controladora E5700SG complete su procesamiento de arranque.

Pasos

1. Observe los códigos en las pantallas de siete segmentos.

   Mientras el hardware se está inicializando durante el encendido, las dos pantallas de siete segmentos muestran una secuencia de códigos. Cuando el hardware se arranca correctamente, las pantallas de siete segmentos muestran códigos diferentes para cada controladora.

2. Revise los códigos de la pantalla de siete segmentos del controlador E5700SG.

   > La instalación y el aprovisionamiento tardan en realizarse. Algunas fases de instalación no notifican las actualizaciones del instalador de dispositivos StorageGRID durante varios minutos.

   Si se produce un error, la pantalla de siete segmentos parpadea en una secuencia, como ÉL.

3. Para comprender qué significan estos códigos, consulte los siguientes recursos:

Controladora	Referencia
Controladora E5700SG	• "Indicadores de Estados en el controlador E5700SG" • "'he error: Sincronización de errores con el software de sistema operativo SANtricity'"
Controladora E2800	*E5700 y Guía de supervisión del sistema E2800* **Nota:** los códigos descritos para el controlador E5700 E-Series no se aplican al controlador E5700SG del aparato.

4. Si esto no se resuelve el problema, póngase en contacto con el soporte técnico.

Información relacionada

Indicadores de estado en el controlador E5700SG

Error: Error al sincronizar con el software de sistema operativo SANtricity

"Sitio de documentación para sistemas E-Series y EF-Series de NetApp"

Error: Error al sincronizar con el software de sistema operativo SANtricity

La visualización de siete segmentos en la controladora de computación muestra un código de error HE si el instalador de dispositivos de StorageGRID no puede sincronizarse con el software de sistema operativo SANtricity.

Acerca de esta tarea

Si se muestra UN código DE error, lleve a cabo esta acción correctiva.

Pasos

1. Compruebe los dos cables de interconexión entre las dos controladoras y confirme que los cables y los transceptores SFP+ están conectados de forma segura.
2. Según sea necesario, reemplace uno o ambos cables o transceptores SFP+ y vuelva a intentarlo.
3. Si esto no se resuelve el problema, póngase en contacto con el soporte técnico.

Solucionar problemas de conexión (SG5700)

Si tiene problemas de conexión durante la instalación del dispositivo StorageGRID, debe ejecutar los pasos de acción correctiva indicados.

No se puede conectar al dispositivo

Si no puede conectarse al dispositivo, puede haber un problema de red o es posible que la instalación del hardware no se haya completado correctamente.

Pasos

1. Si no puede conectarse con el Administrador del sistema SANtricity:
   a. Intente hacer ping al dispositivo con la dirección IP de la controladora E2800 en la red de gestión para System Manager de SANtricity:
   `ping E2800_Controller_IP`
   b. Si no recibe respuesta del ping, confirme que está utilizando la dirección IP correcta.

      Use la dirección IP para el puerto de gestión 1 de la controladora E2800.

   c. Si la dirección IP es correcta, compruebe el cableado del dispositivo y la configuración de la red.

      Si esto no se resuelve el problema, póngase en contacto con el soporte técnico.

   d. Si el ping se ha realizado correctamente, abra un explorador Web.
   e. Introduzca la URL para SANtricity System Manager:
   `https://E2800_Controller_IP`

      Aparece la página de inicio de sesión de SANtricity System Manager.

2. Si no puede conectarse al controlador E5700SG:
   a. Intente hacer ping al dispositivo utilizando la dirección IP del controlador E5700SG:
   `ping E5700SG_Controller_IP`
   b. Si no recibe respuesta del ping, confirme que está utilizando la dirección IP correcta.

      Puede utilizar la dirección IP del dispositivo en la red de grid, la red de administración o la red de cliente.

   c. Si la dirección IP es correcta, compruebe el cableado del dispositivo, los transceptores SFP y la configuración de red.

      Si esto no se resuelve el problema, póngase en contacto con el soporte técnico.

d. Si el ping se ha realizado correctamente, abra un explorador Web.

e. Introduzca la URL para el instalador de dispositivos de StorageGRID:
`https://E5700SG_Controller_IP:8443`

Aparece la página de inicio.

Reinicie el controlador mientras el instalador de dispositivos StorageGRID está en ejecución

Es posible que deba reiniciar la controladora de computación mientras se está ejecutando el instalador de dispositivos de StorageGRID. Por ejemplo, es posible que deba reiniciar la controladora si la instalación falla.

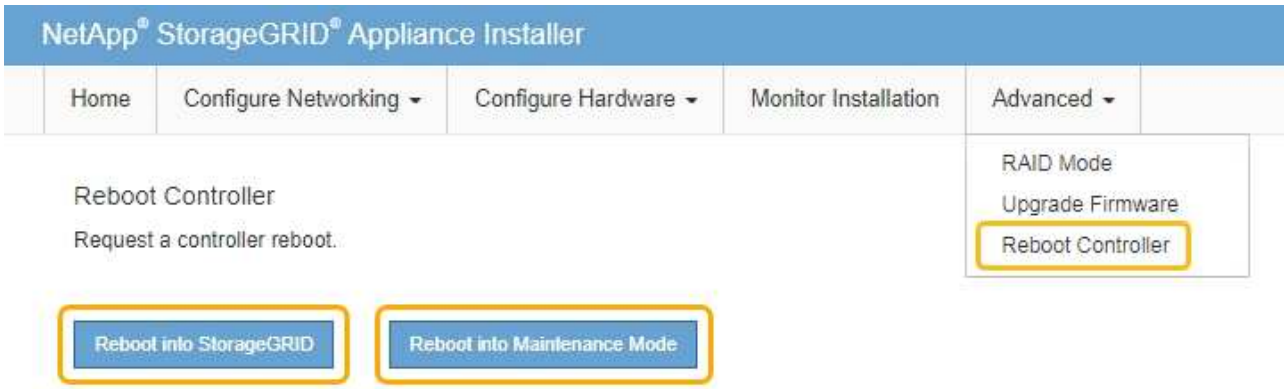
Acerca de esta tarea

Este procedimiento solo se aplica cuando la controladora de computación ejecuta el instalador de dispositivos de StorageGRID. Una vez finalizada la instalación, este paso ya no funciona porque el instalador de dispositivos StorageGRID ya no está disponible.

Pasos

1. En el instalador del dispositivo StorageGRID, haga clic en **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



Se reinicia la controladora.

Mantenga el dispositivo SG5700

Es posible que deba actualizar el software de sistema operativo SANtricity en la controladora E2800, cambiar la configuración de enlace Ethernet de la controladora

E5700SG, reemplazar la controladora E2800 o la controladora E5700SG, o sustituir componentes específicos. En los procedimientos descritos en esta sección se asume que el dispositivo ya se ha puesto en marcha como nodo de almacenamiento en un sistema StorageGRID.

Coloque el dispositivo en modo de mantenimiento

Debe colocar el aparato en modo de mantenimiento antes de realizar procedimientos de mantenimiento específicos.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso de mantenimiento o acceso raíz. Para obtener más detalles, consulte las instrucciones para administrar StorageGRID.

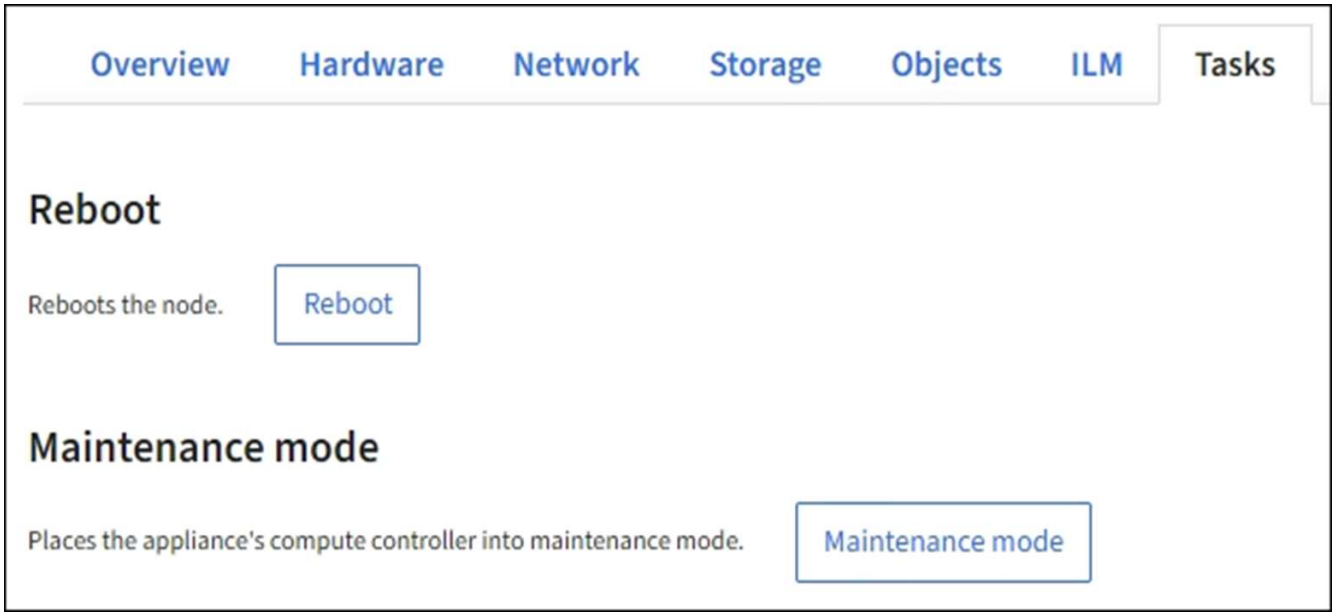
Acerca de esta tarea

En raras ocasiones, una vez que se coloca un dispositivo StorageGRID en modo de mantenimiento puede hacer que el dispositivo no esté disponible para el acceso remoto.

> La contraseña de la cuenta de administrador y las claves de host SSH para un dispositivo StorageGRID en modo de mantenimiento siguen siendo las mismas que en el momento en que el dispositivo estaba en servicio.

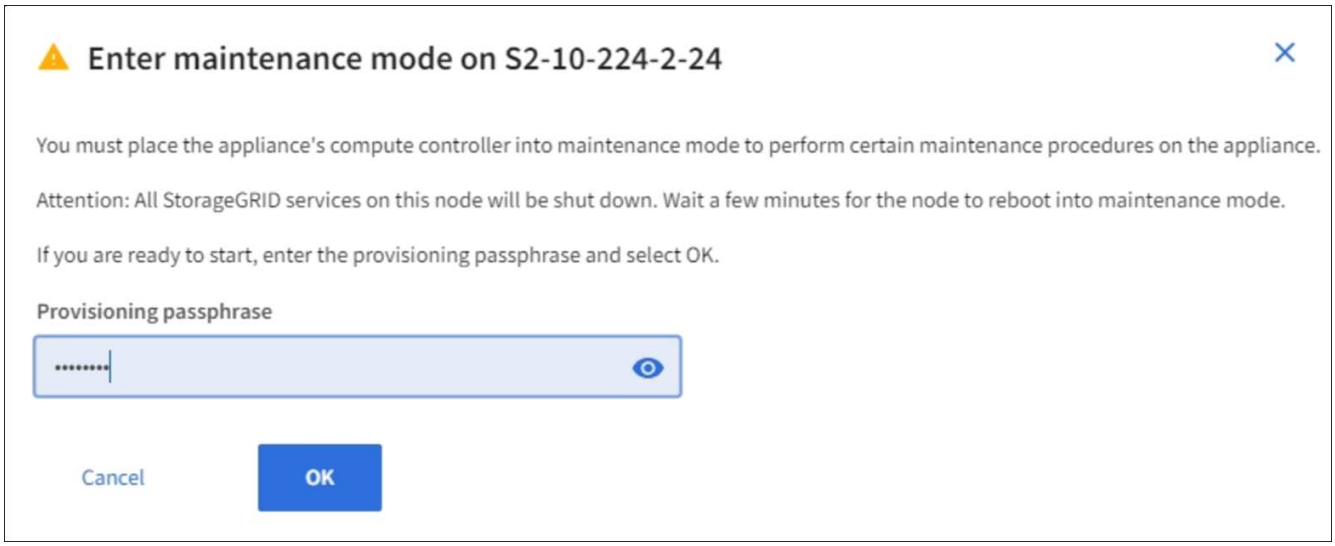
Pasos

1. En Grid Manager, seleccione **NODES**.
2. En la vista de árbol de la página Nodes, seleccione Appliance Storage Node.
3. Seleccione **tareas**.



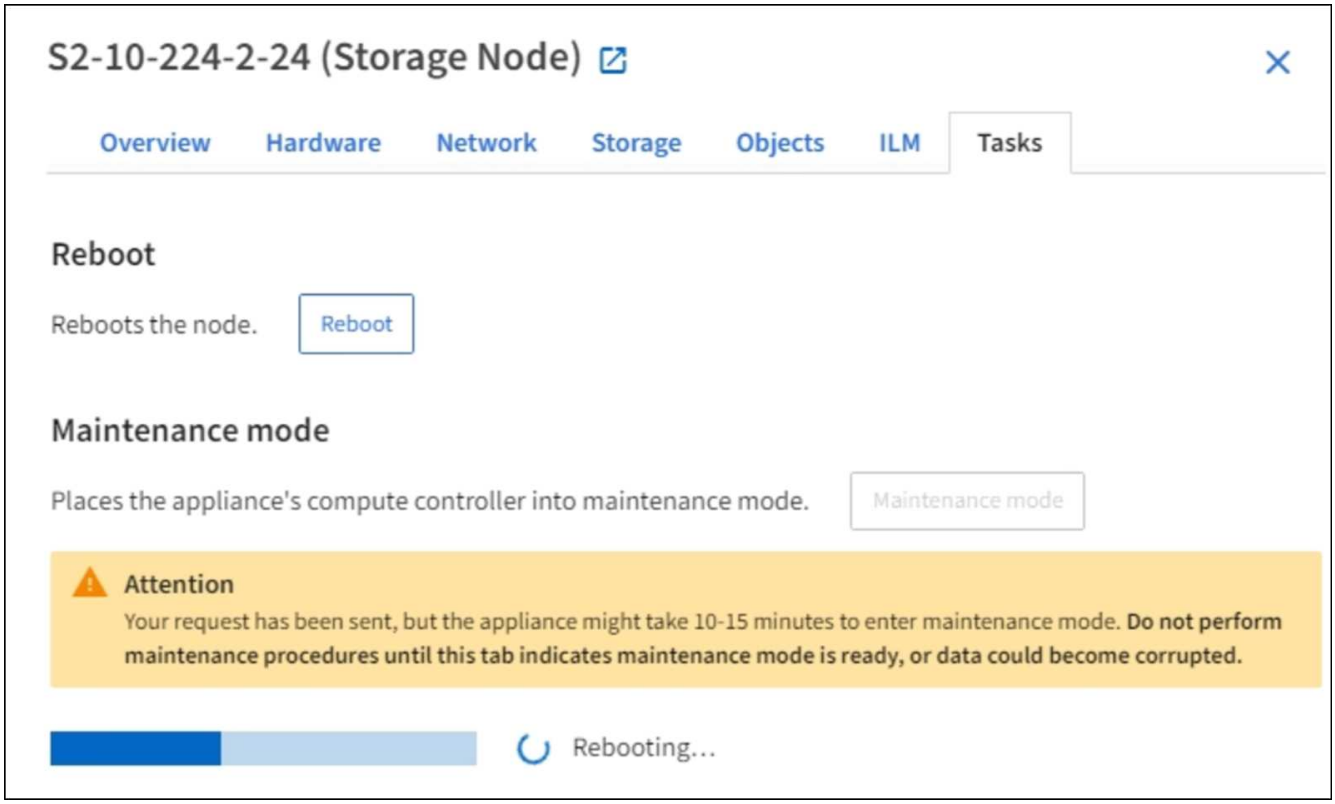
4. Seleccione **modo de mantenimiento**.

   Se muestra un cuadro de diálogo de confirmación.

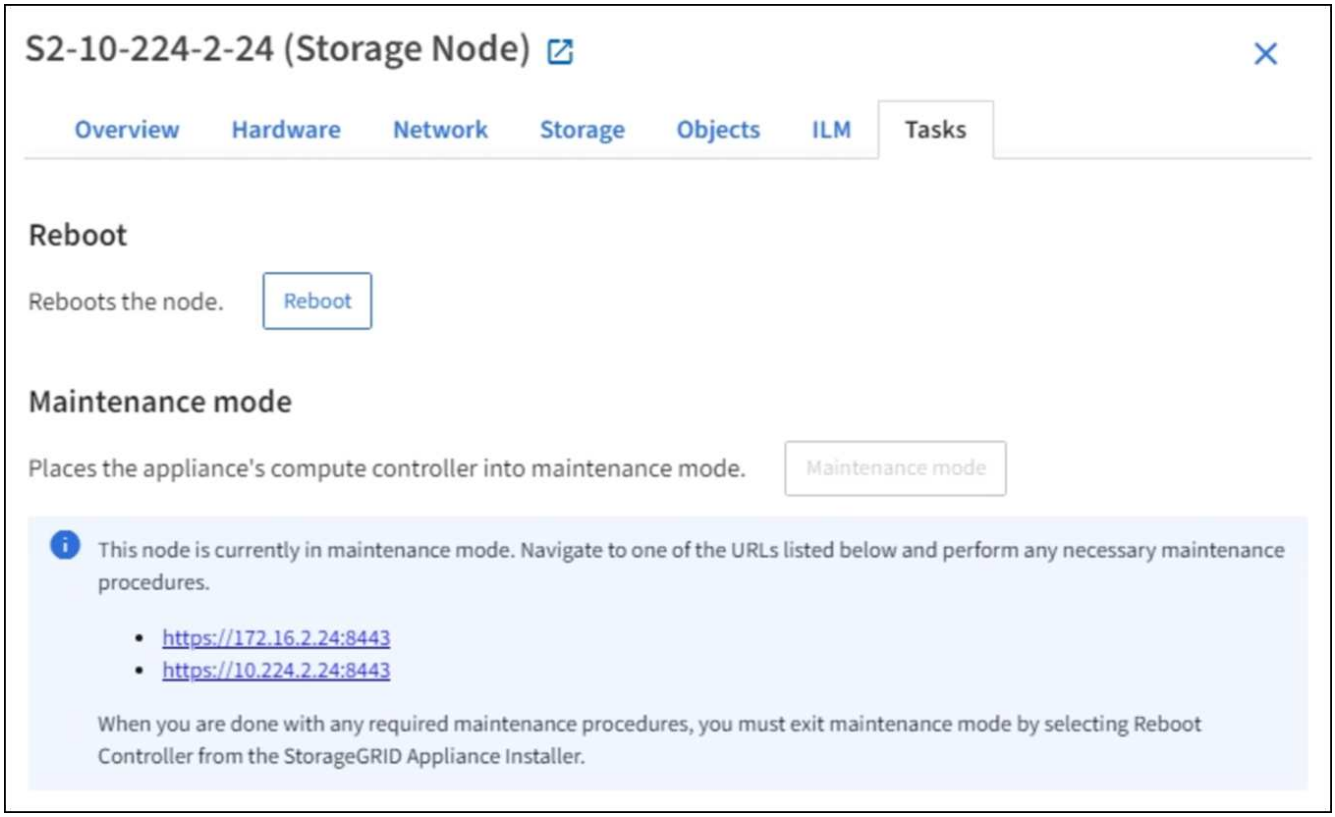


5. Introduzca la contraseña de aprovisionamiento y seleccione **Aceptar**.

   Una barra de progreso y una serie de mensajes, incluidos "solicitud enviada", "detención de StorageGRID" y "reinicio", indican que el dispositivo está llevando a cabo los pasos necesarios para entrar en el modo de mantenimiento.



   Cuando el dispositivo se encuentra en modo de mantenimiento, un mensaje de confirmación enumera las URL que puede utilizar para acceder al instalador de dispositivos de StorageGRID.



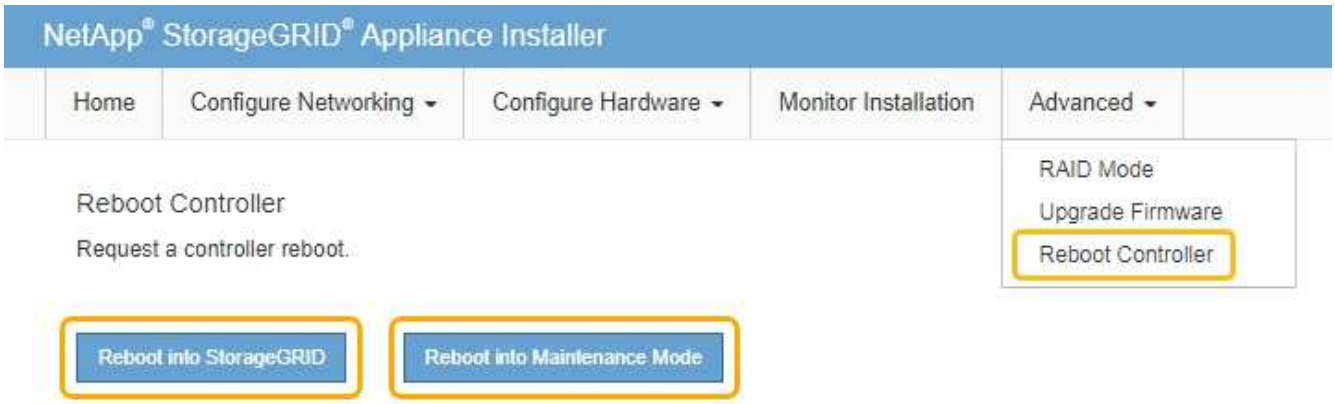
6. Para acceder al instalador de dispositivos de StorageGRID, busque cualquiera de las direcciones URL que se muestren.

   Si es posible, utilice la dirección URL que contiene la dirección IP del puerto de red de administración del dispositivo.

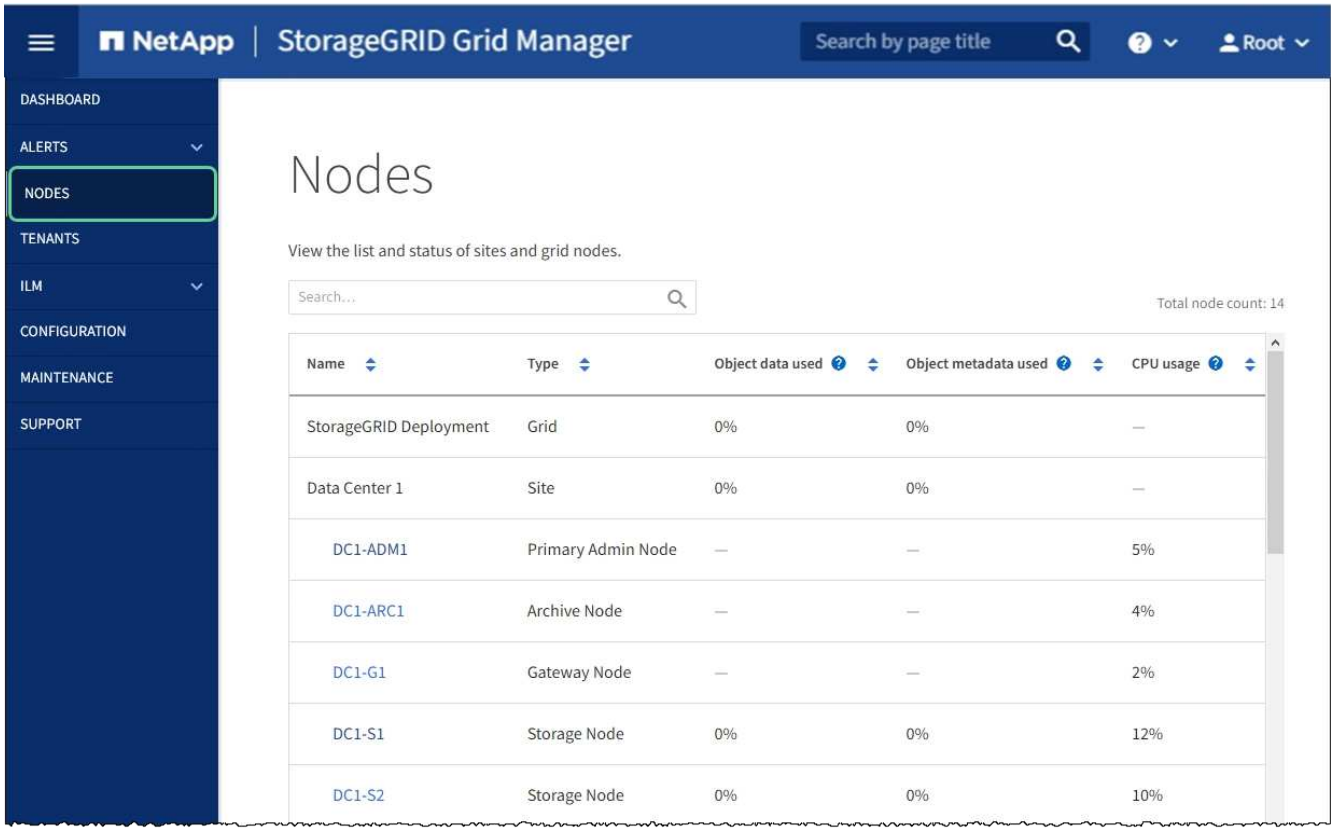
   > Si tiene una conexión directa con el puerto de gestión del dispositivo, utilice `https://169.254.0.1:8443` Para acceder a la página del instalador de dispositivos de StorageGRID.

7. En el instalador de dispositivos StorageGRID, confirme que el dispositivo está en modo de mantenimiento.

8. Realice las tareas de mantenimiento necesarias.
9. Después de completar las tareas de mantenimiento, salga del modo de mantenimiento y reanude el funcionamiento normal del nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione **Reiniciar en StorageGRID**.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Actualizar el sistema operativo SANtricity en la controladora de almacenamiento

Para garantizar el funcionamiento óptimo de la controladora de almacenamiento, debe actualizarse a la versión de mantenimiento más reciente del sistema operativo SANtricity que esté cualificado para su dispositivo StorageGRID. Consulte la herramienta de matriz de interoperabilidad de NetApp (IMT) para determinar qué versión debe utilizar. Si necesita ayuda, póngase en contacto con el soporte técnico.

- Si la controladora de almacenamiento utiliza el sistema operativo SANtricity 08.42.20.00 (11.42) o una versión posterior, use Grid Manager para llevar a cabo la actualización.

  Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante Grid Manager

- Si la controladora de almacenamiento utiliza una versión de sistema operativo SANtricity anterior a 08.42.20.00 (11.42), use el modo de mantenimiento para realizar la actualización.

  Actualice el sistema operativo SANtricity en la controladora E2800 mediante modo de mantenimiento

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

"Descargas de NetApp: Dispositivo de StorageGRID"

Supervisión y solución de problemas

Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante Grid Manager

Para aplicar una actualización, se deben usar Grid Manager para las controladoras de almacenamiento que actualmente utilizan SANtricity OS 08.42.20.00 (11.42) o posterior.

Lo que necesitará

- Ha consultado con la herramienta de matriz de interoperabilidad (IMT) de NetApp para confirmar que la versión del sistema operativo SANtricity que utiliza para la actualización es compatible con su dispositivo.
- Tiene el permiso de mantenimiento o acceso raíz.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene la clave de acceso de aprovisionamiento.
- Tiene acceso a la página de descargas de NetApp para SANtricity OS.

Acerca de esta tarea

No puede realizar otras actualizaciones de software (actualización de software StorageGRID o revisión) hasta que haya completado el proceso de actualización de sistema operativo SANtricity. Si intenta iniciar una revisión o una actualización de software de StorageGRID antes de que haya finalizado el proceso de actualización de SANtricity OS, se le redirigirá a la página de actualización de SANtricity OS.

No se completará el procedimiento hasta que la actualización del sistema operativo SANtricity se haya aplicado correctamente a todos los nodos aplicables seleccionados para la actualización. Es posible que tardar más de 30 minutos cargar el sistema operativo SANtricity en cada nodo (de forma secuencial) y hasta 90 minutos para reiniciar cada dispositivo de almacenamiento StorageGRID.

> Los siguientes pasos sólo son aplicables cuando se utiliza Grid Manager para realizar la actualización. No es posible actualizar las controladoras de almacenamiento en el dispositivo mediante Grid Manager cuando las controladoras utilizan SANtricity OS anteriores a 08.42.20.00 (11.42).

> Este procedimiento actualizará automáticamente la NVSRAM a la versión más reciente asociada con la actualización del sistema operativo SANtricity. No es necesario aplicar un archivo de actualización de NVSRAM aparte.

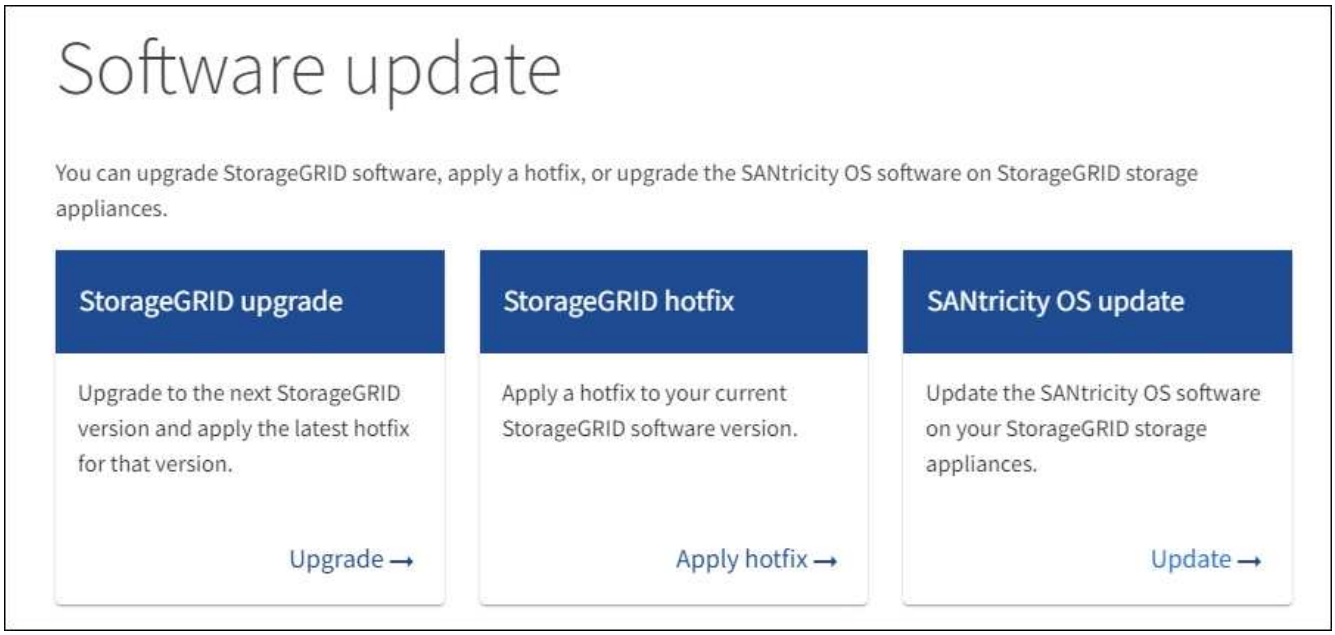
Pasos

1. Descargar el nuevo archivo de software de sistema operativo SANtricity del sitio de soporte de NetApp.

   Asegúrese de elegir la versión de sistema operativo SANtricity para las controladoras de almacenamiento.

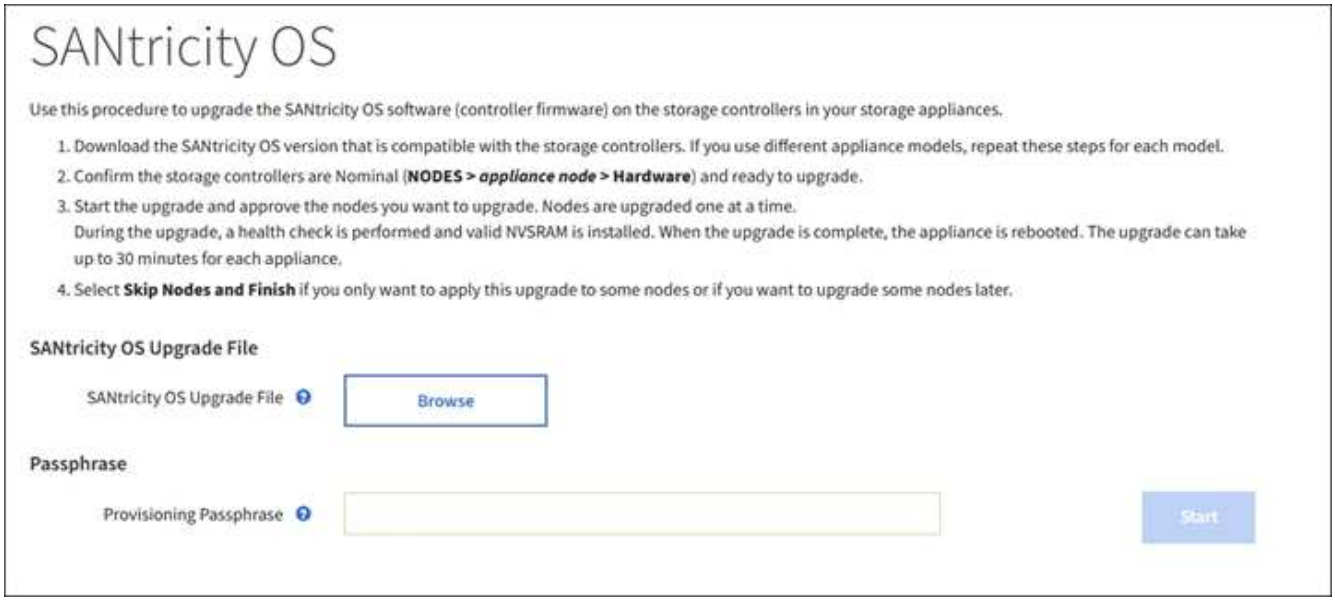
   "Descargas de NetApp: Dispositivo de StorageGRID"

2. Seleccione **MANTENIMIENTO** > **sistema** > **actualización de software**.



3. En la sección actualización del sistema operativo SANtricity, seleccione **Actualizar**.

   Se muestra la página actualización de sistema operativo SANtricity.



4. Seleccione el archivo de actualización del sistema operativo SANtricity que descargó del sitio de soporte de NetApp.

   a. Seleccione **examinar**.

   b. Localice y seleccione el archivo.

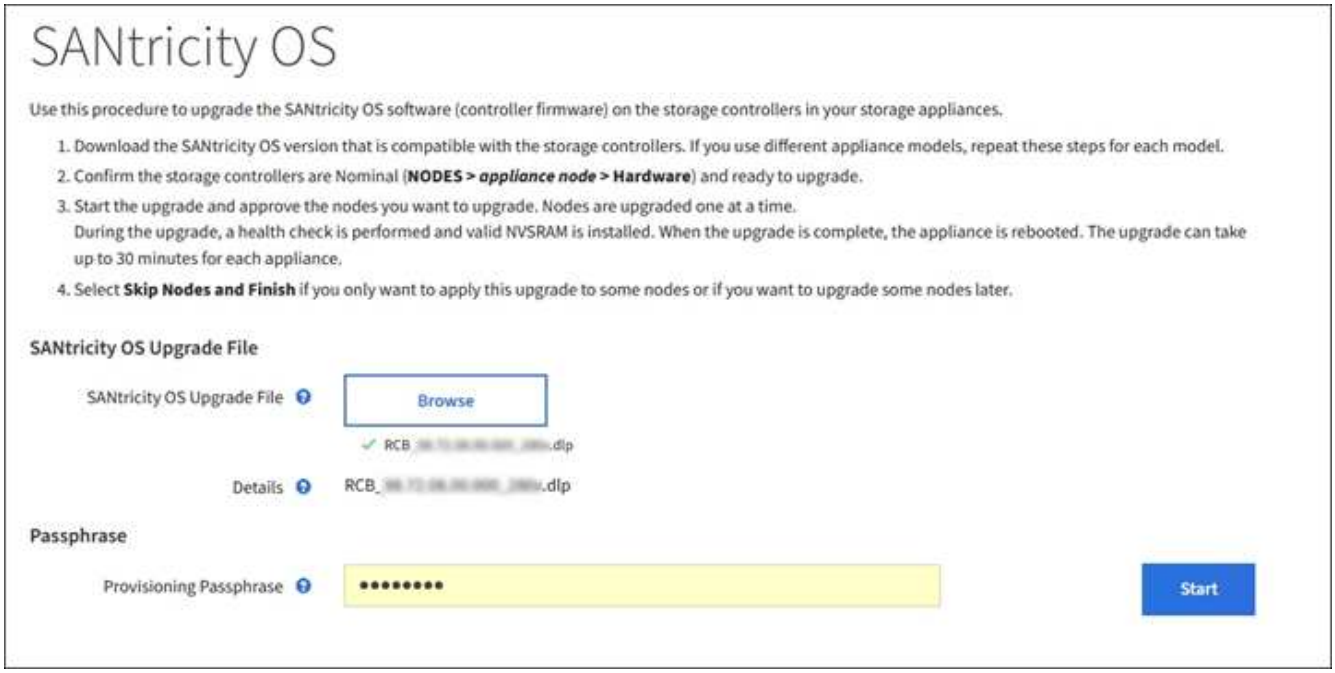
c. Seleccione **Abrir**.

El archivo se carga y se valida. Cuando se realiza el proceso de validación, se muestra el nombre del archivo junto al botón **examinar**.

> No cambie el nombre del archivo ya que forma parte del proceso de verificación.

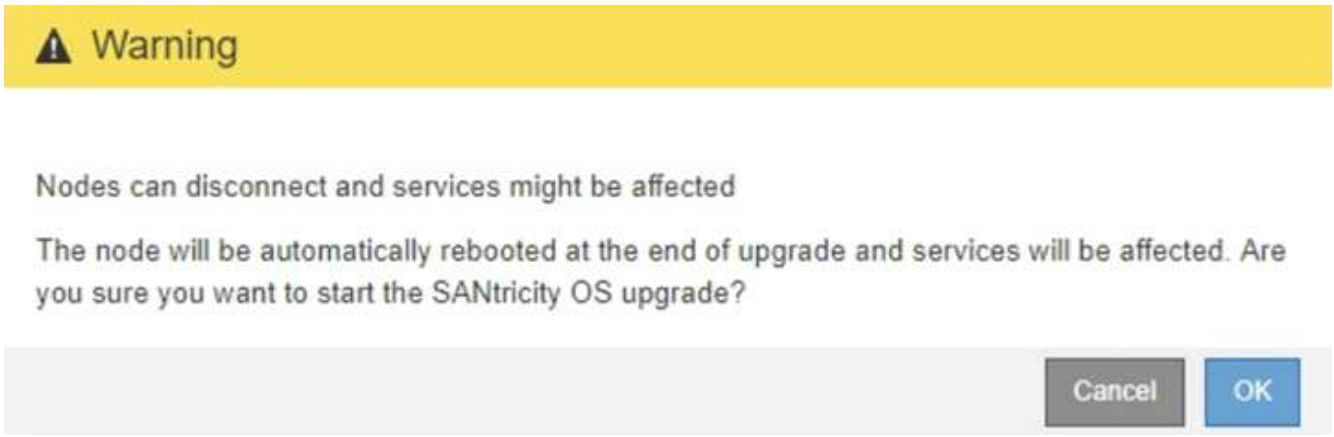
5. Introduzca la clave de acceso de aprovisionamiento.

El botón **Iniciar** está activado.



6. Seleccione **Iniciar**.

Aparece un cuadro de advertencia que indica que es posible que se pierda temporalmente la conexión del explorador como se reinician los servicios de los nodos actualizados.



7. Seleccione **Aceptar** para almacenar el archivo de actualización del sistema operativo SANtricity en el nodo de administración principal.

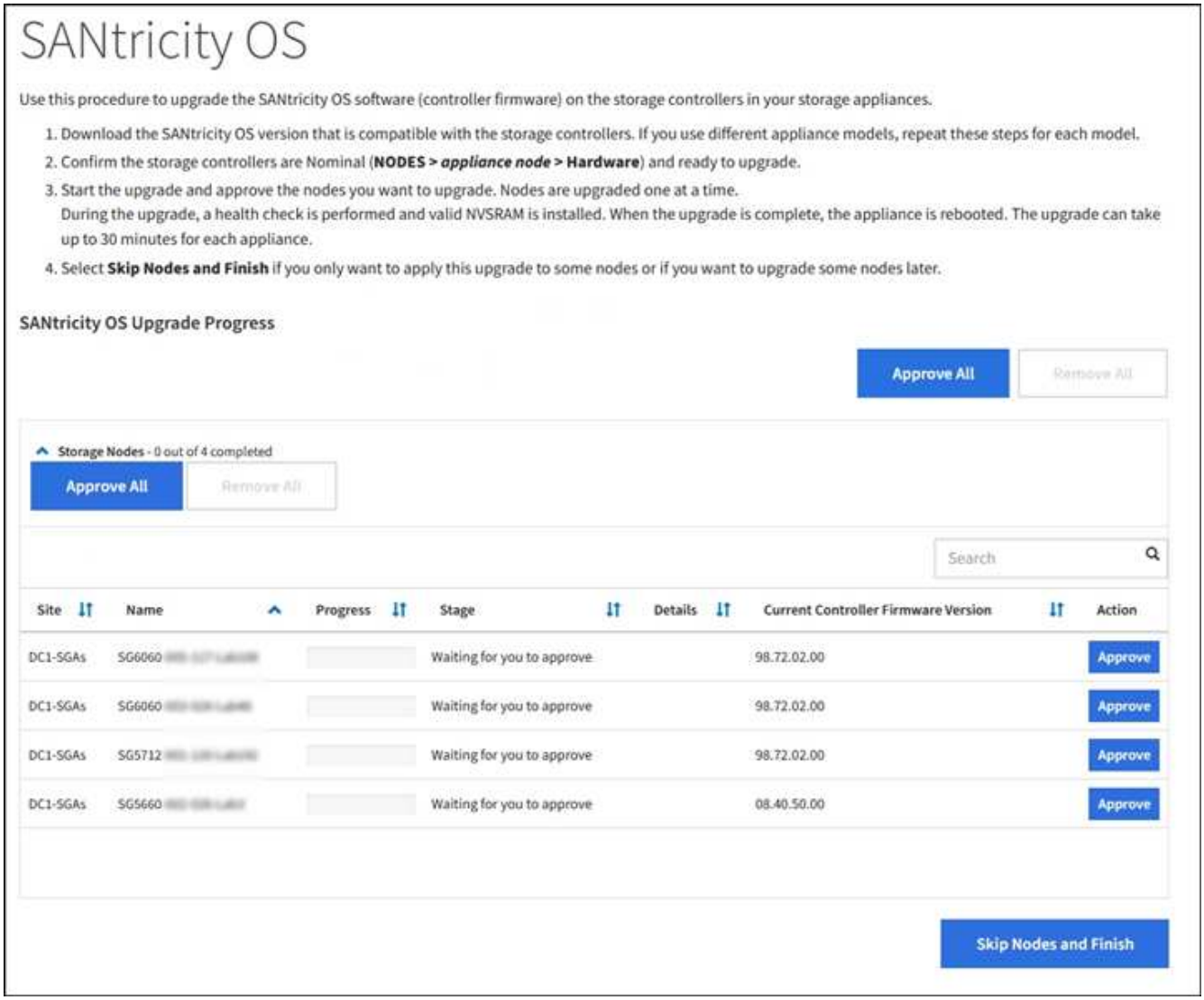
Cuando se inicia la actualización del sistema operativo SANtricity:

a. Se ejecuta la comprobación del estado. Este proceso comprueba que ningún nodo tenga el estado de necesita atención.

> Si se informa de algún error, solucione y seleccione **Iniciar** de nuevo.

b. Se muestra la tabla progreso de actualización de sistema operativo SANtricity. En esta tabla se muestran todos los nodos de almacenamiento del grid y la fase actual de la actualización de cada nodo.

> La tabla muestra todos los nodos de almacenamiento del dispositivo. No se muestran los nodos de almacenamiento basados en software. Seleccione **aprobar** para todos los nodos que requieran la actualización.



8. Opcionalmente, ordene la lista de nodos en orden ascendente o descendente por **Sitio**, **Nombre**, **progreso**, **etapa**, **Detalles**, O **Versión actual del firmware de la controladora**. O bien, introduzca un término en el cuadro **Buscar** para buscar nodos específicos.

   Puede desplazarse por la lista de nodos utilizando las flechas izquierda y derecha de la esquina inferior derecha de la sección.

9. Apruebe los nodos de cuadrícula que está listo para agregar a la cola de actualización. Los nodos aprobados del mismo tipo se actualizan de uno en uno.

> No apruebe la actualización de SANtricity OS para un nodo de almacenamiento de dispositivos a menos que esté seguro de que el nodo esté listo para detenerse y reiniciar. Cuando la actualización de SANtricity OS se aprueba en un nodo, los servicios de ese nodo se detienen y comienza el proceso de actualización. Más tarde, cuando el nodo finaliza la actualización, el nodo del dispositivo se reinicia. Estas operaciones pueden provocar interrupciones del servicio en los clientes que se comunican con el nodo.

   - Seleccione uno de los botones **aprobar todo** para agregar todos los nodos de almacenamiento a la cola de actualización de SANtricity OS.

     > 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 uno o más botones **aprobar** para agregar uno o más nodos a la cola de actualización de SANtricity OS.

     Después de seleccionar **aprobar**, el proceso de actualización determina si se puede actualizar el nodo. Si se puede actualizar un nodo, se agrega a la cola de actualización.

   En algunos nodos, el archivo de actualización seleccionado no se aplica de forma intencional, y se puede completar el proceso de actualización sin actualizar estos nodos específicos. Los nodos no actualizados intencionalmente muestran una etapa de completado (intento de actualización) y muestran el motivo por el que el nodo no se actualizó en la columna Details.

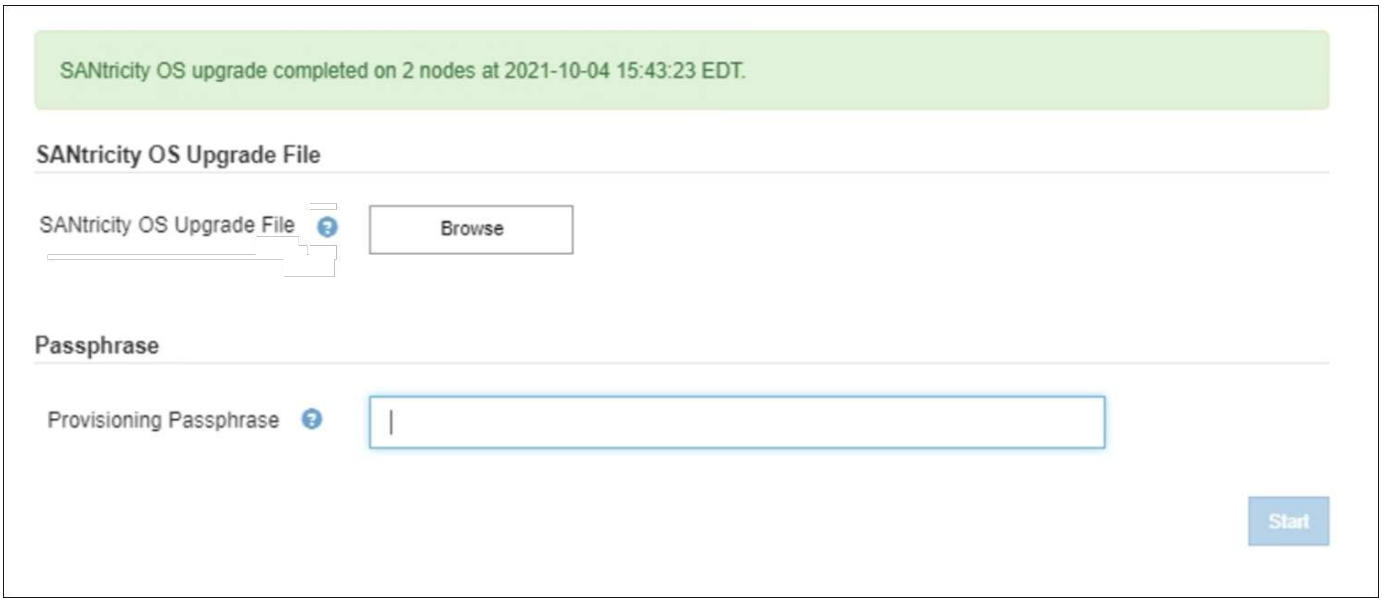
10. Si necesita eliminar un nodo o todos los nodos de la cola de actualización de SANtricity OS, seleccione **Quitar** o **Quitar todo**.

    Cuando la etapa avanza más allá de la cola, el botón **Quitar** está oculto y ya no puede quitar el nodo del proceso de actualización de SANtricity OS.

11. Espere mientras la actualización del SO SANtricity se aplica a cada nodo de grid aprobado.

    - Si alguno de los nodos muestra una etapa de error mientras se aplica la actualización del sistema operativo SANtricity, se produjo un error en la actualización del nodo. Con la ayuda del soporte técnico, es posible que deba colocar el dispositivo en modo de mantenimiento para recuperarlo.
    - Si el firmware del nodo es demasiado antiguo para actualizarse con Grid Manager, el nodo muestra una etapa de error con los detalles: "'debe utilizar el modo de mantenimiento para actualizar SANtricity OS en este nodo. Consulte las instrucciones de instalación y mantenimiento del aparato. Tras la actualización, puede utilizar esta utilidad para futuras actualizaciones». Para resolver el error, haga lo siguiente:
      i. Utilice el modo de mantenimiento para actualizar SANtricity OS en el nodo que muestre una etapa de error.
      ii. Utilice el Administrador de grid para reiniciar y completar la actualización de SANtricity OS.

    Una vez completada la actualización de SANtricity OS en todos los nodos aprobados, la tabla de progreso de la actualización de SANtricity OS se cierra y un banner verde muestra la fecha y la hora en que se completó la actualización de SANtricity OS.



1. Si no se puede actualizar un nodo, tenga en cuenta el motivo que se muestra en la columna Details y realice la acción adecuada:
   - «Ya se ha actualizado el nodo de almacenamiento». No es necesario realizar ninguna otra acción.
   - «'la actualización de SANtricity OS no es aplicable a este nodo». El nodo no tiene una controladora de almacenamiento que pueda gestionar el sistema StorageGRID. Complete el proceso de actualización sin actualizar el nodo que muestra este mensaje.
   - «'el archivo del sistema operativo SANtricity no es compatible con este nodo». El nodo requiere un archivo de SANtricity OS diferente al que seleccionó. Después de completar la actualización actual, descargue el archivo de sistema operativo SANtricity correcto para el nodo y repita el proceso de actualización.

> El proceso de actualización del sistema operativo SANtricity no se completará hasta que apruebe la actualización del sistema operativo SANtricity en todos los nodos de almacenamiento enumerados.

1. Si desea finalizar la aprobación de nodos y volver a la página de SANtricity OS para permitir la carga de un nuevo archivo de SANtricity OS, haga lo siguiente:
   a. Seleccione **Omitir nodos y Finalizar**.

      Aparece una advertencia en la que se pregunta si está seguro de que desea finalizar el proceso de actualización sin actualizar todos los nodos.

   b. Seleccione **Aceptar** para volver a la página **SANtricity OS**.
   c. Cuando esté listo para continuar aprobando nodos, vaya a. Descargue el sistema operativo SANtricity para reiniciar el proceso de actualización.

   > Los nodos ya aprobados y actualizados sin errores siguen actualizando.

2. Repita este procedimiento de actualización para todos los nodos con una etapa de finalización que requieran un archivo de actualización de sistema operativo SANtricity diferente.

   > Para cualquier nodo con el estado necesita atención, utilice el modo de mantenimiento para realizar la actualización.

> Cuando repita el procedimiento de actualización, deberá aprobar los nodos actualizados anteriormente.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Actualice el sistema operativo SANtricity en la controladora E2800 mediante modo de mantenimiento

Actualice el sistema operativo SANtricity en la controladora E2800 mediante modo de mantenimiento

Para las controladoras de almacenamiento que utilizan actualmente el sistema operativo SANtricity con una versión anterior a 08.42.20.00 (11.42), debe utilizar el procedimiento del modo de mantenimiento para aplicar una actualización.

Lo que necesitará

- Ha consultado con la herramienta de matriz de interoperabilidad (IMT) de NetApp para confirmar que la versión del sistema operativo SANtricity que utiliza para la actualización es compatible con su dispositivo.
- Debe colocar la controladora E5700SG en modo de mantenimiento, Que interrumpe la conexión a la controladora E2800.

> En raras ocasiones, una vez que se coloca un dispositivo StorageGRID en modo de mantenimiento puede hacer que el dispositivo no esté disponible para el acceso remoto.

Acerca de esta tarea

No actualice el sistema operativo SANtricity ni NVSRAM en la controladora E-Series en más de un dispositivo StorageGRID a la vez.

> Actualizar más de un dispositivo StorageGRID a la vez puede provocar la falta de disponibilidad de los datos, según el modelo de puesta en marcha y las políticas de ILM.

Pasos

1. Confirme que el aparato está en modo de mantenimiento.
2. Desde un ordenador portátil de servicio, acceda a SANtricity System Manager e inicie sesión.
3. Descargue el nuevo archivo de NVSRAM y de software de sistema operativo SANtricity en el cliente de gestión.

   > La NVSRAM es específica del dispositivo StorageGRID. No use la descarga estándar de NVSRAM.

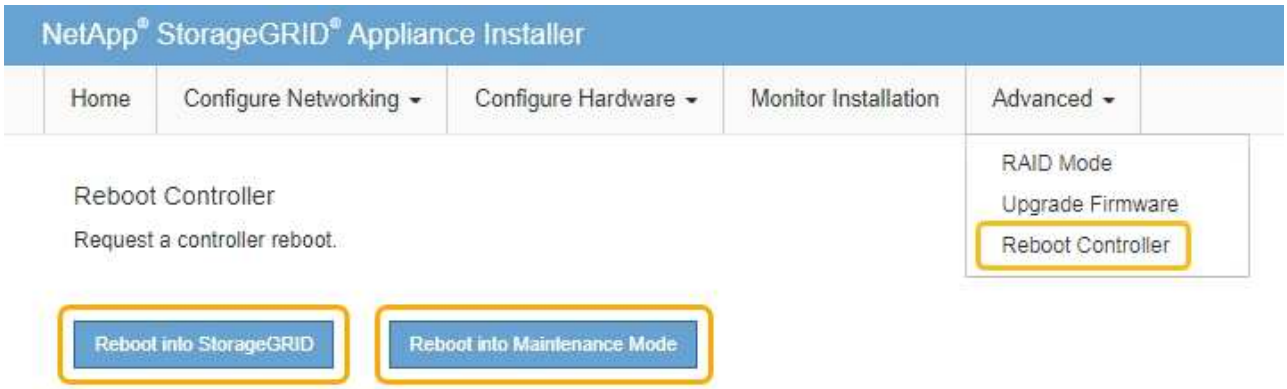
4. Siga las instrucciones de la Guía de actualización de software y firmware SANtricity *E2800 y E5700* o la ayuda en línea de System Manager de SANtricity para actualizar el firmware y NVSRAM de la controladora E2800.

   > Active los archivos de actualización inmediatamente. No aplace la activación.

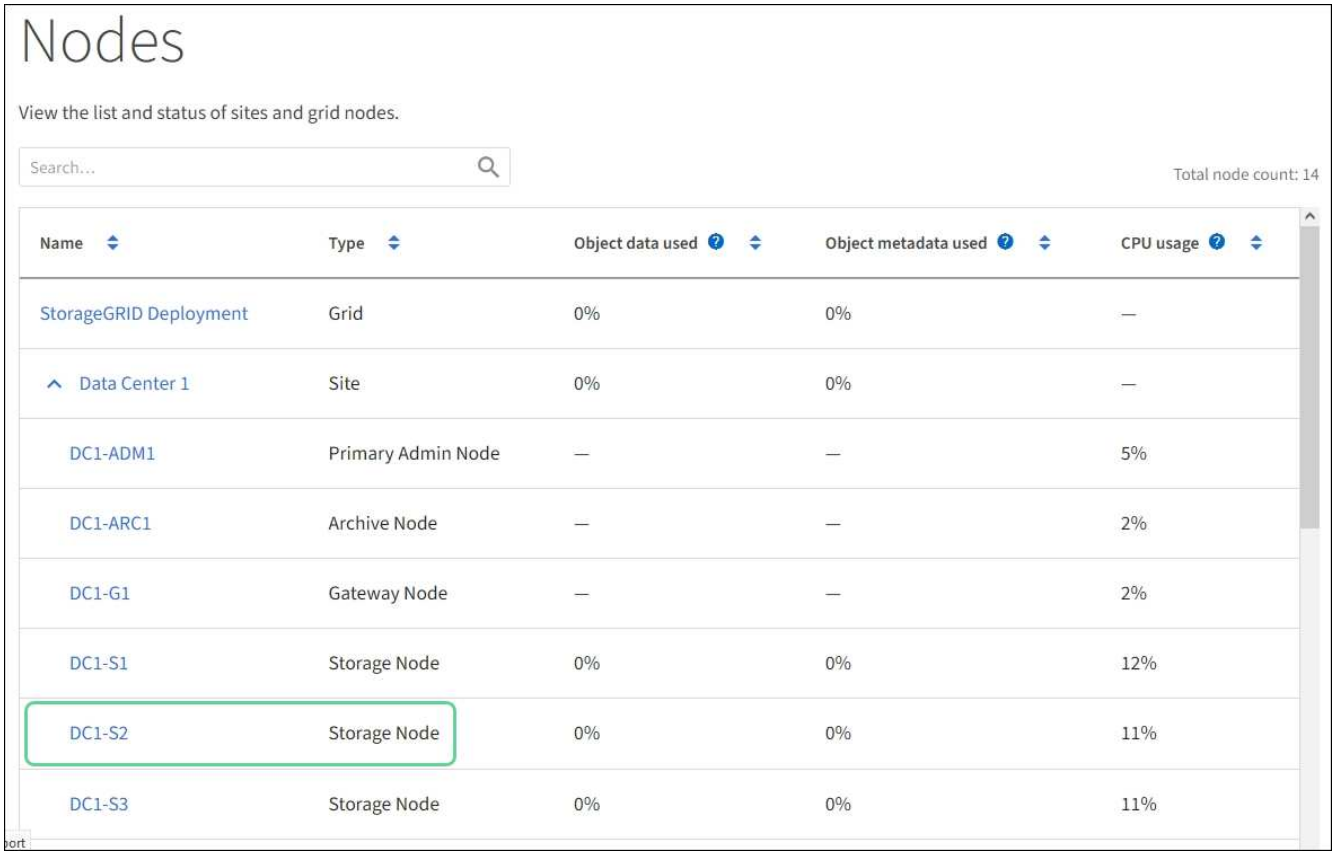
5. Si este procedimiento se completó correctamente y tiene procedimientos adicionales que realizar mientras el nodo se encuentra en modo de mantenimiento, realice ahora. Cuando haya terminado, o si ha experimentado algún fallo y desea volver a empezar, seleccione **Avanzado** > **Reiniciar controlador** y, a

continuación, seleccione una de estas opciones:

- Seleccione **Reiniciar en StorageGRID**
- Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. Seleccione esta opción si ha experimentado algún error durante el procedimiento y desea volver a empezar. Cuando el nodo termine de reiniciarse en el modo de mantenimiento, reinicie desde el paso adecuado del procedimiento en que falló.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página nodos debe mostrar el estado normal (no hay iconos a la izquierda del nombre del nodo) para el nodo de dispositivo, lo que indica que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante Grid Manager

Actualizar el firmware de la unidad mediante System Manager de SANtricity

El firmware de la unidad se actualiza para asegurarse de tener todas las funciones y correcciones de errores más recientes.

Lo que necesitará

- El dispositivo de almacenamiento tiene el estado Optimal.
- Todas las unidades tienen el estado Optimal.
- Tiene instalada la última versión de System Manager de SANtricity que es compatible con la versión de StorageGRID.
- Ya tienes Colocó el dispositivo StorageGRID en modo de mantenimiento.

> El modo de mantenimiento interrumpe la conexión a la controladora de almacenamiento, al detener toda la actividad de I/o y colocar todas las unidades en estado sin conexión.

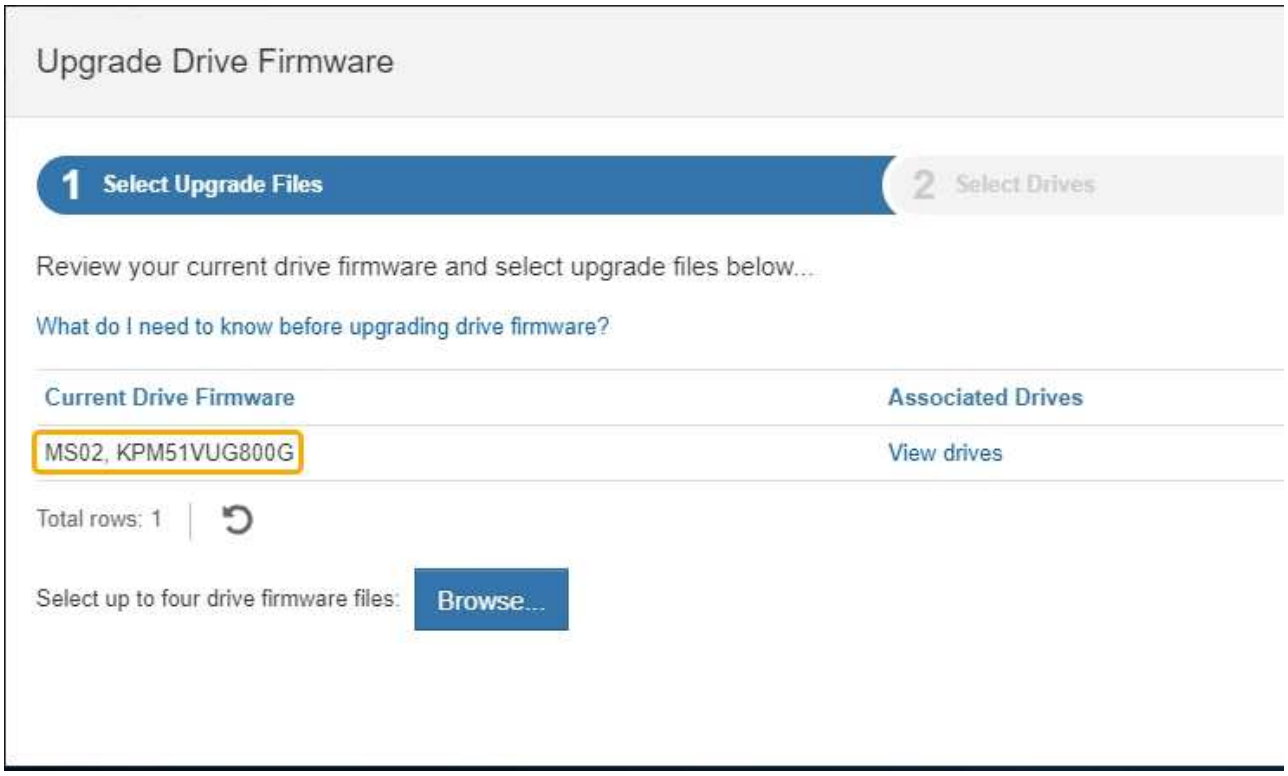
> No actualice el firmware de la unidad en más de un dispositivo StorageGRID a la vez. Si lo hace, puede provocar la falta de disponibilidad de los datos, según el modelo de puesta en marcha y las políticas de ILM.

Pasos

1. Confirme que el aparato está en modo de mantenimiento.
2. Acceda a System Manager de SANtricity mediante uno de estos métodos:
   - Utilice el instalador del dispositivo StorageGRID y seleccione **Avanzado** > **Administrador del sistema SANtricity**
   - Utilice SANtricity System Manager para acceder a la dirección IP de la controladora de almacenamiento:
     `https://Storage_Controller_IP`
3. Si es necesario, introduzca el nombre de usuario y la contraseña del administrador del sistema SANtricity.
4. Compruebe la versión de firmware de la unidad instalada actualmente en el dispositivo de almacenamiento:
   a. En el Administrador del sistema de SANtricity, seleccione **SOPORTE** > **Centro de actualización**.
   b. En actualización del firmware de la unidad, seleccione **Iniciar actualización**.

      El firmware de la unidad de actualización muestra los archivos de firmware de la unidad instalados actualmente.

   c. Tenga en cuenta las revisiones de firmware de la unidad actuales y los identificadores de unidades en la columna firmware de la unidad actual.



En este ejemplo:

- La revisión del firmware de la unidad es **MS02**.
- El identificador de la unidad es **KPM51VUG800G**.

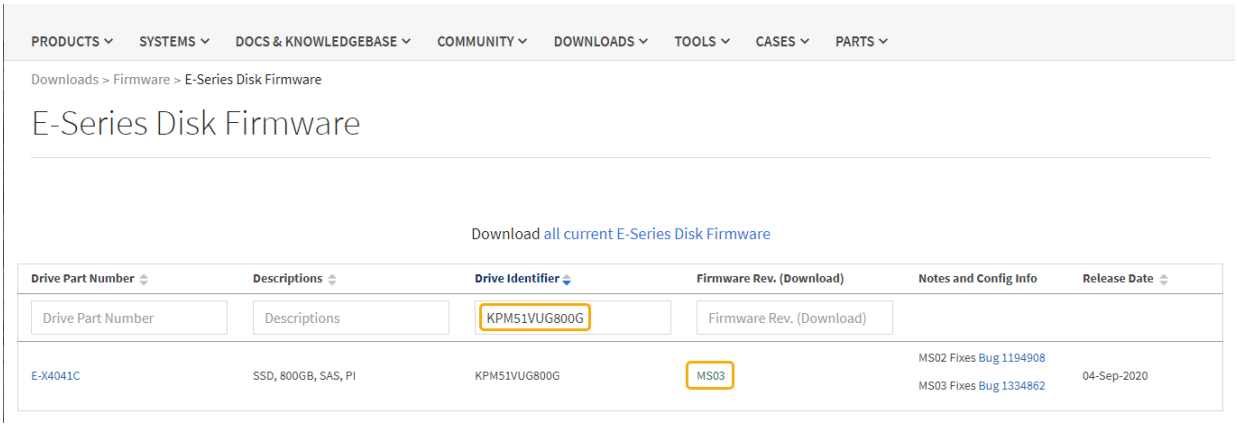
Seleccione **Ver unidades** en la columna unidades asociadas para mostrar dónde están instaladas estas unidades en el dispositivo de almacenamiento.

a. Cierre la ventana Actualizar firmware de la unidad.

5. Descargue y prepare la actualización del firmware de la unidad disponible:
   a. En actualización del firmware de la unidad, seleccione **Soporte de NetApp**.
   b. En el sitio de soporte de NetApp, seleccione la pestaña **Descargas** y, a continuación, seleccione **firmware de las unidades de disco E-Series**.

      Se muestra la página firmware del disco E-Series.

   c. Busque cada **Identificador de unidad** instalado en el dispositivo de almacenamiento y compruebe que cada identificador de unidad tiene la última revisión de firmware.
      - Si la revisión del firmware no es un enlace, este identificador de unidad tiene la revisión de firmware más reciente.
      - Si se enumeran uno o varios números de pieza de unidad para un identificador de unidad, estas unidades tienen disponible una actualización de firmware. Puede seleccionar cualquier enlace para descargar el archivo de firmware.



d. Si aparece una revisión posterior del firmware, seleccione el enlace en la revisión del firmware (Descargar) para descargar una `.zip` archivo que contiene el archivo de firmware.

e. Extraiga (descomprima) los archivos de almacenamiento del firmware de la unidad que descargó del sitio de soporte.

6. Instale la actualización del firmware de la unidad:

a. En el Administrador del sistema de SANtricity, en actualización del firmware de la unidad, seleccione **comenzar actualización**.

b. Seleccione **examinar** y seleccione los nuevos archivos de firmware de la unidad que descargó del sitio de soporte.

Los archivos de firmware de la unidad tienen un nombre de archivo similar a + `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`

Es posible seleccionar hasta cuatro archivos de firmware de la unidad, uno por vez. Si más de un archivo de firmware de la unidad es compatible con la misma unidad, se muestra un error de conflicto de archivo. Decida qué archivo de firmware de la unidad desea usar para la actualización y elimine el otro.

c. Seleccione **Siguiente**.

Select Drives enumera las unidades que se pueden actualizar con los archivos de firmware seleccionados.

Solo se muestran las unidades que son compatibles.

El firmware seleccionado para la unidad aparece en **firmware propuesto**. Si debe cambiar este firmware, seleccione **Atrás**.

d. Seleccione **actualización sin conexión (paralelo)**.

Es posible usar el método de actualización sin conexión debido a que el dispositivo está en modo de mantenimiento, donde se detiene la actividad de I/o de todas las unidades y todos los volúmenes.

> No continúe a menos que esté seguro de que el aparato está en modo de mantenimiento. Si no se coloca el dispositivo en modo de mantenimiento antes de iniciar una actualización del firmware de la unidad sin conexión, se pueden perder datos.

e. En la primera columna de la tabla, seleccione la o las unidades que desea actualizar.

La práctica recomendada es actualizar todas las unidades del mismo modelo a la misma revisión de firmware.

f. Seleccione **Inicio** y confirme que desea realizar la actualización.

Si necesita detener la actualización, seleccione **Detener**. Se completa cualquier descarga de firmware actualmente en curso. Se cancela cualquier descarga de firmware que no haya comenzado.

> Si se detiene la actualización del firmware de la unidad, podrían producirse la pérdida de datos o la falta de disponibilidad de las unidades.

g. (Opcional) para ver una lista de los elementos actualizados, seleccione **Guardar registro**.

El archivo de registro se guarda en la carpeta de descargas del explorador con el nombre `latest-upgrade-log-timestamp.txt`.

Si se produce alguno de los siguientes errores durante el procedimiento de actualización, realice la acción recomendada.

- **Unidades asignadas con errores**

  La causa de este error puede ser que la unidad no tenga la firma apropiada. Asegúrese de que la unidad afectada sea una unidad autorizada. Póngase en contacto con el soporte técnico para obtener más información.

Al reemplazar una unidad, asegúrese de que la capacidad de la unidad de reemplazo sea igual o mayor que la de la unidad con error que desea reemplazar.

Puede reemplazar la unidad con error mientras la cabina de almacenamiento recibe I/O.

- **Compruebe la matriz de almacenamiento**
  - Asegúrese de que se haya asignado una dirección IP a cada controladora.
  - Asegúrese de que ninguno de los cables conectados a la controladora esté dañado.
  - Asegúrese de que todos los cables estén conectados firmemente.
- **Unidades de repuesto en caliente integradas**

  Es necesario corregir esta condición de error para poder actualizar el firmware.

- **Grupos de volúmenes incompletos**

  Si uno o varios grupos de volúmenes o pools de discos se muestran incompletos, es necesario corregir esta condición de error para poder actualizar el firmware.

- **Operaciones exclusivas (que no sean análisis de medios en segundo plano/paridad) que se estén ejecutando actualmente en cualquier grupo de volúmenes**

  Si existe una o varias operaciones exclusivas en curso, es necesario completarlas para poder actualizar el firmware. Utilice System Manager para supervisar el progreso de las operaciones.

- **Volúmenes que faltan**

  Es necesario corregir la condición de volumen ausente para poder actualizar el firmware.

- **Cualquiera de los controladores en un estado distinto al óptimo**

  Se requiere atención en una de las controladoras de la cabina de almacenamiento. Es necesario corregir esta condición para poder actualizar el firmware.

- **La información de partición de almacenamiento no coincide entre los gráficos de objetos del controlador**

  Se produjo un error durante la validación de los datos en las controladoras. Póngase en contacto con el soporte técnico para resolver este problema.

- **La verificación del controlador de base de datos de SPM falla**

  Se produjo un error en la base de datos de asignación de particiones de almacenamiento de una controladora. Póngase en contacto con el soporte técnico para resolver este problema.

- **Validación de la base de datos de configuración (si es compatible con la versión del controlador de la matriz de almacenamiento)**

  Se produjo un error en la base de datos de configuración de una controladora. Póngase en contacto con el soporte técnico para resolver este problema.

- **Comprobaciones relacionadas con MEL**

  Póngase en contacto con el soporte técnico para resolver este problema.

- **Se notificaron más de 10 eventos críticos MEL o informativos DDE en los últimos 7 días**

  Póngase en contacto con el soporte técnico para resolver este problema.

- **Se notificaron más de 2 Eventos críticos MEL de página 2C en los últimos 7 días**

  Póngase en contacto con el soporte técnico para resolver este problema.

- **Se notificaron más de 2 eventos críticos MEL del canal de unidad degradado en los últimos 7 días**

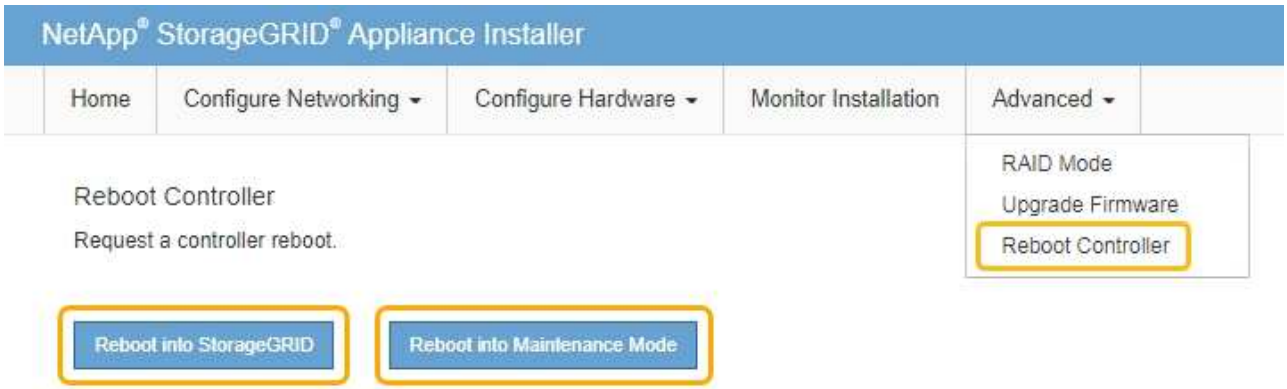
  Póngase en contacto con el soporte técnico para resolver este problema.

- * Más de 4 entradas cruciales MEL en los últimos 7 días*

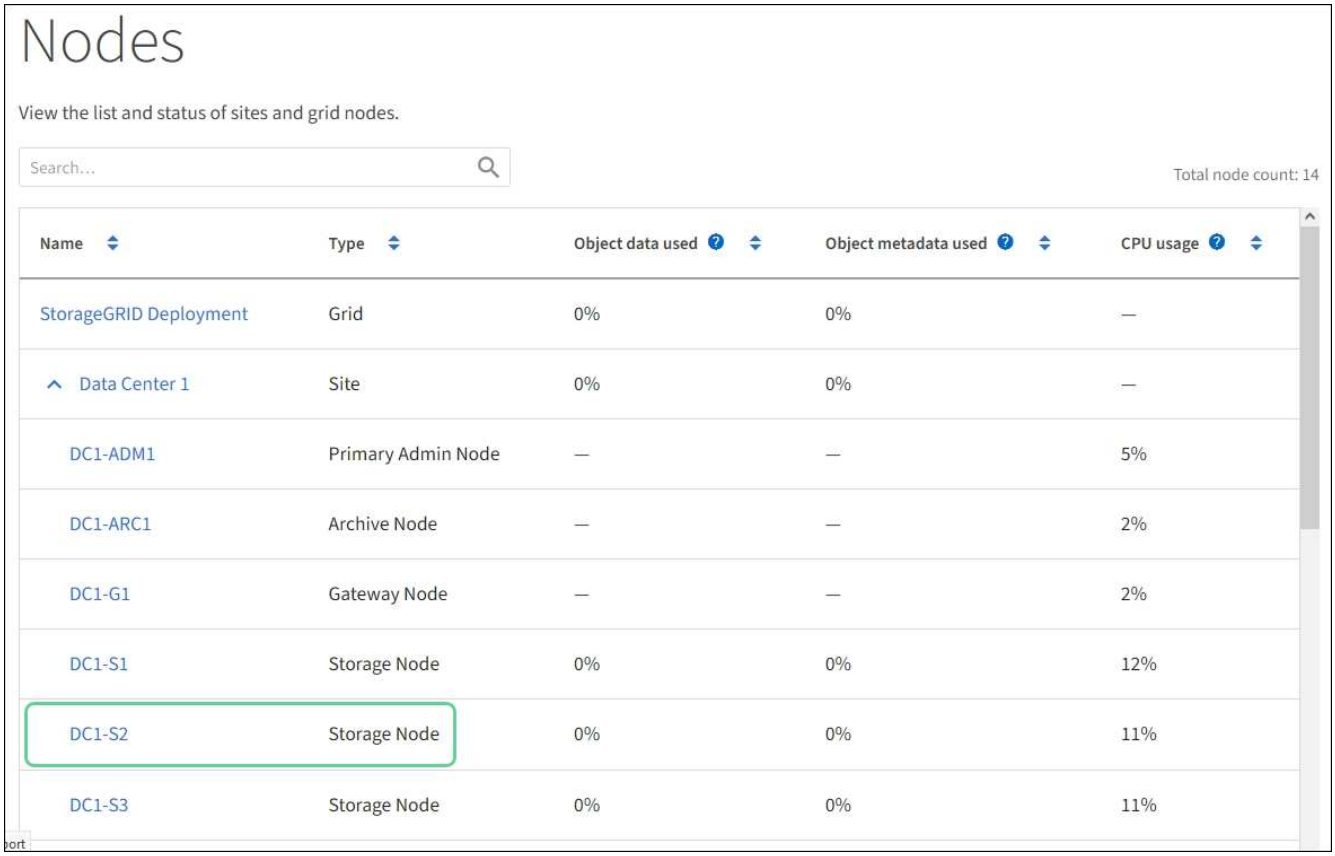
  Póngase en contacto con el soporte técnico para resolver este problema.

7. . Si este procedimiento se completó correctamente y tiene procedimientos adicionales que realizar mientras el nodo se encuentra en modo de mantenimiento, realice ahora. Cuando haya terminado, o si ha experimentado algún fallo y desea volver a empezar, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID**
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. Seleccione esta opción si ha experimentado algún error durante el procedimiento y desea volver a empezar. Cuando el nodo termine de reiniciarse en el modo de mantenimiento, reinicie desde el paso adecuado del procedimiento en que falló.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página nodos debe mostrar el estado normal (no hay iconos a la izquierda del nombre del nodo) para el nodo de dispositivo, lo que indica que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Actualice el sistema operativo SANtricity en la controladora de almacenamiento

Sustituye la controladora de almacenamiento de la serie E2800 en SG5700

Es posible que deba sustituir la controladora serie E2800 si no funciona de forma óptima o si ha fallado.

Acerca de esta tarea

- Tiene una controladora de sustitución con el mismo número de pieza que la controladora que desea sustituir.

> No confíe en las instrucciones de E-Series para sustituir una controladora en el dispositivo StorageGRID, ya que los procedimientos no son los mismos.

- Tiene etiquetas para identificar cada cable conectado a la controladora.
- Si todas las unidades están protegidas, debe revisar los pasos del procedimiento de reemplazo de controladora serie E2800 simple, Las cuales incluyen descargar e instalar E-Series SANtricity Storage Manager desde el sitio de soporte de NetApp y, a continuación, utilizar Enterprise Management Window (EMW) para desbloquear las unidades seguras después de reemplazar la controladora.

> No podrá utilizar el aparato hasta que desbloquee las unidades con la tecla guardada.

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

Acerca de esta tarea

Puede determinar si tiene un contenedor de controladora con errores de dos maneras:

- Recovery Guru en System Manager de SANtricity le dirige al usuario reemplazar la controladora.
- El LED de alerta ámbar del controlador está encendido, lo que indica que el controlador tiene un fallo.

No se podrá acceder al nodo de almacenamiento del dispositivo cuando se sustituye la controladora. Si la controladora de la serie E2800 funciona lo suficiente, puede hacerlo Coloque la controladora E5700SG en modo de mantenimiento.

Al sustituir una controladora, debe quitar la batería de la controladora original e instalarla en la controladora de reemplazo. En algunos casos, es posible que también necesite quitar la tarjeta de interfaz del host de la controladora original e instalarla en la controladora de reemplazo.

> En la mayoría de los modelos de dispositivos, las controladoras de almacenamiento no incluyen tarjetas de interfaz del host (HIC).

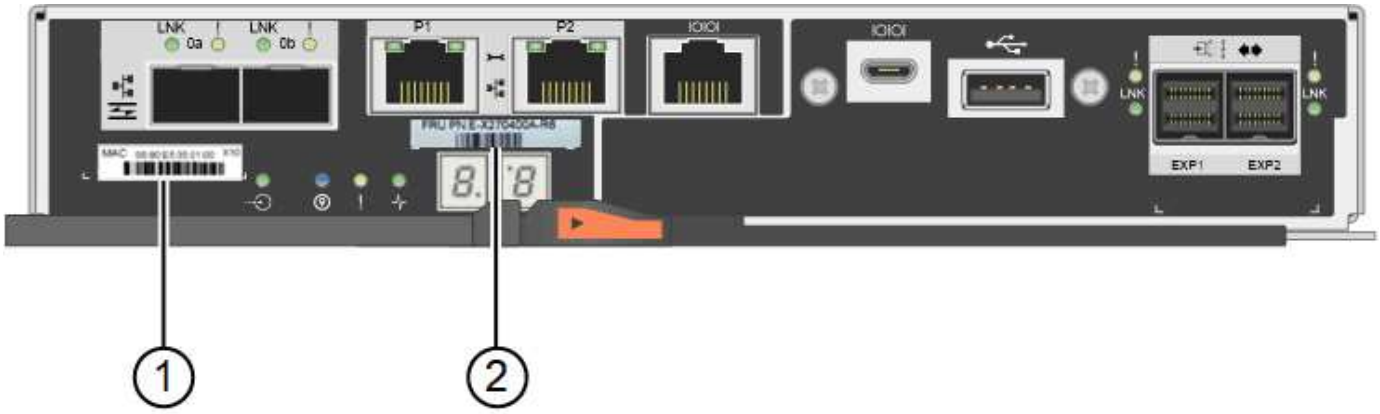
Esta tarea consta de las siguientes partes:

1. Prepare
2. Desconectar la controladora
3. Quite la controladora
4. Mueva la batería a la nueva controladora
5. Si es necesario, mueva HIC a una nueva controladora
6. Sustituya la controladora

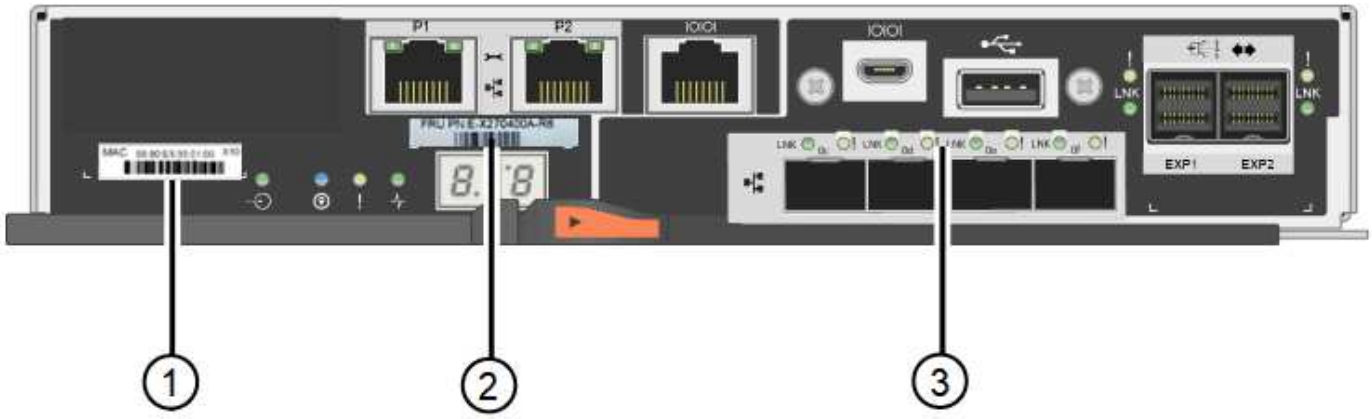
Prepare

Estas figuras muestran la controladora E2800A y la controladora E2800B. El procedimiento para sustituir las controladoras de la serie E2800 y la controladora EF570 es idéntico.

E2800A Storage Controller



E2800B Storage Controller



Etiqueta	componente	Descripción
1	Dirección MAC	La dirección MAC para el puerto de gestión 1 ("'P1 en el E2800A y 0a en la E2800B'"). Si utilizó DHCP para obtener la dirección IP de la controladora original, necesitará esta dirección para conectarse a la nueva controladora.
2	Número de pieza de FRU	El número de pieza de FRU. Este número debe coincidir con el número de pieza de repuesto de la controladora instalada actualmente.
3	HIC de 4 puertos	La tarjeta de interfaz del host (HIC) de 4 puertos. Esta tarjeta se debe mover al nuevo controlador cuando realice la sustitución. **Nota**: El controlador E2800A no tiene HIC.

Pasos

1. Siga las instrucciones del procedimiento de reemplazo de controladora E2800 para preparar la extracción de la controladora.

   SANtricity System Manager se utiliza para realizar estos pasos.

a. Anote en qué versión del software de sistema operativo SANtricity está instalada actualmente en la controladora.

b. Anote en qué versión de NVSRAM está instalada actualmente.

c. Si la función Drive Security está habilitada, asegúrese de que existe una clave guardada y de que conoce la frase de contraseña necesaria para instalarla.

> **Posible pérdida de acceso a datos y#8212;** Si todas las unidades del dispositivo tienen la seguridad habilitada, el nuevo controlador no podrá acceder al dispositivo hasta que desbloquee las unidades seguras mediante la ventana de administración empresarial de SANtricity Storage Manager.

d. Realice un backup de la base de datos de configuración.

   Si se produce un problema al quitar una controladora, puede usar el archivo guardado para restaurar la configuración.

e. Recopile datos de soporte del dispositivo.

> La recogida de datos de soporte antes y después de reemplazar un componente garantiza que se pueda enviar un conjunto completo de registros al soporte técnico en caso de que el reemplazo no resuelva el problema.

Desconectar la controladora

Pasos

1. Si el dispositivo StorageGRID se ejecuta en un sistema StorageGRID, Coloque la controladora E5700SG en modo de mantenimiento.
2. Si la controladora E2800 funciona lo suficiente como para permitir un apagado controlado, confirme que todas las operaciones han finalizado.
   a. En la página de inicio del Administrador del sistema de SANtricity, seleccione **Ver operaciones en curso**.
   b. Confirmar que se han completado todas las operaciones.

Quite la controladora

Pasos

1. Retire el controlador del dispositivo:
   a. Coloque una muñequera ESD o tome otras precauciones antiestáticas.
   b. Etiquete los cables y desconecte los cables y SFP.

   > Para evitar un rendimiento degradado, no gire, pliegue, pellizque ni pellizque los cables.

   c. Suelte el controlador del aparato apretando el pestillo del asa de la leva hasta que se suelte y, a continuación, abra el asa de leva a la derecha.
   d. Con dos manos y el mango de la leva, deslice el controlador para sacarlo del aparato.

   > Utilice siempre dos manos para soportar el peso del controlador.

e. Coloque el controlador sobre una superficie plana y sin estática con la cubierta extraíble hacia arriba.

f. Retire la cubierta presionando el botón y deslizando la cubierta hacia fuera.

Mueva la batería a la nueva controladora

Pasos

1. Retire la batería de la controladora con errores e instálela en la controladora de reemplazo:

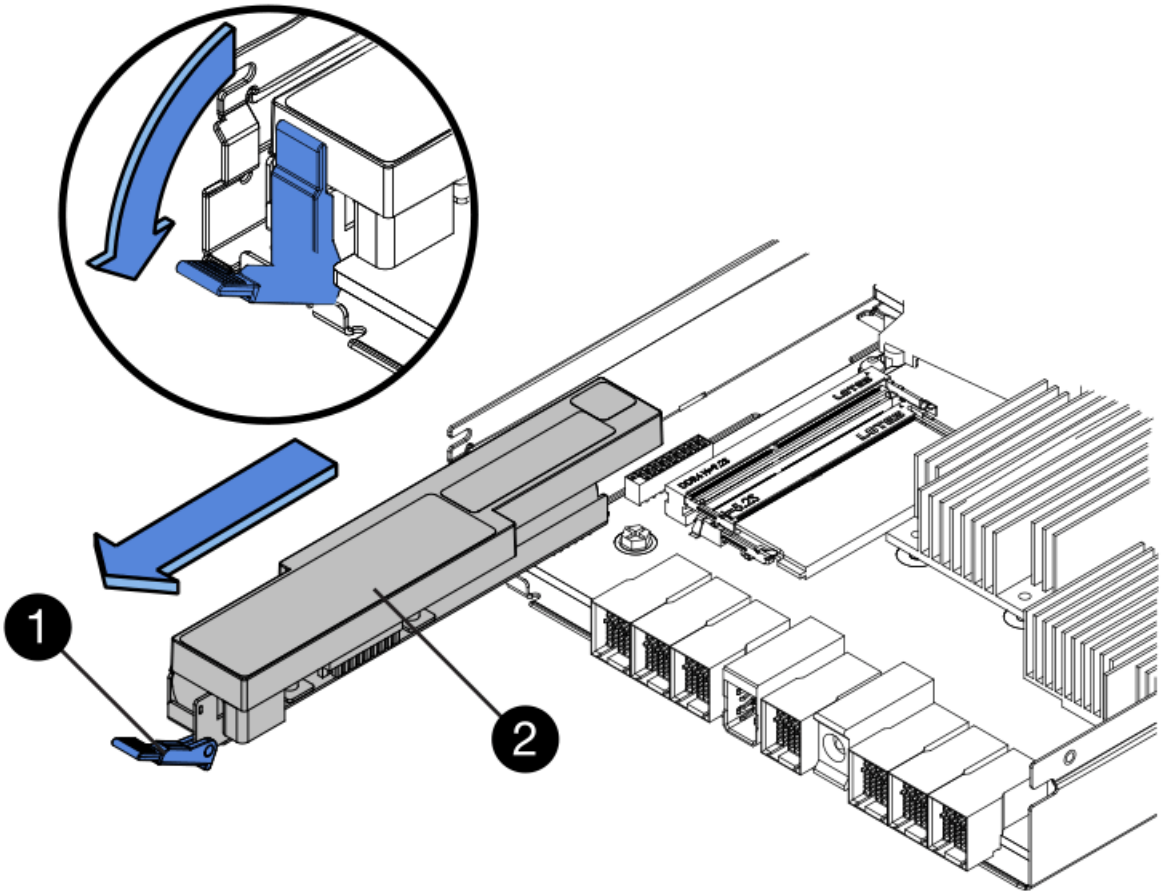
   a. Confirme que el LED verde dentro del controlador (entre la batería y los DIMM) está apagado.

      Si este LED verde está encendido, el controlador sigue utilizando la batería. Debe esperar a que este LED se apague antes de quitar los componentes.

Elemento	Descripción
1	LED de caché interna activa
2	Batería

   b. Localice el pestillo de liberación azul de la batería.

   c. Para desenganchar la batería, presione el pestillo de liberación hacia abajo y hacia fuera del controlador.



Elemento	Descripción
1	Pestillo de liberación de la batería
2	Batería

d. Levante la batería y deslícela fuera del controlador.
e. Retire la cubierta del controlador de recambio.
f. Oriente el controlador de repuesto de manera que la ranura de la batería quede orientada hacia usted.
g. Inserte la batería en el controlador en un ángulo ligeramente descendente.

   Debe insertar la brida metálica de la parte frontal de la batería en la ranura de la parte inferior del controlador y deslizar la parte superior de la batería por debajo del pasador de alineación pequeño del lado izquierdo del controlador.

h. Mueva el pestillo de la batería hacia arriba para fijar la batería.

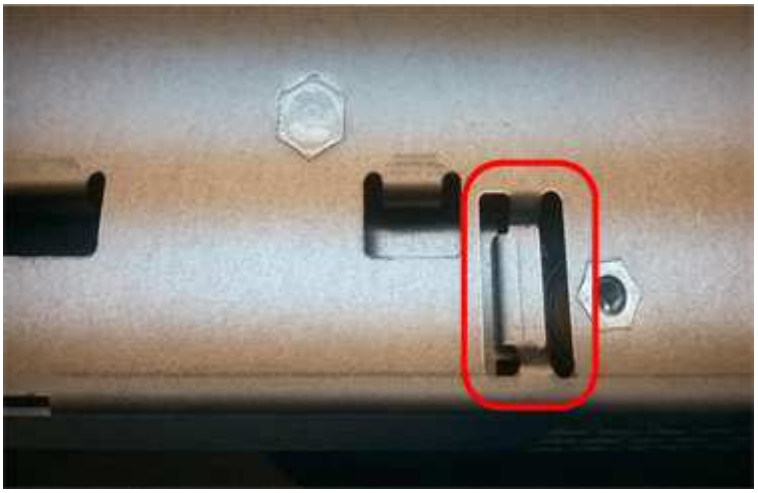
   Cuando el pestillo hace clic en su lugar, la parte inferior del pestillo se engancha a una ranura metálica del chasis.

i. Dé la vuelta al controlador para confirmar que la batería está instalada correctamente.

Posible daño de hardware — la brida metálica de la parte frontal de la batería debe estar completamente insertada en la ranura del controlador (como se muestra en la primera figura). Si la batería no está instalada correctamente (como se muestra en la segunda figura), la brida metálica podría entrar en contacto con la placa del controlador, causando daños.

- **Correcto — la brida metálica de la batería está completamente insertada en la ranura del controlador:**

- **Incorrecto — la brida metálica de la batería no está insertada en la ranura del controlador:**



2. Vuelva a colocar la cubierta del controlador.

Si es necesario, mueva HIC a una nueva controladora

Pasos

1. Si la controladora con errores incluye una tarjeta de interfaz del host (HIC), mueva la HIC de la controladora con error a la controladora de reemplazo.

   Una HIC independiente se utiliza únicamente para la controladora E2800B. La HIC se monta en la placa del controlador principal e incluye dos conectores SPF.

   Las ilustraciones de este procedimiento muestran una HIC de 2 puertos. La HIC de la controladora puede tener una cantidad de puertos diferente.

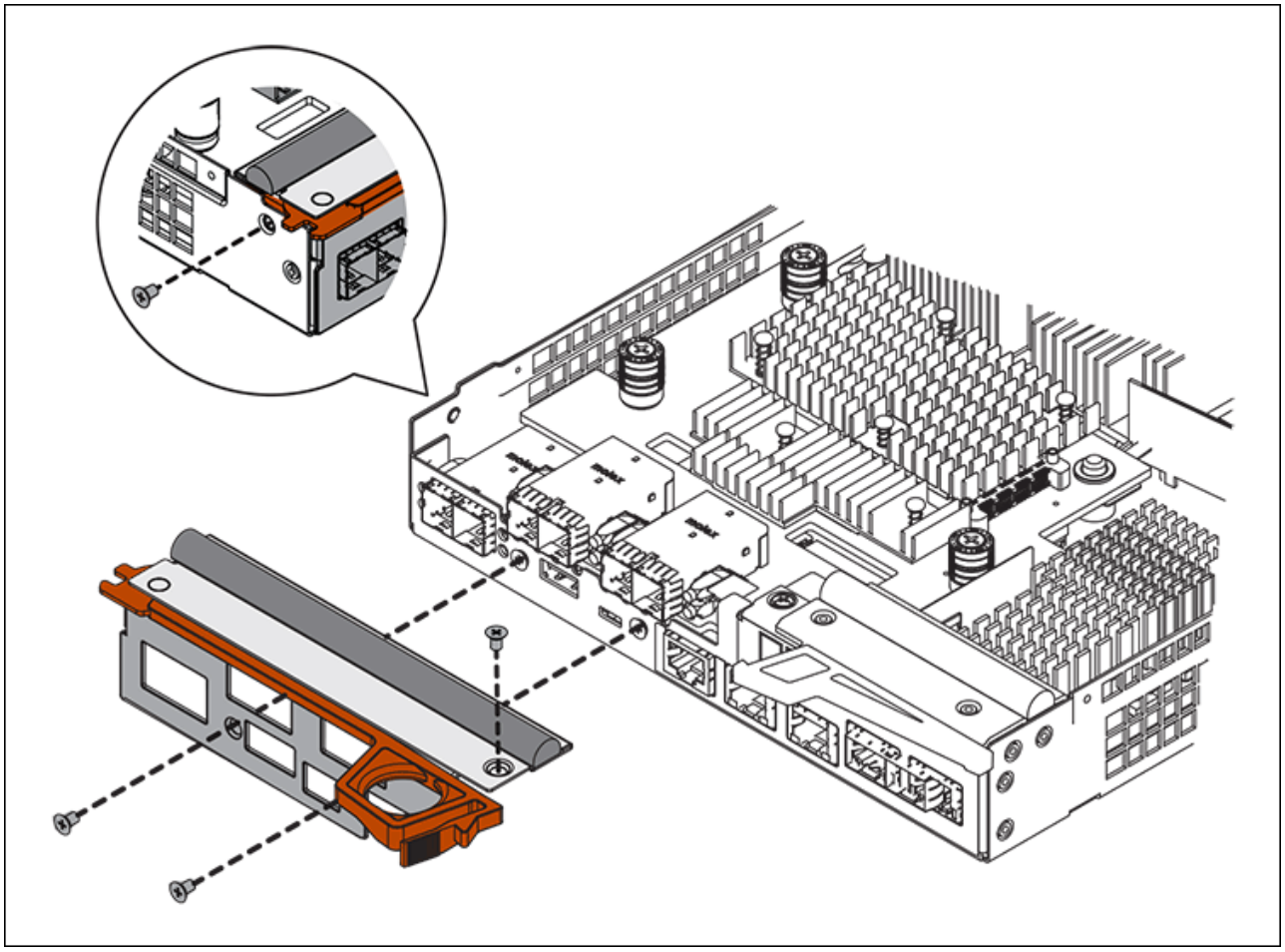
2. Si la controladora no tiene una HIC (E2800A), reemplace la cubierta de la controladora. Si la controladora tiene una HIC (E2800B), continúe a. Mueva la HIC de la controladora con errores a la controladora de reemplazo.

   a. Si está equipado con una HIC, mueva la HIC de la controladora con error a la controladora de reemplazo.

   b. Quite todos los SFP de la HIC.

   c. Con un destornillador Phillips del número 1, quite los tornillos que conectan la placa frontal de HIC a la controladora.

      Hay cuatro tornillos: Uno en la parte superior, uno en el lateral y dos en la parte delantera.

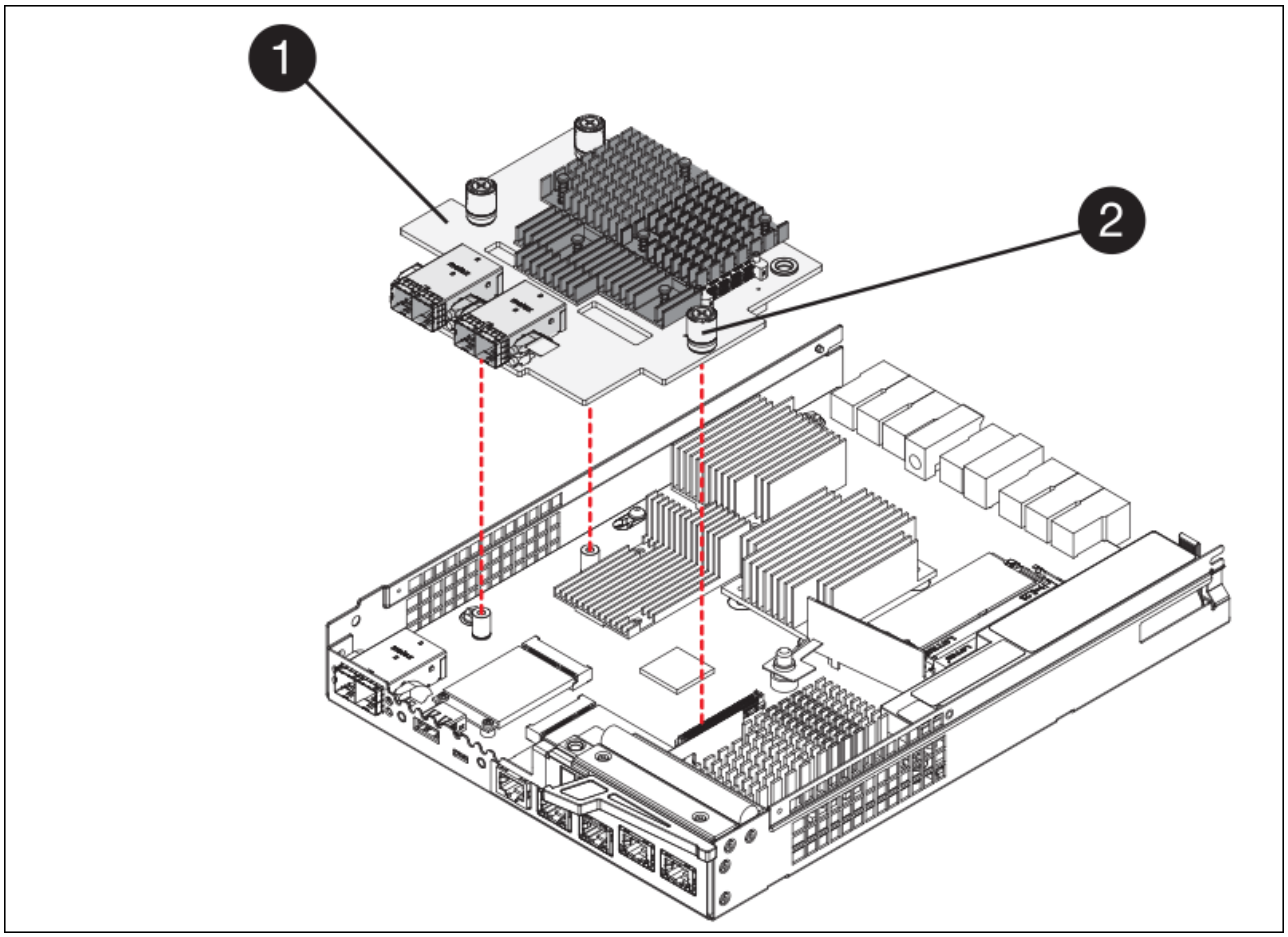


   d. Quite la placa frontal de HIC.

   e. Con los dedos o un destornillador Phillips, afloje los tres tornillos de ajuste manual que fijan la HIC a la tarjeta controladora.

   f. Retire con cuidado la tarjeta HIC de la tarjeta controladora levantando la tarjeta y deslizándola hacia atrás.

      Tenga cuidado de no arañar ni golpear los componentes en la parte inferior de la HIC o en la parte superior de la tarjeta de la controladora.



Etiqueta	Descripción
1	Tarjeta de interfaz del host
2	Tornillos de apriete manual

g. Coloque la HIC en una superficie sin estática.

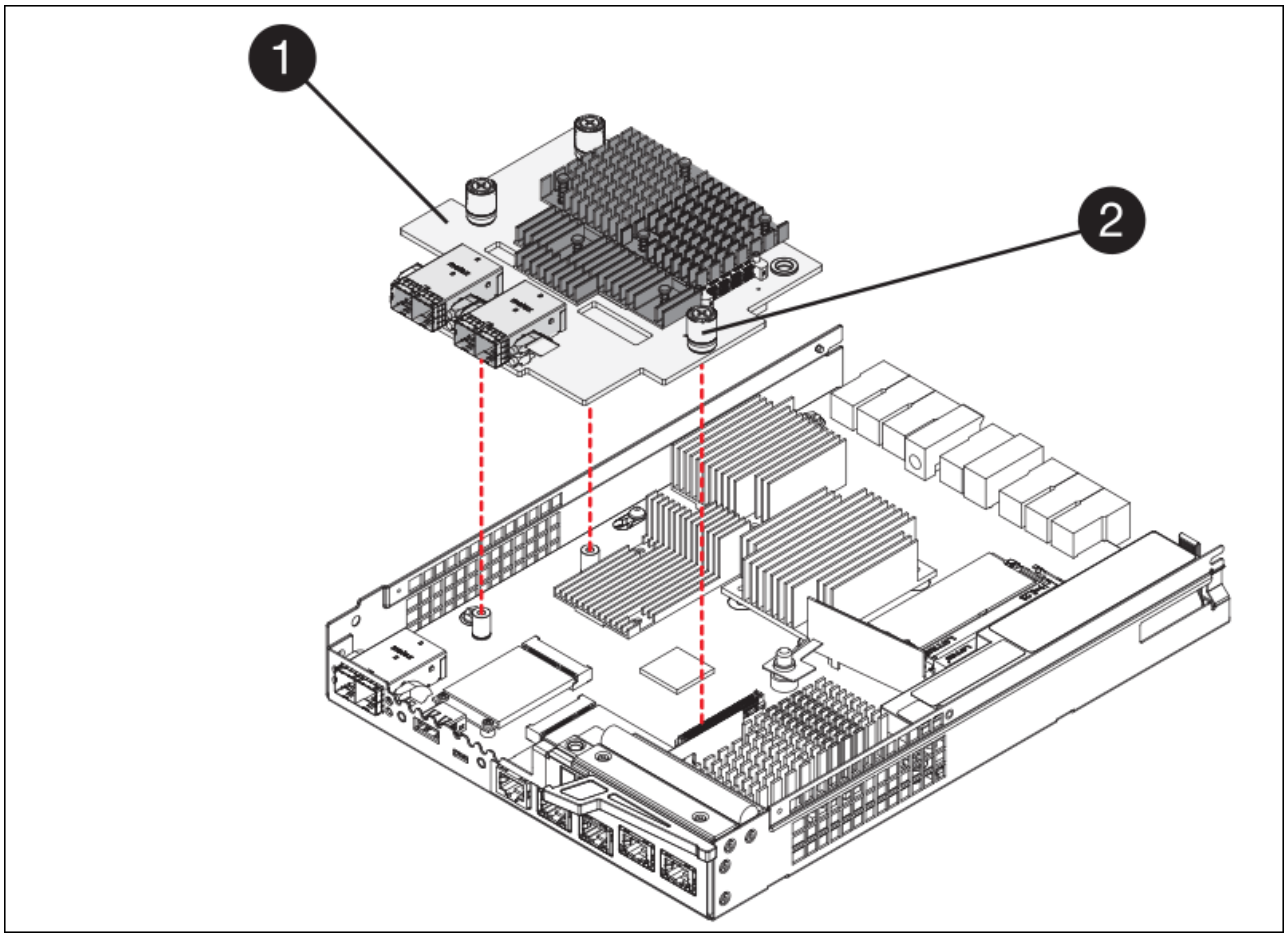
h. Con un destornillador Phillips del número 1, quite los cuatro tornillos que fijan la placa frontal vacía al controlador de repuesto y quite la placa frontal.

i. Alinee los tres tornillos de apriete manual de la HIC con los orificios correspondientes de la controladora de reemplazo y alinee el conector de la parte inferior de la HIC con el conector de la interfaz HIC de la tarjeta controladora.

   Tenga cuidado de no arañar ni golpear los componentes en la parte inferior de la HIC o en la parte superior de la tarjeta de la controladora.

j. Baje con cuidado la HIC en su lugar y coloque el conector de la HIC presionando suavemente en la HIC.

Posible daño en el equipo — tenga mucho cuidado de no pellizcar el conector de la cinta de oro para los LED del controlador entre la HIC y los tornillos de mariposa.

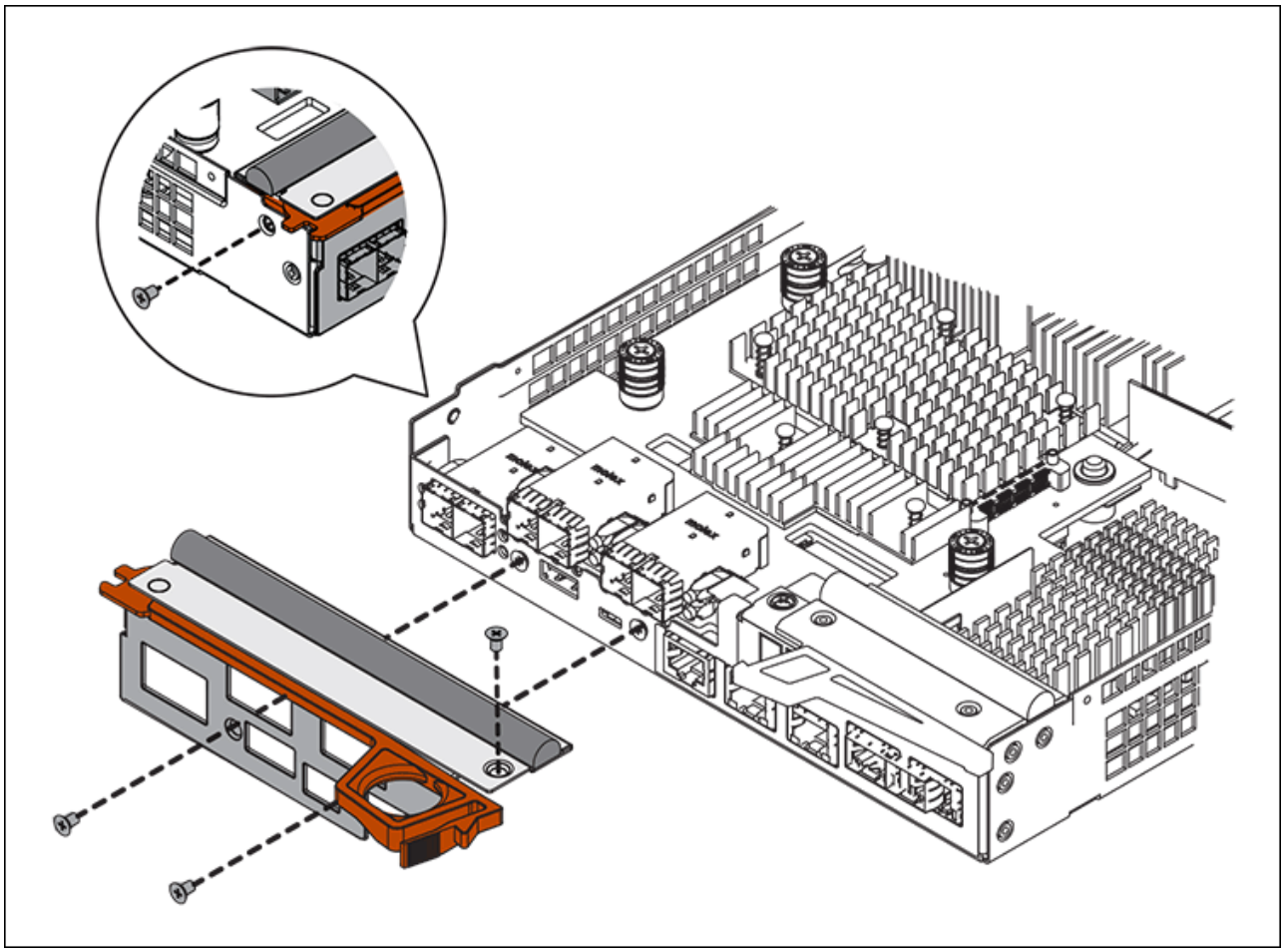


Etiqueta	Descripción
1	Tarjeta de interfaz del host
2	Tornillos de apriete manual

a. Apriete a mano los tornillos de mariposa HIC.

   No utilice un destornillador, o puede apretar los tornillos en exceso.

b. Con un destornillador Phillips del número 1, conecte la placa frontal de la HIC que quitó de la controladora original a la nueva controladora con cuatro tornillos.



c. Vuelva a instalar todos los SFP que se hayan quitado en la HIC.

Sustituya la controladora

Pasos

1. Instale el controlador de repuesto en el aparato.

   a. Dé la vuelta al controlador de modo que la cubierta extraíble quede orientada hacia abajo.

   b. Con el mango de la leva en la posición abierta, deslice el controlador completamente en el aparato.

   c. Mueva la palanca de leva hacia la izquierda para bloquear el controlador en su sitio.

   d. Sustituya los cables y SFP.

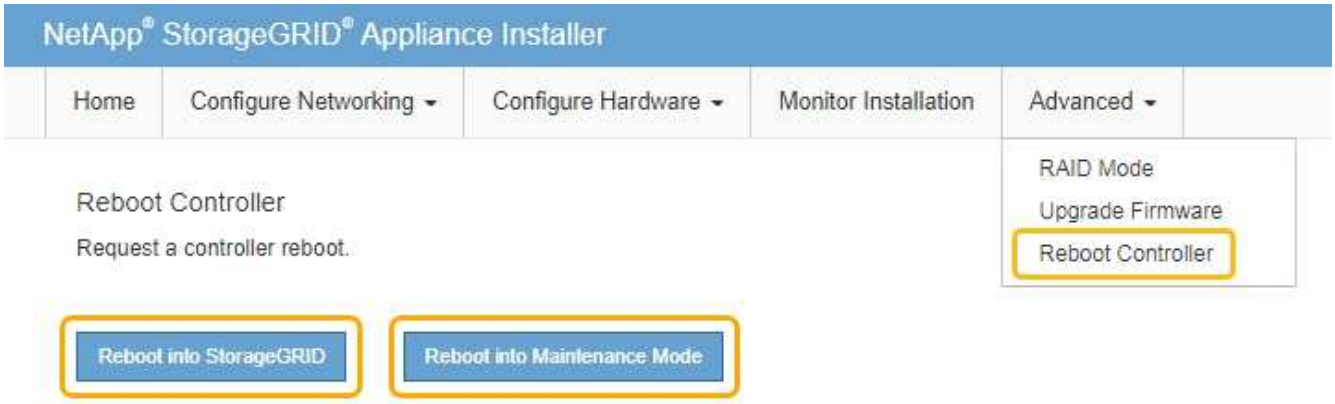
   e. Espere a que se reinicie la controladora E2800. Compruebe que la pantalla de siete segmentos muestra el estado de `99`.

   f. Determinar cómo se asignará una dirección IP a la controladora de reemplazo.

   > Los pasos para asignar una dirección IP a la controladora de reemplazo dependen de si se conectó el puerto de gestión 1 a una red con un servidor DHCP y si todas las unidades están protegidas.

   Si el puerto de gestión 1 está conectado a una red con un servidor DHCP, la nueva controladora obtendrá su dirección IP del servidor DHCP. Este valor puede ser diferente de la dirección IP de la controladora original.

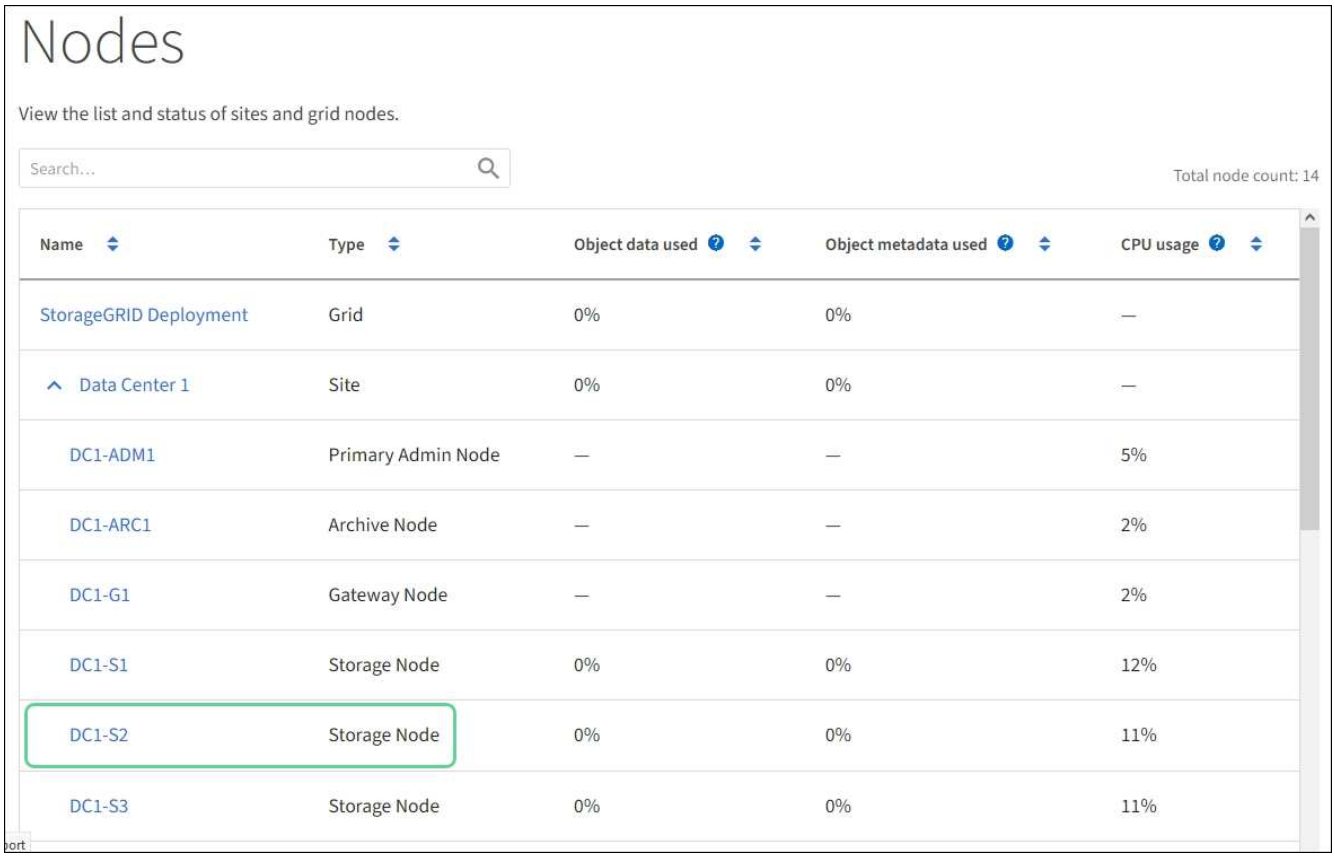
2. Si el dispositivo utiliza unidades seguras, siga las instrucciones del procedimiento de reemplazo de la controladora E2800 para importar la clave de seguridad de la unidad.
3. Vuelva a poner el aparato en modo de funcionamiento normal. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione **Reiniciar en StorageGRID**.



4. Durante el reinicio, supervise el estado del nodo para determinar cuándo se ha reUnido a la cuadrícula.

   El dispositivo se reinicia y vuelve a unir la cuadrícula. Este proceso puede llevar hasta 20 minutos.

5. Confirme que el reinicio ha finalizado y que el nodo se ha vuelto a unir a la cuadrícula. En Grid Manager, compruebe que la página Nodes muestra un estado normal (sin iconos a la izquierda del nombre del nodo) del nodo de dispositivo, lo que indica que no hay alertas activas y que el nodo está conectado a la cuadrícula.



6. En SANtricity System Manager, confirme que el estado de la nueva controladora es óptimo y recoja datos de soporte.

Tras sustituir la pieza, devuelva la pieza que ha fallado a NetApp, tal y como se describe en las instrucciones de RMA incluidas con el kit. Consulte "Retorno de artículo sustituciones" para obtener más información.

Información relacionada

"Sitio de documentación para sistemas E-Series y EF-Series de NetApp"

Sustituya la controladora E5700SG

Es posible que deba sustituir la controladora E5700SG si no funciona de forma óptima o si ha fallado.

Lo que necesitará

- Tiene una controladora de sustitución con el mismo número de pieza que la controladora que desea sustituir.
- Ha descargado las instrucciones de E-Series para reemplazar una controladora E5700 con errores.

> Utilice las instrucciones E-Series como referencia solo si necesita más detalles para realizar un paso específico. No confíe en las instrucciones de E-Series para sustituir una controladora en el dispositivo StorageGRID, ya que los procedimientos no son los mismos. Por ejemplo, las instrucciones de E-Series para la controladora E5700 describen cómo quitar la batería y la tarjeta de interfaz del host (HIC) de una controladora con errores e instalarlas en una controladora de reemplazo. Estos pasos no se aplican al controlador E5700SG.

- Tiene etiquetas para identificar cada cable conectado a la controladora.
- El aparato se ha estado se colocó en modo de mantenimiento.

Acerca de esta tarea

No se podrá acceder al nodo de almacenamiento del dispositivo cuando se sustituye la controladora. Si el controlador E5700SG funciona lo suficiente, puede realizar un apagado controlado al inicio de este procedimiento.

> Si va a sustituir la controladora antes de instalar el software StorageGRID, es posible que no pueda acceder al instalador de dispositivos de StorageGRID inmediatamente después de completar este procedimiento. Aunque puede acceder al instalador del dispositivo StorageGRID desde otros hosts de la misma subred que el dispositivo, no puede acceder al mismo desde hosts de otras subredes. Esta condición debe resolverse dentro de los 15 minutos (cuando se agota cualquier entrada de caché ARP para el tiempo de espera original de la controladora); asimismo, puede borrar la condición de inmediato mediante la purga manual de todas las entradas antiguas de la caché ARP desde el enrutador o la puerta de enlace local.

Pasos

1. Cuando el dispositivo se haya puesto en modo de mantenimiento, apague el controlador E5700SG.
   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. Apague el controlador E5700SG:
      `shutdown -h now`
   c. Espere a que se escriban en las unidades todos los datos de la memoria caché.

      El LED verde de caché activa en la parte posterior de la controladora E2800 está encendido cuando es necesario escribir datos en caché en las unidades. Debe esperar a que se apague este LED.

2. Apague la alimentación.
   a. En la página de inicio del Administrador del sistema de SANtricity, seleccione **Ver operaciones en curso**.
   b. Confirmar que se han completado todas las operaciones.
   c. Apague los dos interruptores de alimentación del aparato.
   d. Espere a que se apagen todos los LED.
3. Si las redes StorageGRID conectadas a la controladora utilizan servidores DHCP:
   a. Tenga en cuenta las direcciones MAC de los puertos de la controladora de reemplazo (que se encuentran en las etiquetas de la controladora).
   b. Solicite al administrador de red que actualice la configuración de la dirección IP de la controladora original para reflejar las direcciones MAC de la controladora de reemplazo.

> Debe asegurarse de que las direcciones IP de la controladora original se hayan actualizado antes de aplicar alimentación a la controladora de reemplazo. De lo contrario, la controladora obtendrá nuevas direcciones IP de DHCP cuando se arranca y es posible que no pueda volver a conectarse a StorageGRID. Este paso se aplica a todas las redes StorageGRID conectadas a la controladora.

4. Retire el controlador del dispositivo:
   a. Coloque una muñequera ESD o tome otras precauciones antiestáticas.
   b. Etiquete los cables y desconecte los cables y SFP.

      > Para evitar un rendimiento degradado, no gire, pliegue, pellizque ni pellizque los cables.

   c. Suelte el controlador del aparato apretando el pestillo del asa de la leva hasta que se suelte y, a continuación, abra el asa de leva a la derecha.
   d. Con dos manos y el mango de la leva, deslice el controlador para sacarlo del aparato.

      > Utilice siempre dos manos para soportar el peso del controlador.

5. Instale el controlador de repuesto en el aparato.
   a. Dé la vuelta al controlador de modo que la cubierta extraíble quede orientada hacia abajo.
   b. Con el mango de la leva en la posición abierta, deslice el controlador completamente en el aparato.
   c. Mueva la palanca de leva hacia la izquierda para bloquear el controlador en su sitio.
   d. Sustituya los cables y SFP.
6. Encienda el dispositivo y supervise los LED del controlador y las pantallas de siete segmentos.

   Una vez que las controladoras se hayan iniciado correctamente, las pantallas de siete segmentos deberían mostrar lo siguiente:

   - Controladora E2800:

     El estado final es `99`.

   - Controladora E5700SG:

     El estado final es `HA`.

7. Confirme que el nodo de almacenamiento del dispositivo aparece en Grid Manager y que no aparece ninguna alarma.

Información relacionada

"Sitio de documentación para sistemas E-Series y EF-Series de NetApp"

Sustituir otros componentes de hardware

Puede que necesite sustituir una batería de controladora, una unidad, un ventilador o un suministro de alimentación en el dispositivo StorageGRID.

Lo que necesitará

- Tiene el procedimiento de sustitución del hardware E-Series.
- El aparato se ha estado se colocó en modo de mantenimiento si el procedimiento de sustitución de componentes requiere que apague el aparato.

Acerca de esta tarea

Para sustituir la batería en la controladora E2800, consulte las instrucciones de estas instrucciones para sustituir la controladora E2800. Estas instrucciones describen cómo extraer el controlador del aparato, extraer la batería del controlador, instalar la batería y sustituir el controlador.

Para sustituir una unidad, un contenedor de alimentación/ventilador, un contenedor de ventilador, un contenedor de alimentación o un cajón de unidades en el dispositivo, acceda a los procedimientos de E-Series para mantener el hardware E2800.

Instrucciones para la sustitución de componentes SG5712

FRU	Consulte las instrucciones de E-Series para
Unidad	Reemplazar una unidad en bandejas de 12 o 24 unidades E2800
Contenedor de alimentación/ventilador	Reemplazar un contenedor de alimentación-ventilador en bandejas E2800

Instrucciones para la sustitución de componentes SG5760

FRU	Consulte las instrucciones de E-Series para
Unidad	Reemplazar una unidad en bandejas E2860
Contenedor de alimentación	Reemplazar un contenedor de alimentación en bandejas E2860
Contenedor de ventilador	Reemplazar un contenedor de ventiladores en bandejas E2860
Cajón de unidades	Reemplazar un cajón de unidades en bandejas E2860

Información relacionada

Sustituya la controladora E2800

"Sitio de documentación para sistemas E-Series y EF-Series de NetApp"

Cambie la configuración del enlace de la controladora E5700SG

Es posible cambiar la configuración del enlace Ethernet de la controladora E5700SG. Puede cambiar el modo de enlace de puerto, el modo de enlace de red y la velocidad del enlace.

Lo que necesitará

Coloque la controladora E5700SG en modo de mantenimiento.

> En raras ocasiones, una vez que se coloca un dispositivo StorageGRID en modo de mantenimiento puede hacer que el dispositivo no esté disponible para el acceso remoto.

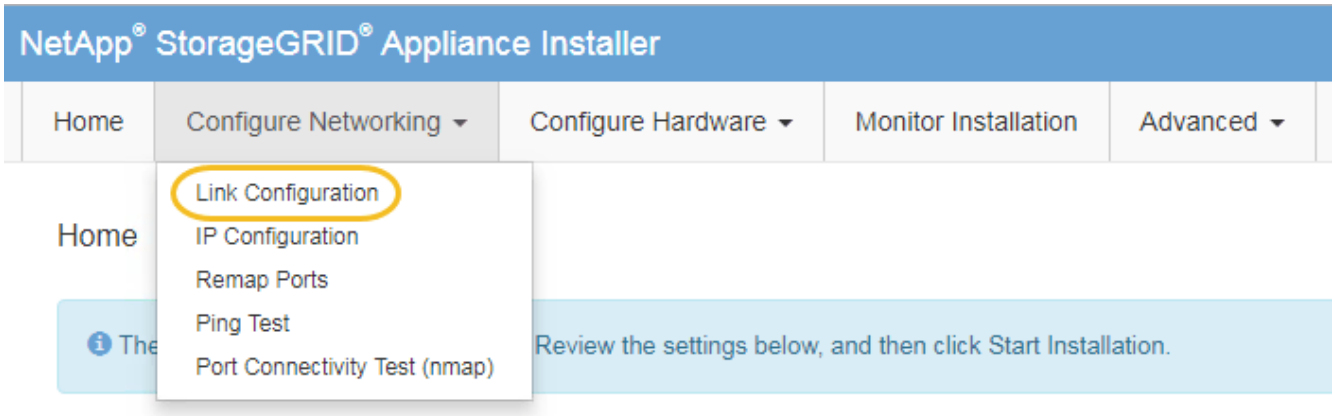
Acerca de esta tarea

Entre las opciones para cambiar la configuración del enlace Ethernet de la controladora E5700SG se incluyen:

- Cambiando **modo de enlace de puerto** de fijo a agregado, o de agregado a fijo
- Cambio del **modo de enlace de red** de Active-Backup a LACP o de LACP a Active-Backup
- Habilitar o deshabilitar el etiquetado de VLAN, o cambiar el valor de una etiqueta de VLAN
- Cambio de la velocidad de enlace de 10-GbE a 25-GbE, o de 25-GbE a 10-GbE

Pasos

1. Seleccione **Configurar red** > **Configuración de enlace** en el menú.



2. realice los cambios deseados en la configuración del enlace.

   Para obtener más información sobre las opciones, consulte «"Configuración de enlaces de red".

3. Cuando esté satisfecho con sus selecciones, haga clic en **Guardar**.

   > Puede perder la conexión si ha realizado cambios en la red o el enlace que está conectado a través de. Si no vuelve a conectarse en un minuto, vuelva a introducir la URL del instalador de dispositivos StorageGRID utilizando una de las otras direcciones IP asignadas al dispositivo:
   > `https://E5700SG_Controller_IP:8443`

   Si ha realizado cambios en la configuración de VLAN, es posible que la subred del dispositivo haya cambiado. Si necesita cambiar las direcciones IP del dispositivo, siga el Establezca la configuración de IP instrucciones.

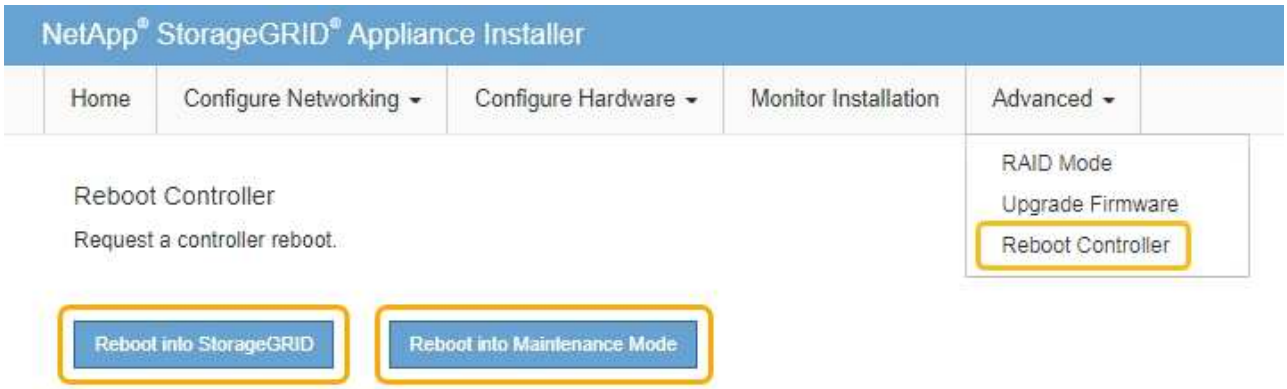
4. En el instalador del dispositivo StorageGRID, seleccione **Configurar redes** > **Prueba de ping**.
5. Utilice la herramienta Ping Test para comprobar la conectividad a las direcciones IP en cualquier red que pudiera haber sido afectada por los cambios de configuración de vínculos realizados en Cambiar la configuración del enlace paso.

   Además de todas las pruebas que elija realizar, confirme que puede hacer ping a la dirección IP de grid

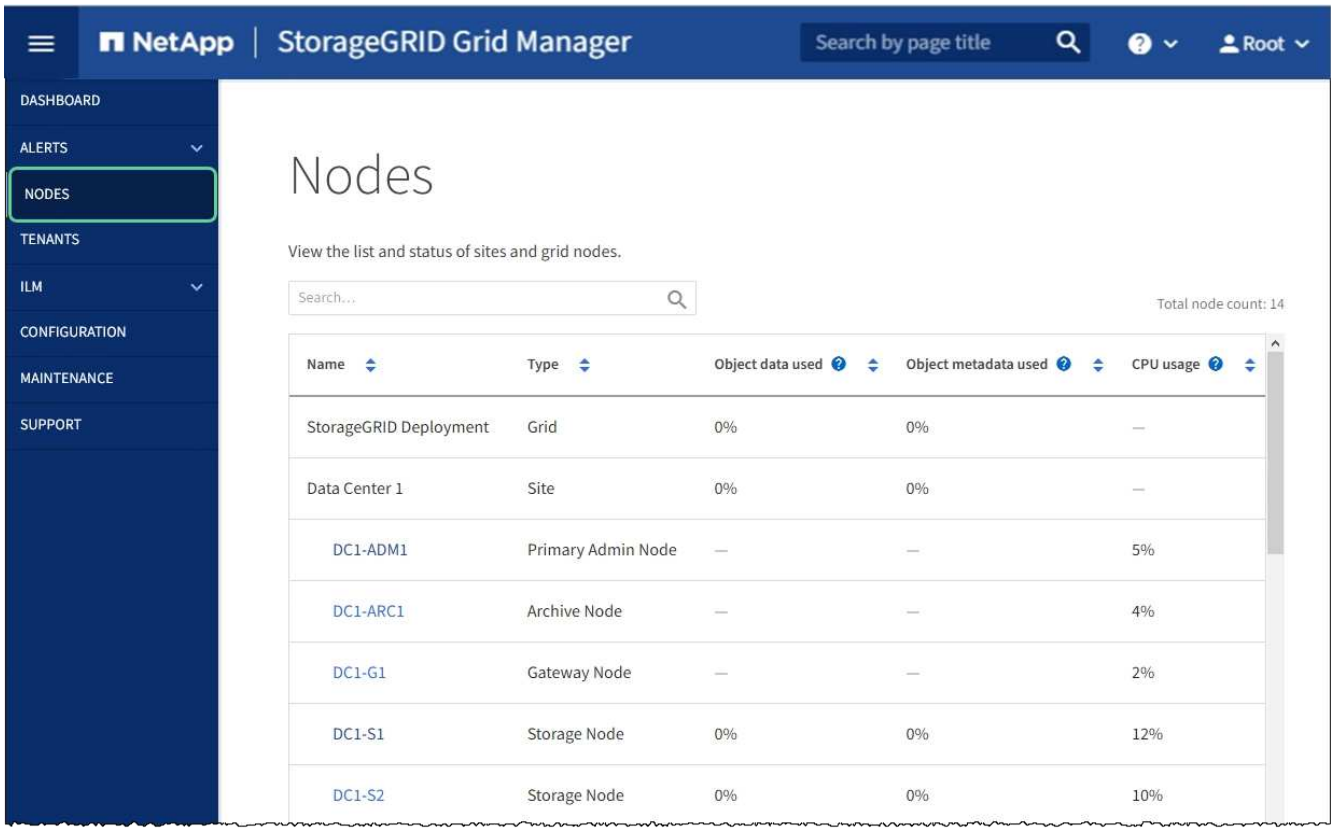
del nodo de administración principal y a la dirección IP de grid del al menos otro nodo de almacenamiento. Si es necesario, corrija los problemas de configuración de los enlaces.

6. Una vez que esté satisfecho de que los cambios en la configuración del enlace funcionan, reinicie el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



   El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Configurar enlaces de red (SG5700)

Cambie la configuración de MTU

Puede cambiar la configuración de MTU que asigne al configurar las direcciones IP para el nodo del dispositivo.

> **Acerca de esta tarea**
>
> 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. Los valores de MTU no tienen que ser iguales para todos los tipos de red.

Para cambiar la configuración de MTU sin reiniciar el nodo del dispositivo, Utilice la herramienta Cambiar IP.

Si la red de cliente o administrador no se configuró en el instalador de dispositivos de StorageGRID durante la instalación inicial, Cambie la configuración de MTU con el modo de mantenimiento.

Cambie la configuración de MTU mediante la herramienta Cambiar IP

Lo que necesitará

Usted tiene la `Passwords.txt` Archivo para utilizar la herramienta Cambiar IP.

Pasos

Acceda a la herramienta Cambiar IP y actualice la configuración de MTU como se describe en Cambie la configuración de red de los nodos.

Cambie la configuración de MTU con el modo de mantenimiento

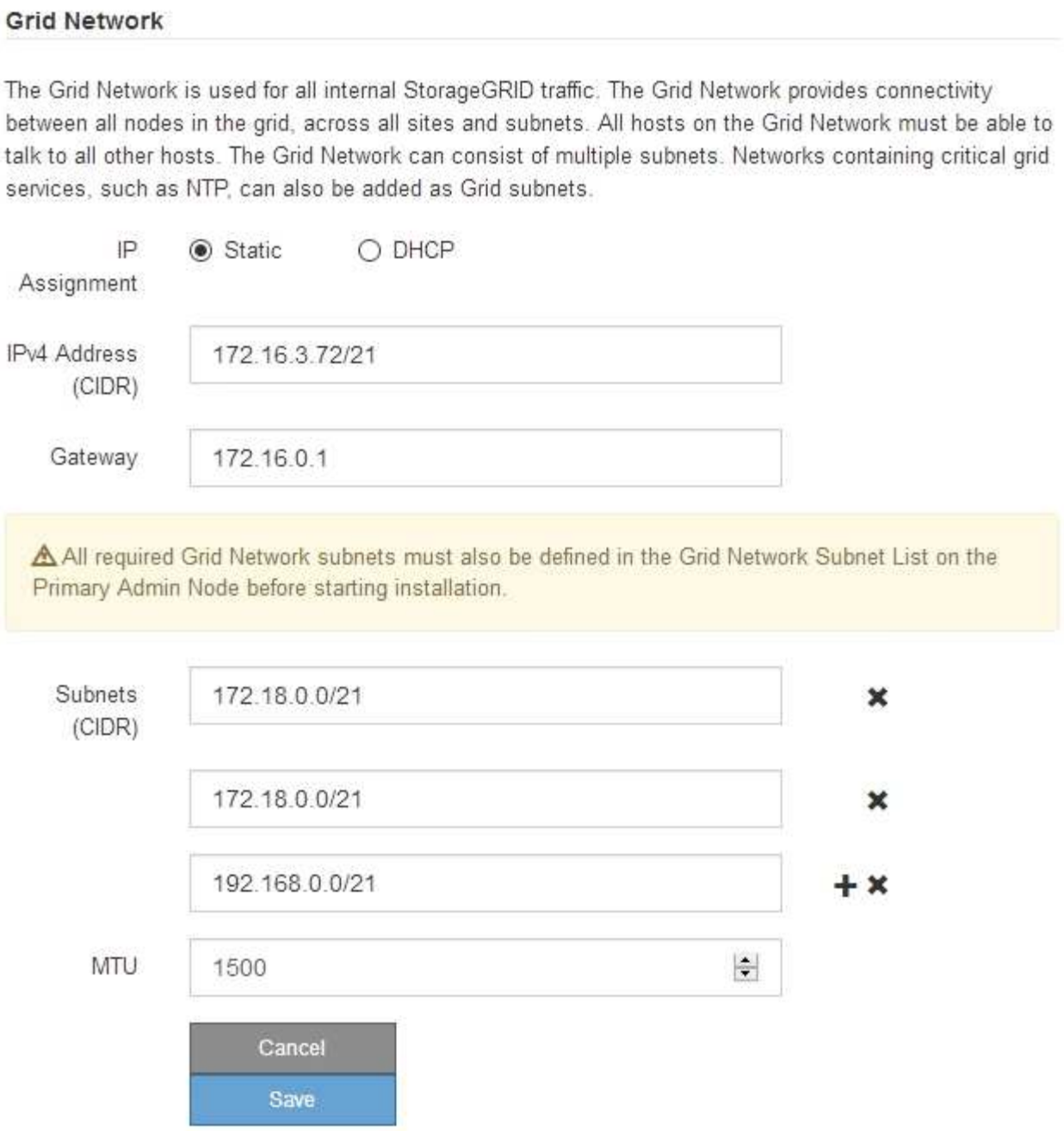
Cambie la configuración de MTU mediante el modo de mantenimiento si no puede acceder a estas opciones con la herramienta Cambiar IP.

Lo que necesitará

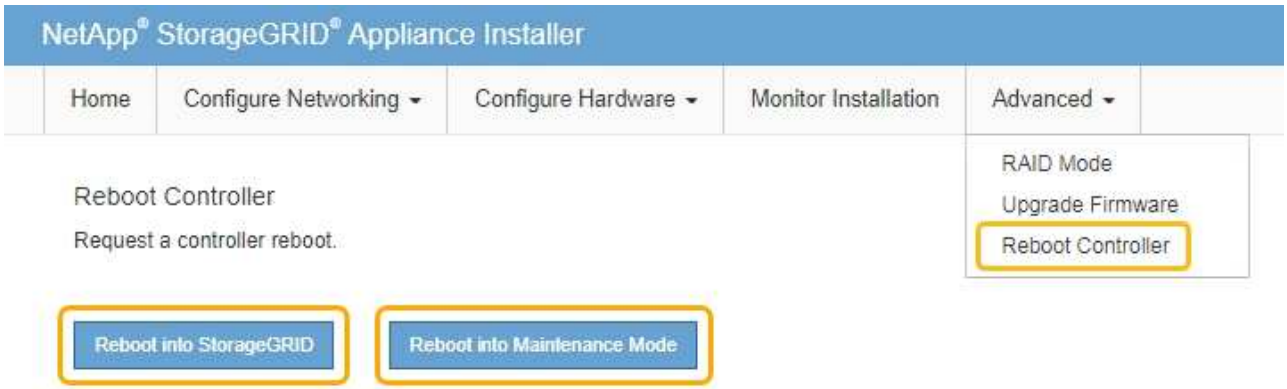
El aparato se ha estado se colocó en modo de mantenimiento.

Pasos

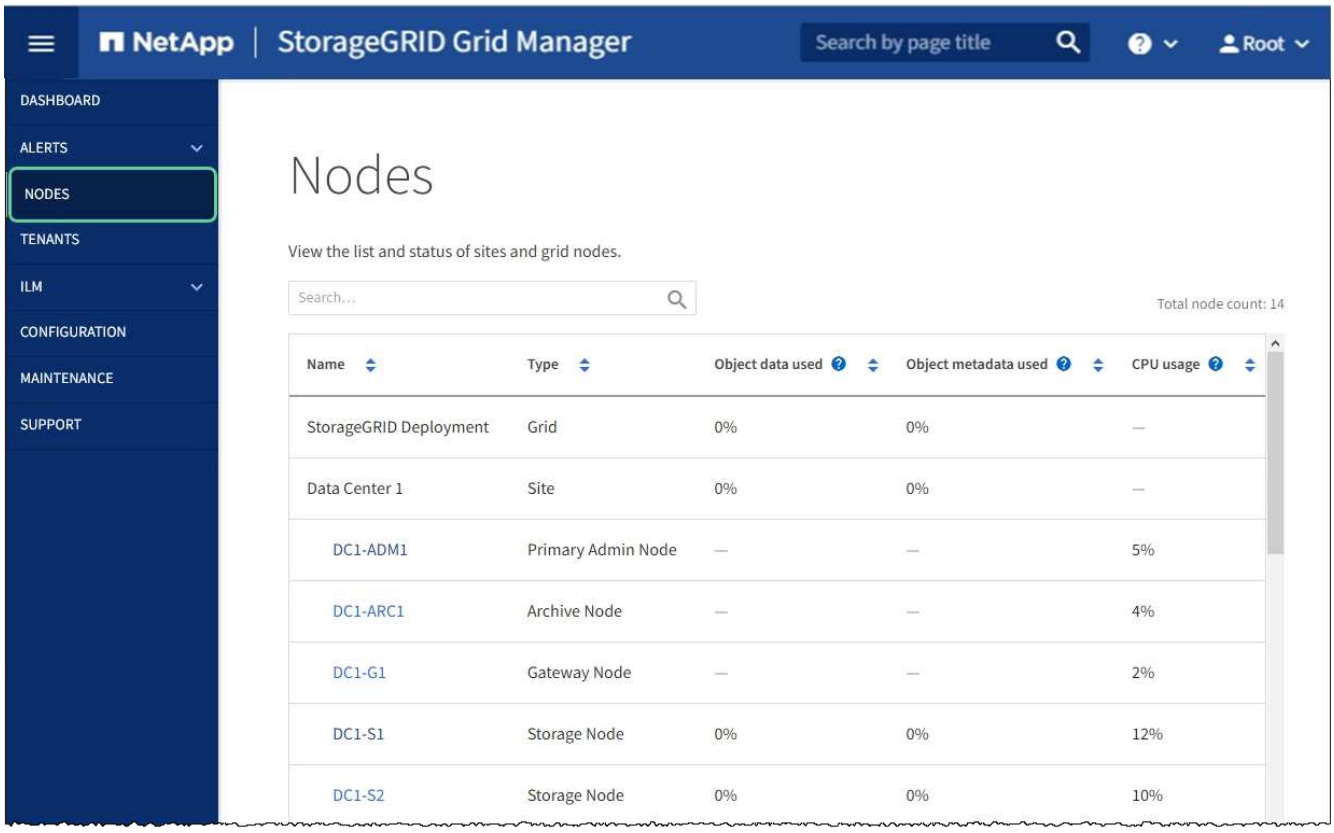
1. En el instalador del dispositivo StorageGRID, seleccione **Configurar redes** > **Configuración IP**.
2. Realice los cambios deseados en la configuración de MTU para la red de grid, la red de administración y la red de cliente.



3. Cuando esté satisfecho con los ajustes, seleccione **Guardar**.
4. Si este procedimiento se completó correctamente y tiene procedimientos adicionales que realizar mientras el nodo se encuentra en modo de mantenimiento, realice ahora. Cuando haya terminado, o si ha experimentado algún fallo y desea volver a empezar, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:
    - Seleccione **Reiniciar en StorageGRID**
    - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. Seleccione esta opción si ha experimentado algún error durante el procedimiento y desea volver a empezar. Cuando el nodo termine de reiniciarse en el modo de mantenimiento, reinicie desde el paso adecuado del procedimiento en que falló.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Administre StorageGRID

Comprobar la configuración del servidor DNS

Puede comprobar y cambiar temporalmente los servidores del sistema de nombres de dominio (DNS) que está utilizando actualmente este nodo de dispositivo.

Lo que necesitará

El aparato se ha estado se colocó en modo de mantenimiento.

Acerca de esta tarea

Es posible que deba cambiar la configuración del servidor DNS si un dispositivo cifrado no puede conectarse con el servidor de gestión de claves (KMS) o un clúster KMS porque el nombre de host del KMS se especificó como un nombre de dominio en lugar de una dirección IP. Cualquier cambio realizado en la configuración de DNS del dispositivo es temporal y se pierde al salir del modo de mantenimiento. Para que estos cambios sean permanentes, especifique los servidores DNS en Grid Manager (**MAINTENANCE** > **Network** > **servidores DNS**).

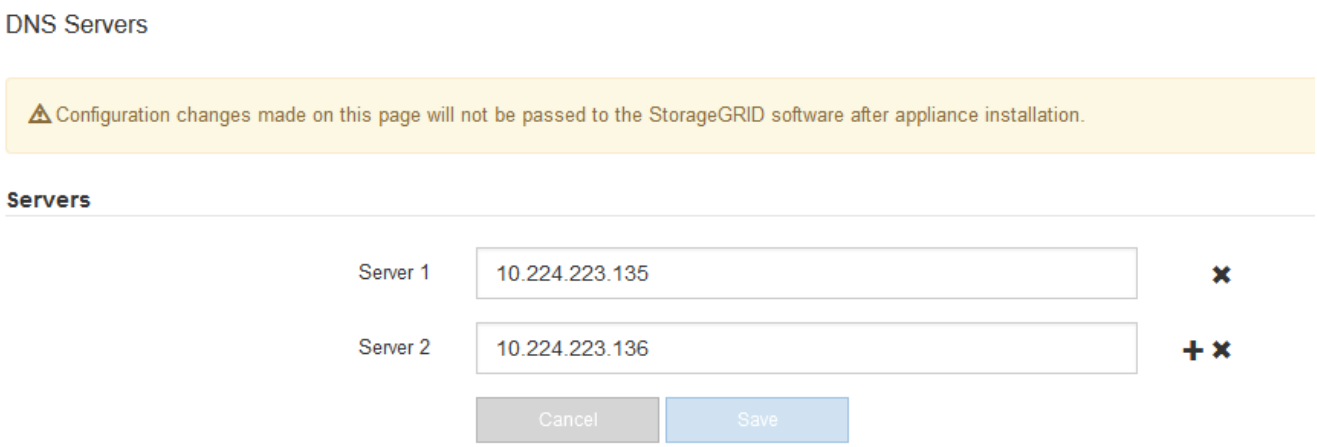
- Los cambios temporales en la configuración DNS sólo son necesarios para los dispositivos cifrados por nodo en los que el servidor KMS se define mediante un nombre de dominio completo, en lugar de una dirección IP, para el nombre de host.
- Cuando un dispositivo cifrado por nodo se conecta a un KMS mediante un nombre de dominio, debe conectarse a uno de los servidores DNS definidos para la cuadrícula. A continuación, uno de estos servidores DNS convierte el nombre de dominio en una dirección IP.
- Si el nodo no puede llegar a un servidor DNS para la cuadrícula, o si cambió la configuración de DNS para toda la cuadrícula cuando un nodo de dispositivo cifrado por nodo estaba sin conexión, el nodo no podrá conectarse al KMS. Los datos cifrados en el dispositivo no se pueden descifrar hasta que se resuelva el problema de DNS.

Para resolver un problema de DNS que impide la conexión de KMS, especifique la dirección IP de uno o más servidores DNS en el instalador de dispositivos de StorageGRID. Estas configuraciones temporales de DNS permiten que el dispositivo se conecte al KMS y descifre los datos en el nodo.

Por ejemplo, si el servidor DNS de la cuadrícula cambia mientras un nodo cifrado estaba desconectado, el nodo no podrá llegar al KMS cuando vuelva a conectarse, ya que sigue utilizando los valores DNS anteriores. La introducción de la nueva dirección IP del servidor DNS en el instalador de dispositivos de StorageGRID permite que una conexión KMS temporal descifre los datos del nodo.

Pasos

1. En el instalador de dispositivos StorageGRID, seleccione **Configurar redes** > **Configuración de DNS**.
2. Compruebe que los servidores DNS especificados sean correctos.



3. Si es necesario, cambie los servidores DNS.

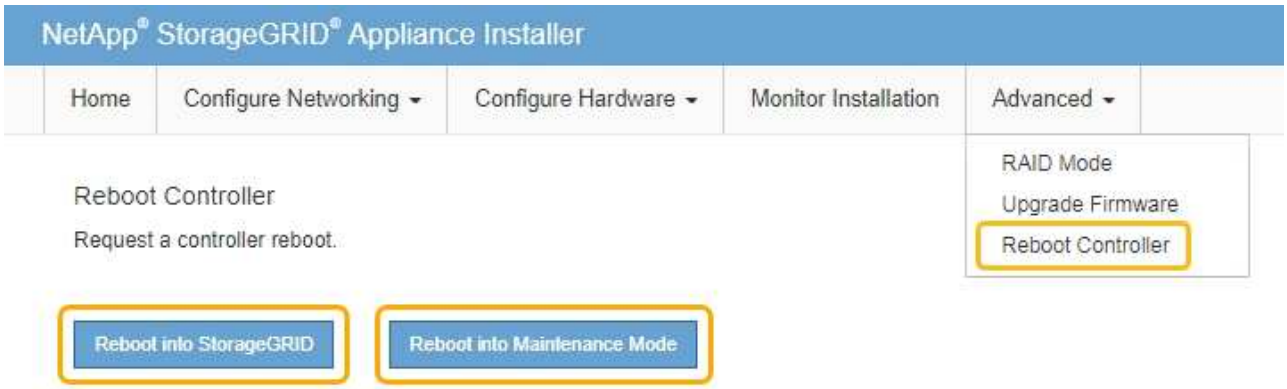
> Los cambios realizados en la configuración de DNS son temporales y se pierden al salir del modo de mantenimiento.

4. Cuando esté satisfecho con la configuración temporal de DNS, seleccione **Guardar**.

   El nodo utiliza la configuración del servidor DNS especificada en esta página para volver a conectarse al KMS, lo que permite descifrar los datos del nodo.

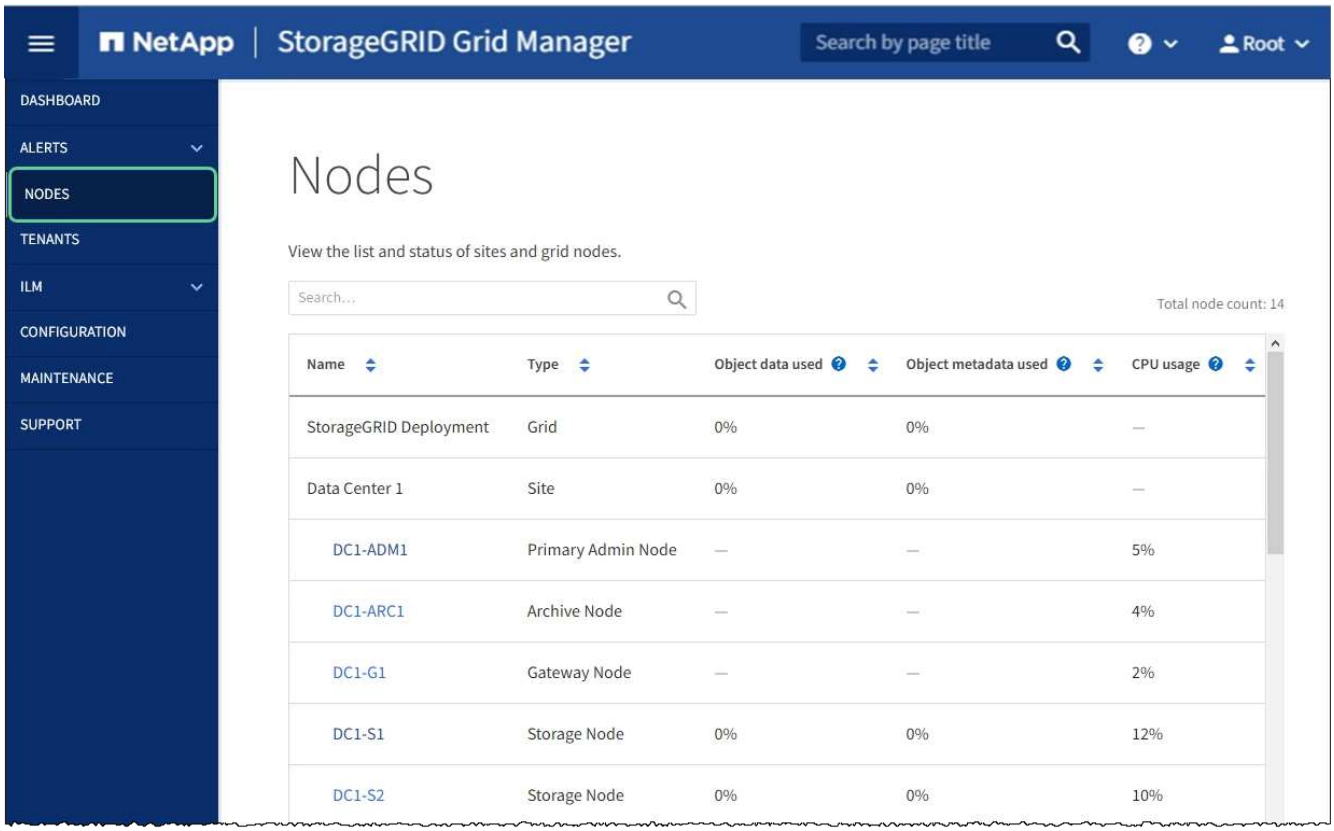
5. Tras descifrar los datos del nodo, reinicie el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



> Cuando el nodo se reinicia y se vuelve a unir a la cuadrícula, utiliza los servidores DNS de todo el sistema enumerados en Grid Manager. Después de volver a unirse a la cuadrícula, el dispositivo ya no utilizará los servidores DNS temporales especificados en el instalador de dispositivos StorageGRID mientras el dispositivo estaba en modo de mantenimiento.

El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Supervisar el cifrado de nodo en modo de mantenimiento (SG5700)

Si habilitó el cifrado de nodos para el dispositivo durante la instalación, puede supervisar el estado de cifrado del nodo de cada nodo de dispositivo, incluidos el estado del cifrado del nodo y detalles del servidor de gestión de claves (KMS).

Lo que necesitará

- El cifrado de nodos debe haber estado habilitado para el dispositivo durante la instalación. No se puede habilitar el cifrado de nodos después de que el dispositivo se haya instalado.
- El aparato se ha estado se pone en modo de mantenimiento.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Configurar hardware** > **cifrado de nodos**.

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption ☑

Save

Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate >

Client certificate >

Clear KMS Key

Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

La página cifrado de nodos incluye estas tres secciones:

- El estado de cifrado muestra si el cifrado de nodos está habilitado o deshabilitado para el dispositivo.
- Detalles del servidor de gestión de claves muestra información sobre el KMS que se utiliza para cifrar el dispositivo. Puede expandir las secciones de certificados de servidor y cliente para ver los detalles y el estado del certificado.
  - Para solucionar problemas con los propios certificados, como renovar certificados caducados, consulte la información sobre KMS en las instrucciones para administrar StorageGRID.
  - Si hay problemas inesperados al conectarse a los hosts KMS, compruebe que los servidores del sistema de nombres de dominio (DNS) son correctos y que la red del dispositivo está configurada correctamente.

    Comprobar la configuración del servidor DNS

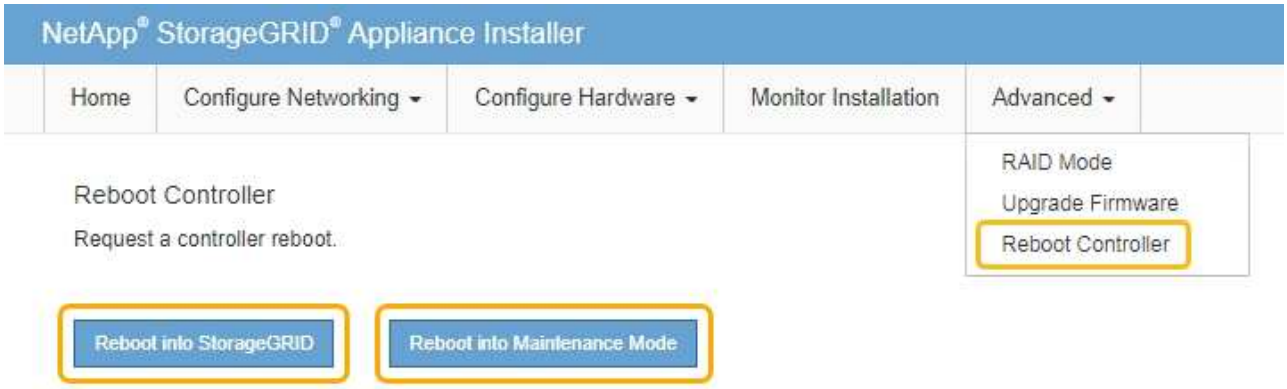
  - Si no puede resolver problemas de certificado, póngase en contacto con el soporte técnico.
- Clear KMS Key deshabilita el cifrado de nodos para el dispositivo, elimina la asociación entre el

dispositivo y el servidor de gestión de claves configurado para el sitio StorageGRID y elimina todos los datos del dispositivo. Debe borrar la clave KMS antes de poder instalar el dispositivo en otro sistema StorageGRID.

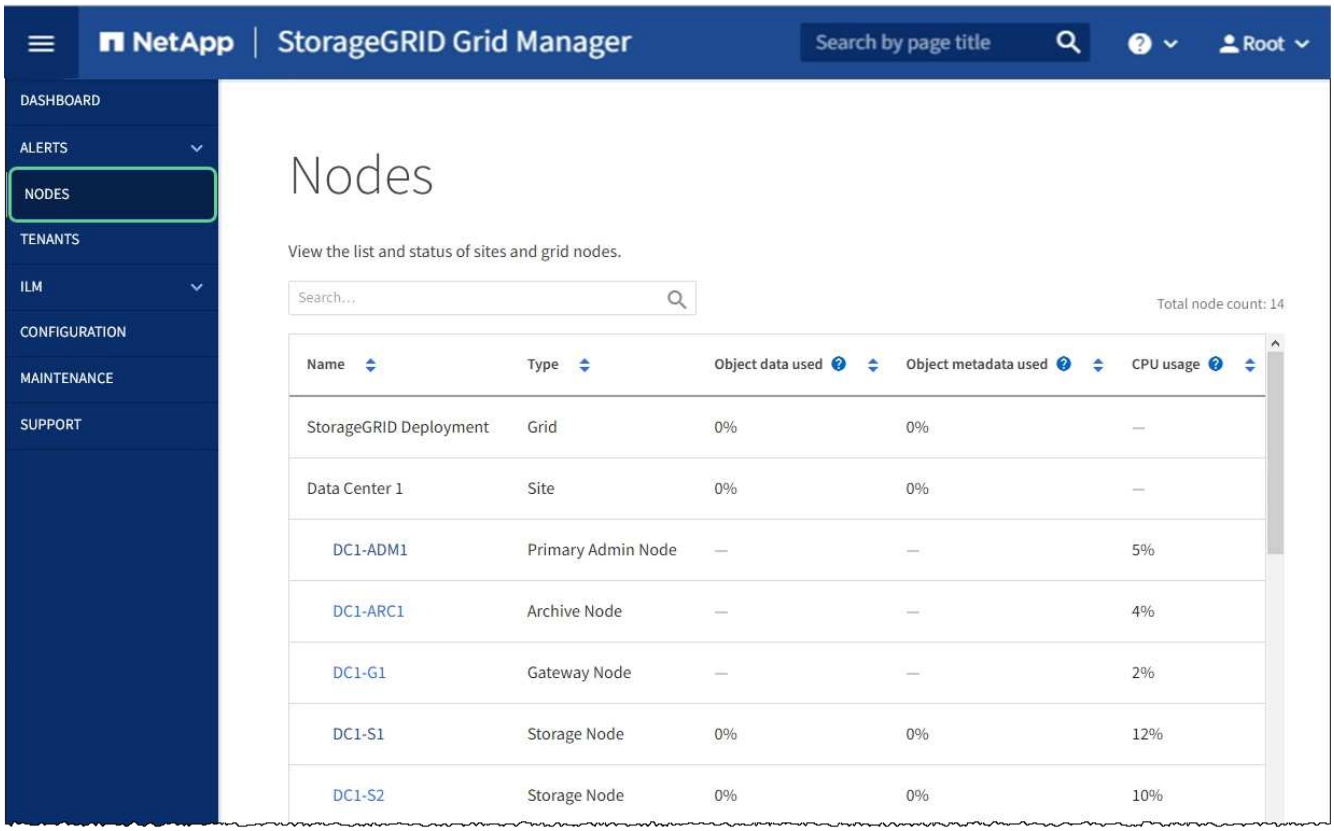
Borrar configuración de servidor de gestión de claves

> Al borrar la configuración de KMS se eliminan los datos del dispositivo, lo que hace que no se pueda acceder a ellos de forma permanente. Estos datos no se pueden recuperar.

2. Cuando haya terminado de comprobar el estado de cifrado de nodo, reinicie el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:
   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Administre StorageGRID

Borrar configuración de servidor de gestión de claves

Al borrar la configuración del servidor de gestión de claves (KMS), se deshabilita el cifrado de nodos en el dispositivo. Tras borrar la configuración de KMS, los datos del dispositivo se eliminan de forma permanente y ya no se puede acceder a ellos. Estos datos no se pueden recuperar.

Lo que necesitará

Si necesita conservar datos en el dispositivo, debe realizar un procedimiento de retirada del nodo o clonar el nodo antes de borrar la configuración de KMS.

> Cuando se borra KMS, los datos del dispositivo se eliminan de forma permanente y ya no se puede acceder a ellos. Estos datos no se pueden recuperar.

Retire el nodo Para mover los datos que contiene a otros nodos en StorageGRID.

Acerca de esta tarea

Al borrar la configuración de KMS del dispositivo, se deshabilita el cifrado de nodos y se elimina la asociación entre el nodo del dispositivo y la configuración de KMS del sitio StorageGRID. Los datos del dispositivo se eliminan y el dispositivo se deja en estado previo a la instalación. Este proceso no se puede revertir.

Debe borrar la configuración de KMS:

- Antes de poder instalar el dispositivo en otro sistema StorageGRID, que no utiliza un KMS o que utiliza un

KMS diferente.

> No borre la configuración de KMS si piensa volver a instalar un nodo de dispositivo en un sistema StorageGRID que utilice la misma clave KMS.

- Antes de poder recuperar y volver a instalar un nodo en el que se perdió la configuración de KMS y la clave KMS no se puede recuperar.
- Antes de devolver cualquier aparato que se haya utilizado anteriormente en su centro.
- Después de retirar un dispositivo con el cifrado de nodos habilitado.

> Retire el dispositivo antes de borrar KMS para mover sus datos a otros nodos del sistema StorageGRID. La eliminación de KMS antes de retirar el dispositivo provocará la pérdida de datos y podría hacer que el dispositivo deje de funcionar.

Pasos

1. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.
   `https://Controller_IP:8443`

   `Controller_IP` Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Configurar hardware** > **cifrado de nodos**.

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption ☑

Save

Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate >

Client certificate >

Clear KMS Key

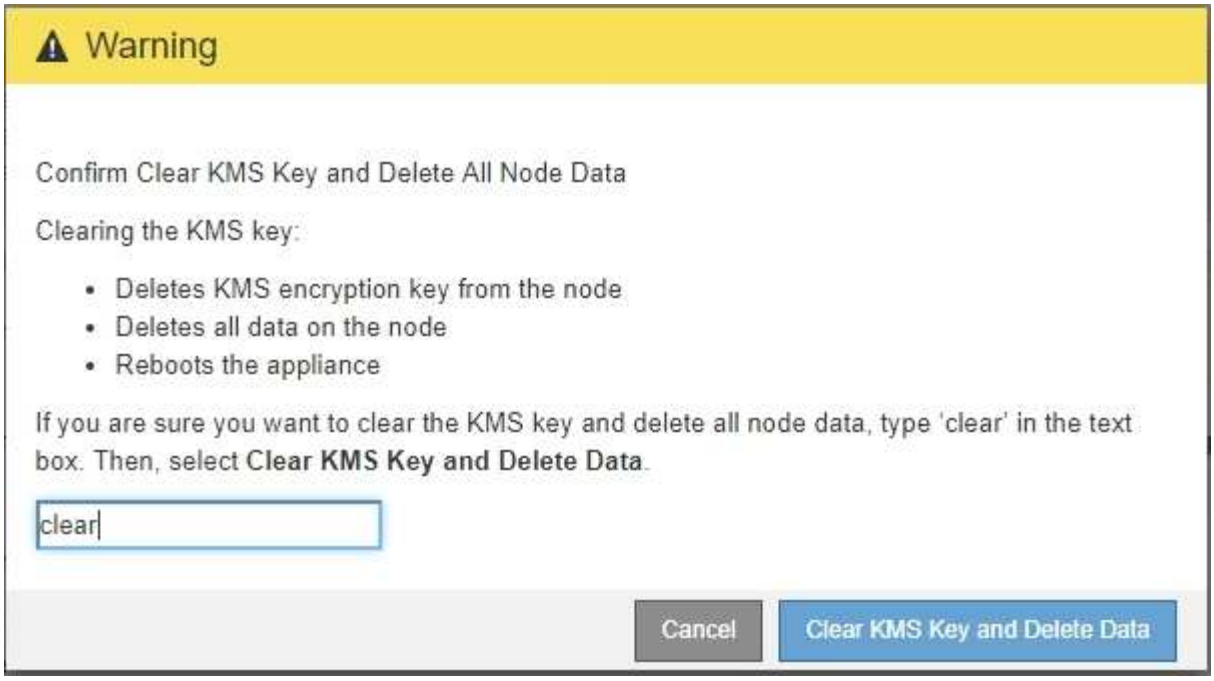
Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

> Si se borra la configuración de KMS, los datos del dispositivo se eliminarán permanentemente. Estos datos no se pueden recuperar.

3. En la parte inferior de la ventana, seleccione **Borrar clave KMS y Eliminar datos**.
4. Si está seguro de que desea borrar la configuración de KMS, escriba `clear` + y seleccione **Borrar clave KMS y Eliminar datos**.



La clave de cifrado KMS y todos los datos se eliminan del nodo y el dispositivo se reinicia. Esto puede tardar hasta 20 minutos.

5. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.
   `https://Controller_IP:8443`

   `Controller_IP` Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

6. Seleccione **Configurar hardware** > **cifrado de nodos**.
7. Compruebe que el cifrado de nodos está desactivado y que la información de claves y certificados de **Detalles del servidor de administración de claves** y el control **Borrar clave KMS y Eliminar datos** se eliminan de la ventana.

   El cifrado de nodos no se puede volver a habilitar en el dispositivo hasta que se vuelva a instalar en una cuadrícula.

Después de terminar

Una vez que el dispositivo se haya reiniciado y haya verificado que se ha borrado KMS y que el dispositivo está en estado previo a la instalación, puede quitar físicamente el dispositivo del sistema de StorageGRID. Consulte las instrucciones de recuperación y mantenimiento para obtener información acerca de Prepare el aparato para su reinstalación.

Información relacionada

Administre StorageGRID

Dispositivos de almacenamiento SG5600

Dispositivos SG5600: Información general

El dispositivo SG5600 de StorageGRID es una plataforma integrada de almacenamiento y computación que funciona como un nodo de almacenamiento en un grid StorageGRID.

El dispositivo SG5600 StorageGRID incluye los siguientes componentes:

Componente	Descripción
Controladora E5600SG	Compute ServerLa controladora E5600SG ejecuta el sistema operativo Linux y el software StorageGRID. Esta controladora se conecta a las siguientes: • Las redes de administración, grid y cliente del sistema StorageGRID • La controladora E2700, utiliza rutas SAS duales (activo/activo) con la controladora E5600SG funcionando como iniciador
Controladora E2700	Controlador de almacenamiento la controladora E2700 funciona como cabina de almacenamiento E-Series estándar en modo simple y ejecuta el sistema operativo SANtricity (firmware de la controladora). Esta controladora se conecta a las siguientes: • La red de gestión en la que se ha instalado SANtricity Storage Manager • La controladora E5600SG, utiliza rutas SAS duales (activo/activo) con la controladora E2700 que funciona como objetivo

El dispositivo SG5600 también incluye los siguientes componentes, según el modelo:

Componente	Modelo SG5612	Modelo SG5660
Unidades	12 unidades NL-SAS	60 unidades NL-SAS
Compartimento	El compartimento DE1600, un chasis de unidad rack (2U) que aloja las unidades y las controladoras	Compartimento DE6600, cuatro chasis de unidad rack (4U) que alojan las unidades y las controladoras
Fuentes de alimentación y ventiladores	Dos contenedores de alimentación/ventilador	Dos fuentes de alimentación y dos ventiladores

El controlador E5600SG está muy personalizado para su uso en el dispositivo StorageGRID. Todos los demás componentes funcionan de la forma descrita en la documentación de E-Series, excepto si se indica en estas instrucciones.

El almacenamiento bruto máximo disponible en cada nodo de almacenamiento del dispositivo StorageGRID es fijo, según el modelo y la configuración del dispositivo. No se puede expandir el almacenamiento disponible si se añade una bandeja con unidades adicionales.

Funcionalidades del dispositivo StorageGRID

El dispositivo SG5600 de StorageGRID proporciona una solución de almacenamiento integrada para crear un nuevo sistema StorageGRID o para ampliar la capacidad de un sistema existente.

El dispositivo StorageGRID ofrece las siguientes funciones:

- Combina los elementos de almacenamiento y computación de nodos de almacenamiento de StorageGRID en una única solución integrada y eficiente
- Simplifica la instalación y configuración de un nodo de almacenamiento, con lo que se automatiza la mayor parte del proceso necesario
- Proporciona una solución de almacenamiento de alta densidad con dos opciones de compartimento: Una que sea 2U y otra que sea 4U
- Utiliza interfaces IP de 10 GbE directamente al nodo de almacenamiento, sin necesidad de interfaces de almacenamiento intermedias, como FC o iSCSI
- Se puede utilizar en un entorno de grid híbrido que utiliza dispositivos StorageGRID y nodos de almacenamiento virtuales (basados en software)
- Incluye almacenamiento preconfigurado y viene precargado con el instalador de dispositivos StorageGRID (en la controladora E5600SG) para obtener integración e implementación de software listos para el campo

Diagramas de hardware

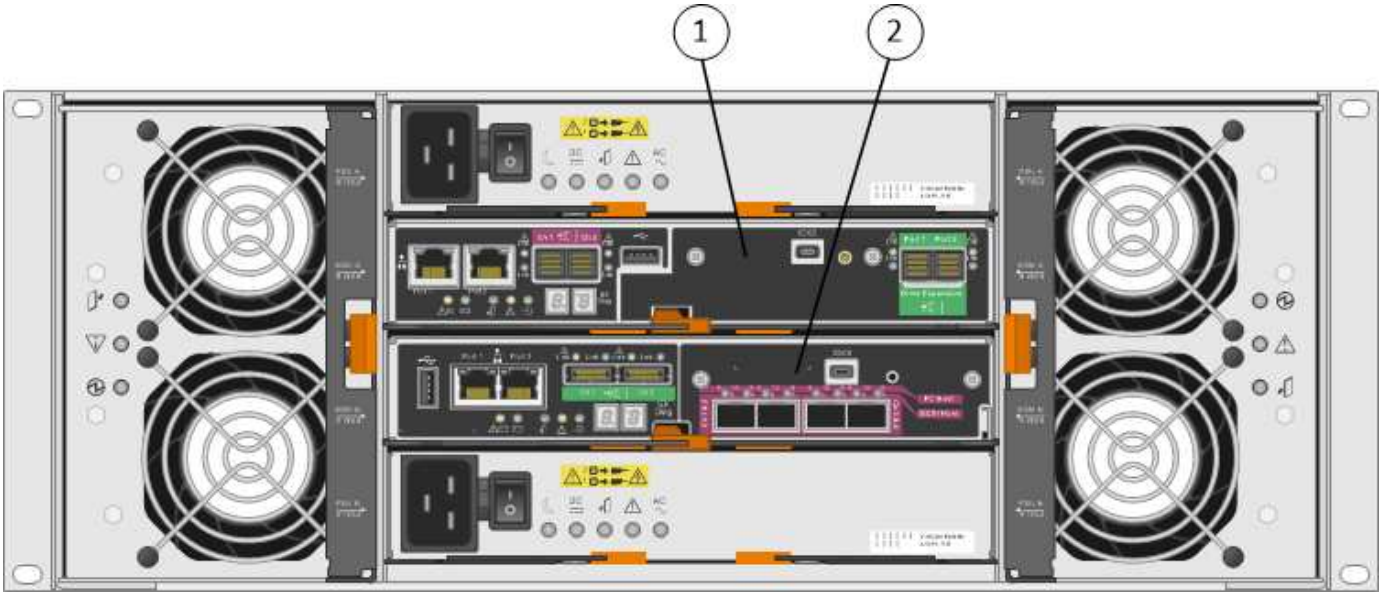
Los modelos SG5612 y SG5660 del dispositivo StorageGRID incluyen una controladora E2700 y una controladora E5600SG. Debe revisar los diagramas para conocer las diferencias entre los modelos y las controladoras.

Modelo SG5612 2U: Vista posterior de la controladora E2700 y la controladora E5600SG

Llamada	Descripción
1	Controladora E2700
2	Controladora E5600SG

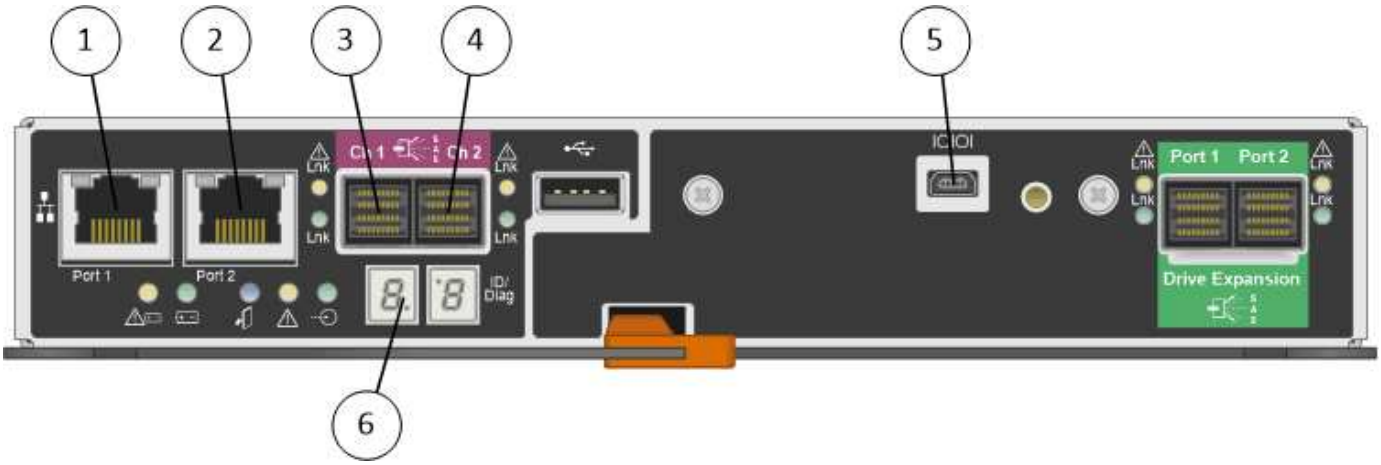
Modelo SG5660 4U: Vista trasera de la controladora E2700 y de la controladora E5600SG

La controladora E2700 está por encima de la controladora E5600SG.



Llamada	Descripción
1	Controladora E2700
2	Controladora E5600SG

Parte posterior de la controladora E2700

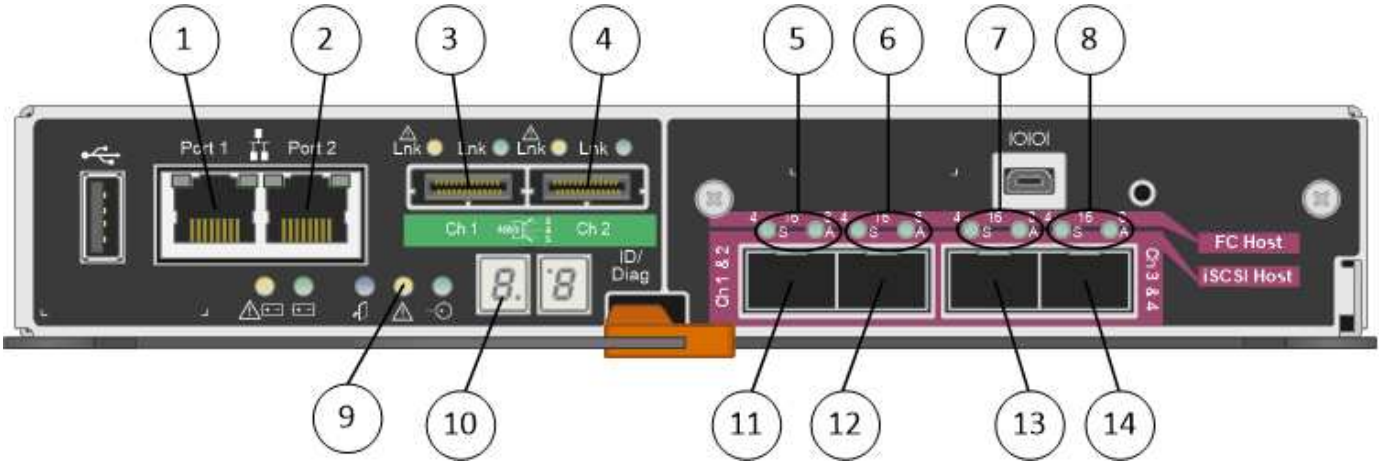


Llamada	Descripción
1	Puerto de gestión 1 (conéctese a la red donde está instalado SANtricity Storage Manager).
2	Puerto de gestión 2 (utilice durante la instalación para conectarse a un portátil).

Llamada	Descripción
3	Puerto 1 de interconexión SAS
4	Puerto de interconexión SAS 2
5	Puerto de conexión serie
6	Pantalla de siete segmentos

Los dos puertos SAS con la etiqueta Drive Expansion (verde) en la parte posterior del controlador E2700 no se utilizan. El dispositivo StorageGRID no admite bandejas de unidades de ampliación.

Vista trasera de la controladora E5600SG



Llamada	Descripción
1	El puerto de gestión 1se conecta a la red de administración para StorageGRID.
2	Opciones del puerto de gestión 2: • Bond con el puerto de gestión 1 para una conexión redundante con la red de administrador para StorageGRID. • Deje sin cables y disponible para acceso local temporal (IP 169.254.0.1). • Durante la instalación, utilice esta opción para la configuración IP si las direcciones IP asignadas por DHCP no están disponibles.
3	Puerto 1 de interconexión SAS
4	Puerto de interconexión SAS 2

Llamada	Descripción
5	LED de fallo y activo para el puerto de red 10-GbE 1
6	LED de fallo y activo para el puerto de red de 10 GbE 2
7	LED de fallo y activo para el puerto de red 10-GbE 3
8	LED de fallo y activo para el puerto de red 10-GbE 4
9	Necesita el LED de atención
10	Pantalla de siete segmentos
11	Puerto de red 10 GbE 1
12	Puerto de red de 10 GbE 2
13	Puerto de red 10-GbE 3
14	Puerto de red 10-GbE 4

La tarjeta de interfaz del host (HIC) en la controladora del dispositivo StorageGRID E5600SG admite solo conexiones Ethernet de 10 GB. No se puede utilizar para conexiones iSCSI.

Información general sobre la instalación y la implementación

Puede instalar uno o varios dispositivos StorageGRID cuando implemente StorageGRID por primera vez, o bien puede añadir nodos de almacenamiento del dispositivo más adelante como parte de una ampliación. Es posible que también se deba instalar un nodo de almacenamiento del dispositivo como parte de una operación de recuperación.

Añadir un dispositivo de almacenamiento StorageGRID a un sistema StorageGRID incluye cuatro pasos principales:

1. Preparación de la instalación:
    - Preparación del sitio de instalación
    - Desembalaje de las cajas y comprobación del contenido
    - Obtención de equipos y herramientas adicionales
    - Recopilación de direcciones IP e información de red
    - Opcional: Configurar un servidor de gestión de claves (KMS) externo si planea cifrar todos los datos del dispositivo. Consulte detalles sobre la gestión de claves externas en las instrucciones para administrar StorageGRID.
2. Instalar el hardware:

- Registrar el hardware
- Instalación del dispositivo en un armario o rack
- Instalar las unidades (solo SG5660)
- Cableado del aparato
- Conexión de los cables de alimentación y alimentación
- Ver los códigos de estado de inicio

3. Configurar el hardware:
   - Acceder a Administrador de almacenamiento de SANtricity, configurar una dirección IP estática para el puerto de gestión 1 en la controladora E2700 y los ajustes de Administrador de almacenamiento de SANtricity
   - Acceder al instalador de dispositivos de StorageGRID y configurar los ajustes de enlace e IP de red necesarios para conectarse a redes StorageGRID
   - Opcional: Habilitar el cifrado de nodos si tiene previsto utilizar un KMS externo para cifrar los datos del dispositivo.
   - Opcional: Cambiar el modo RAID.
4. Poner en marcha el dispositivo como nodo de almacenamiento:

Tarea	Consulte
Poner en marcha un nodo de almacenamiento del dispositivo en un nuevo sistema StorageGRID	Ponga en marcha el nodo de almacenamiento del dispositivo
Añadir un nodo de almacenamiento del dispositivo a un sistema StorageGRID existente	Instrucciones para ampliar un sistema StorageGRID
Poner en marcha un nodo de almacenamiento del dispositivo como parte de una operación de recuperación de nodo de almacenamiento	Instrucciones para recuperación y mantenimiento

Información relacionada

Preparación de la instalación (SG5600)

Instalar el hardware (SG5600)

Configurar el hardware (SG5600)

Amplíe su grid

Recuperación y mantenimiento

Administre StorageGRID

Preparación de la instalación (SG5600)

Para preparar la instalación de un dispositivo StorageGRID es necesario preparar el sitio y obtener todo el hardware, cables y herramientas necesarios. También debe recopilar información sobre las direcciones IP y la red.

Información relacionada

Requisitos del navegador web

Preparar el sitio (SG5600)

Antes de instalar el dispositivo, debe asegurarse de que el sitio y el armario o rack que desee usar cumplan con las especificaciones de un dispositivo StorageGRID.

Pasos

1. Confirmar que el emplazamiento cumple los requisitos de temperatura, humedad, rango de altitud, flujo de aire, disipación de calor, cableado, alimentación y conexión a tierra. Si desea obtener más información, consulte Hardware Universe de NetApp.
2. Obtenga un armario o rack de 19 pulgadas (48.3 cm) para colocar bandejas de este tamaño (sin cables):

Modelo de dispositivo	Altura	Anchura	Profundidad	Peso máximo
SG5612 (12 unidades)	3.40 pda (8.64 cm)	19.0 pda (48.26 cm)	21.75 pda (55.25 cm)	59.5 lb (27 kg)
SG5660 (60 unidades)	7.00 pda (17.78 cm)	17.75 pda (45.08 cm)	32.50 pda (82.55 cm)	236.2 lb. (107.1 kg)

3. Instale los switches de red necesarios. Consulte la herramienta de la matriz de interoperabilidad de NetApp para obtener información de compatibilidad.

Información relacionada

"Hardware Universe de NetApp"

"Interoperabilidad de NetApp"

Cajas de desempaquetado (SG5600)

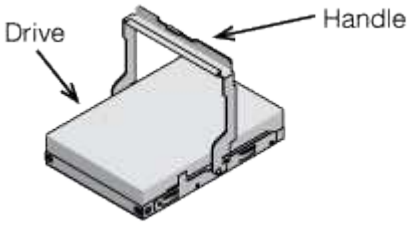
Antes de instalar el aparato StorageGRID, desembale todas las cajas y compare el contenido con los artículos del recibo de embalaje.

- **Carcasa SG5660, un chasis 4U con 60 unidades**

- **SG5612, un chasis 2U con 12 unidades**

- **Cubierta 4U o tapas 2U**

- **Unidades NL-SAS**



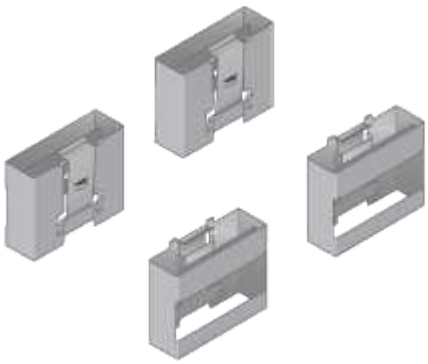
Las unidades están preinstalados en 2U SG5612, pero no en 4U SG5660 para seguridad de envío.

- **Controlador E5600SG**

- **Controladora E2700**

- **Raíles y tornillos de montaje**

- **Asas de gabinete (sólo carcasas 4U)**



Cables y conectores

El envío del dispositivo StorageGRID incluye los siguientes cables y conectores:

- **Cables de alimentación para su país**

  El aparato se suministra con dos cables de alimentación de CA para conectarse a una fuente de alimentación externa, como un enchufe de pared. Es posible que el armario tenga cables de alimentación especiales que utilice en lugar de los cables de alimentación que se suministran con el aparato.

- **Cables de interconexión SAS**

Dos cables de interconexión SAS de 0.5 metros con conectores mini-SAS-HD y mini-SAS.

El conector cuadrado se conecta a la controladora E2700 y el conector rectangular se conecta a la controladora E5600SG.

Obtener herramientas y equipos adicionales (SG5600)

Antes de instalar el dispositivo SG5600, confirme que dispone de todos los equipos y herramientas adicionales que necesita.

- **Destornilladores**

Phillips no 2 destornillador

Destornilladores de hoja plana medianos

- **Muñequera ESD**

- **Cables Ethernet**

- **Interruptor Ethernet**

- *Portátil de servicio*Navegador web compatible

Requisitos de mantenimiento de los portátiles

Antes de instalar el hardware del dispositivo StorageGRID, debe comprobar si el portátil de servicio tiene los recursos mínimos necesarios.

El ordenador portátil de servicio, necesario para la instalación del hardware, debe cumplir los siguientes requisitos:

- Sistema operativo Microsoft Windows
- Puerto de red
- Navegador web compatible
- NetApp SANtricity Storage Manager, versión 11.40 o posterior
- Cliente SSH (por ejemplo, PuTTY)

Información relacionada

Requisitos del navegador web

"Documentación de NetApp: SANtricity Storage Manager"

Revisar las conexiones de red del dispositivo (SG5600)

Antes de instalar el dispositivo StorageGRID, debe comprender qué redes se pueden conectar al dispositivo y cómo se utilizan los puertos de cada controladora.

Redes de dispositivos StorageGRID

Al poner en marcha un dispositivo StorageGRID como nodo de almacenamiento, puede conectarlo a las siguientes redes:

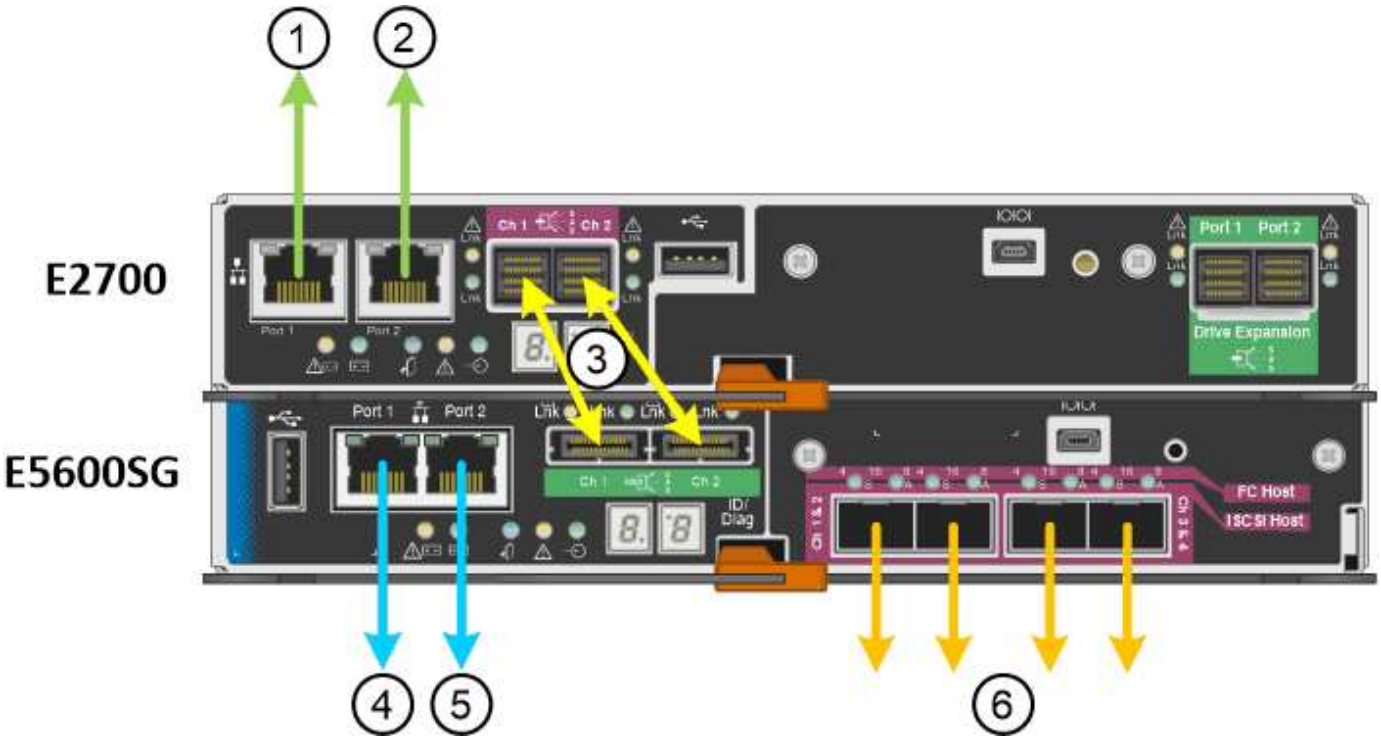
- **Red de Grid para StorageGRID**: La red de red se utiliza para todo el tráfico interno de StorageGRID. Proporciona conectividad entre todos los nodos de la cuadrícula, en todos los sitios y subredes. Se requiere la red de red.
- **Red de administración para StorageGRID**: La Red de administración es una red cerrada que se utiliza para la administración y el mantenimiento del sistema. La red de administración suele ser una red privada y no es necesario que se pueda enrutar entre sitios. La red administrativa es opcional.
- **Red de clientes para StorageGRID**: La red de clientes es una red abierta que se utiliza para proporcionar acceso a las aplicaciones cliente, incluidos S3 y Swift. La red de cliente proporciona acceso de protocolo de cliente a la cuadrícula, de modo que la red de red de red pueda aislarse y protegerse. La red cliente es opcional.
- **Red de administración para el Administrador de almacenamiento de SANtricity** (opcional): El controlador E2700 se conecta a la red de administración donde está instalado el Administrador de almacenamiento de SANtricity, lo que le permite supervisar y administrar los componentes de hardware del dispositivo. Esta red de gestión puede ser la misma que la Red de administración para StorageGRID, o bien puede ser una red de gestión independiente.

  Si la red opcional de Administrador de almacenamiento de SANtricity no está conectada, es posible que no pueda utilizar algunas funciones de SANtricity.

> Para obtener información detallada acerca de las redes StorageGRID, consulte *Grid primer*.

Conexiones de dispositivos StorageGRID

Al instalar un dispositivo StorageGRID, debe conectar las dos controladoras entre sí y a las redes necesarias. La figura muestra las dos controladoras en SG5660, con la controladora E2700 en la parte superior y la controladora E5600SG en la parte inferior. En SG5612, la controladora E2700 se encuentra a la izquierda de la controladora E5600SG.



Elemento	Puerto	Tipo de puerto	Función
1	Puerto de gestión 1 en la controladora E2700	Ethernet de 1 GB (RJ-45)	Conecta la controladora E2700 a la red en la que se ha instalado SANtricity Storage Manager.
2	Puerto de gestión 2 en la controladora E2700	Ethernet de 1 GB (RJ-45)	Conecta la controladora E2700 a un portátil de servicio durante la instalación.
3	Dos puertos de interconexión SAS de cada controladora, etiquetados como Ch 1 y Ch 2	Controladora E2700: Mini-SAS-HD Controladora E5600SG: Mini-SAS	Conecte las dos controladoras entre sí.
4	Puerto de gestión 1 en la controladora E5600SG	Ethernet de 1 GB (RJ-45)	Conecta la controladora E5600SG a la red de administrador para StorageGRID.

Elemento	Puerto	Tipo de puerto	Función
5	Puerto de gestión 2 en la controladora E5600SG	Ethernet de 1 GB (RJ-45)	• Se puede unir al puerto de administración 1 si desea una conexión redundante a la red de administración. • Puede dejarse sin cables y disponible para acceso local temporal (IP 169.254.0.1). • Se puede utilizar para conectar el controlador E5600SG a un portátil de servicio durante la instalación si no hay disponible una dirección IP asignada por DHCP.
6	Cuatro puertos de red en la controladora E5600SG	10 GbE (óptico)	Conéctese a la red de red y a la red de cliente para StorageGRID. Consulte «'conexiones de puertos 10 GbE para la controladora E5600SG'».

Información relacionada

Modos de enlace de puertos para los puertos de la controladora E5600SG

Recopilar información de instalación (SG5600)

Dispositivo de cable (SG5600)

Directrices sobre redes

Instale VMware

Instale Red Hat Enterprise Linux o CentOS

Instalar Ubuntu o Debian

Modos de enlace de puertos para los puertos de la controladora E5600SG

Al configurar los enlaces de red para los puertos de controladoras E5600SG, puede utilizar la vinculación de puertos para los puertos 10-GbE que se conectan a la red de grid y la red de cliente opcional, y los puertos de gestión de 1-GbE que se conectan a la red de administración opcional. El enlace de puertos ayuda a proteger los datos

proporcionando rutas redundantes entre las redes StorageGRID y el dispositivo.

Información relacionada

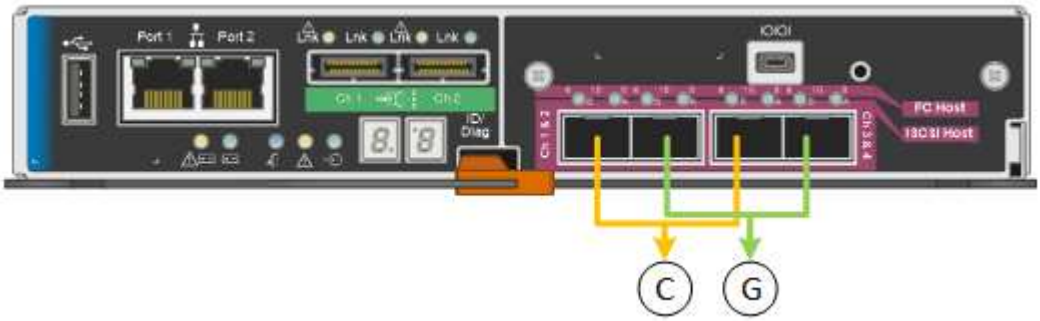
Configurar enlaces de red (SG5600)

Modos de enlace de red para puertos de 10 GbE

Los puertos de red de 10 GbE de la controladora E5600SG admiten el modo de enlace de puerto fijo o el modo de enlace de puerto agregado para las conexiones de red de grid y red de cliente.

Modo de enlace de puerto fijo

El modo fijo es la configuración predeterminada para los puertos de red de 10 GbE.



Llamada	Qué puertos están Unidos
C	Los puertos 1 y 3 se unen para la red cliente, si se utiliza esta red.
G	Los puertos 2 y 4 están Unidos para la red de cuadrícula.

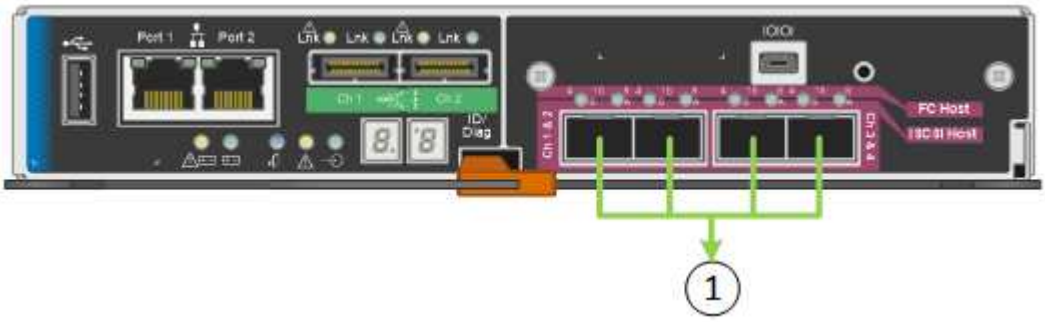
Cuando se utiliza el modo de enlace de puerto fijo, los puertos se pueden enlazar mediante el modo de copia de seguridad activa o el modo de protocolo de control de agregación de enlaces (LACP 802.3ad).

- En el modo activo-backup (predeterminado), solo hay un puerto activo a la vez. Si se produce un error en el puerto activo, su puerto de backup proporciona automáticamente una conexión de conmutación por error. El puerto 4 proporciona una ruta de copia de seguridad para el puerto 2 (red de red de cuadrícula) y el puerto 3 proporciona una ruta de copia de seguridad para el puerto 1 (red de cliente).
- En el modo LACP, cada par de puertos forma un canal lógico entre la controladora y la red, lo que permite un mayor rendimiento. Si un puerto falla, el otro continúa proporcionando el canal. El rendimiento se reduce, pero la conectividad no se ve afectada.

> Si no necesita conexiones redundantes, sólo puede utilizar un puerto para cada red. Sin embargo, tenga en cuenta que se generará una alarma en el administrador de grid después de instalar StorageGRID, lo que indica que se ha desenchufado un cable. Puede reconocer esta alarma de forma segura para borrarla.

Modo de enlace de puerto agregado

El modo de enlace de puerto de agregado aumenta de forma significativa las mejoras en cada red StorageGRID y proporciona rutas de conmutación al nodo de respaldo adicionales.



Llamada	Qué puertos están Unidos
1	Todos los puertos conectados se agrupan en un único enlace LACP, lo que permite que todos los puertos se usen para el tráfico de red de grid y de red de cliente.

Si tiene pensado utilizar el modo de enlace de puerto agregado:

- Debe usar el modo de enlace de red LACP.
- Debe especificar una etiqueta de VLAN exclusiva para cada red. Esta etiqueta VLAN se añadirá a cada paquete de red para garantizar que el tráfico de red se dirija a la red correcta.
- Los puertos deben estar conectados a switches que sean compatibles con VLAN y LACP. Si varios switches participan en el enlace LACP, los switches deben ser compatibles con los grupos de agregación de enlaces de varios chasis (MLAG), o equivalentes.
- Debe comprender cómo configurar los switches para que utilicen VLAN, LACP y MLAG, o equivalente.

Si no desea usar los cuatro puertos de 10-GbE, puede usar uno, dos o tres puertos. El uso de más de un puerto maximiza la posibilidad de que cierta conectividad de red permanezca disponible si falla uno de los puertos de 10 GbE.

> Si decide utilizar menos de cuatro puertos, tenga en cuenta que puede activarse una alerta * de enlace de dispositivo de servicios* en Grid Manager después de instalar el nodo del dispositivo, lo que indica que se ha desenchufado un cable. Puede deshabilitar con seguridad esta regla de alerta para la alerta activada. En Grid Manager, seleccione **ALERTS** > **Reglas**, seleccione la regla y haga clic en **Editar regla**. A continuación, desactive la casilla de verificación **Activado**.

Modos de enlace de red para puertos de gestión de 1 GbE

Para los dos puertos de gestión de 1 GbE en la controladora E5600SG, puede elegir modo de enlace de red independiente o modo de enlace de red Active-Backup para conectarse con la red de administrador opcional.

En modo independiente, solo el puerto de gestión 1 está conectado a la red del administrador. Este modo no proporciona una ruta de acceso redundante. El puerto de administración 2 no tiene cables y está disponible para las conexiones locales temporales (utilice la dirección IP 169.254.0.1)

En el modo Active-Backup, los puertos de gestión 1 y 2 están conectados a la red Admin. Solo hay un puerto activo a la vez. Si se produce un error en el puerto activo, su puerto de backup proporciona automáticamente una conexión de conmutación por error. La vinculación de estos dos puertos físicos en un puerto de gestión lógica proporciona una ruta redundante a la red de administración.

> Si necesita establecer una conexión local temporal con la controladora E5600SG cuando los puertos de gestión de 1-GbE están configurados para modo Active-Backup, quite los cables de ambos puertos de gestión, enchufe el cable temporal al puerto de gestión 2 y acceda al dispositivo con la dirección IP 169.254.0.1.

Recopilar información de instalación (SG5600)

Al instalar y configurar el dispositivo StorageGRID, debe tomar decisiones y recopilar información acerca de los puertos del switch Ethernet, las direcciones IP y los modos de enlace de puerto y red.

Acerca de esta tarea

Puede utilizar las siguientes tablas para registrar la información de cada red que conecte al dispositivo. Estos valores son necesarios para instalar y configurar el hardware.

Información necesaria para conectar la controladora E2700 a SANtricity Storage Manager

Debe conectar la controladora E2700 a la red de gestión que utilizará para SANtricity Storage Manager.

Información necesaria	Su valor
El puerto del switch Ethernet se conectará al puerto de gestión 1	
Dirección MAC del puerto de gestión 1 (impreso en una etiqueta cerca del puerto P1)	
Dirección IP asignada por DHCP para el puerto de gestión 1, si está disponible después de encenderse **Nota:** Si la red que va a conectar al controlador E2700 incluye un servidor DHCP, el administrador de red puede utilizar la dirección MAC para determinar la dirección IP asignada por el servidor DHCP.	

Información necesaria	Su valor
Velocidad y modo doble **Nota:** debe asegurarse de que el conmutador Ethernet de la red de administración de SANtricity Storage Manager está establecido en Negotiate automático.	Debe ser: • Autonegociar (predeterminado)
Formato de dirección IP	Elija una opción: • IPv4 • IPv6
Dirección IP estática que planea usar para el dispositivo en la red de gestión	Para IPv4: • Dirección IPv4: • Máscara de subred: • Puerta de enlace: Para IPv6: • Dirección IPv6: • Dirección IP enrutable: • Dirección IP del enrutador de la controladora E2700:

Información necesaria para conectar el controlador E5600SG a la red de administrador

La red de administración de StorageGRID es una red opcional que se utiliza para la administración y el mantenimiento del sistema. El dispositivo se conecta a la red de administrador mediante los puertos de gestión de 1-GbE en la controladora E5600SG.

Información necesaria	Su valor
Red de administrador habilitada	Elija una opción: • No • Sí (predeterminado)
Modo de enlace de red	Elija una opción: • Independiente • Copia de seguridad activa
Puerto del switch para el puerto de gestión 1 (P1)	

Información necesaria	Su valor
Puerto de switch para el puerto de administración 2 (P2; activo-Backup, solo modo de enlace de red)	
Dirección MAC del puerto de gestión 1 (impreso en una etiqueta cerca del puerto P1)	
Dirección IP asignada por DHCP para el puerto de gestión 1, si está disponible después de encenderse **Nota:** Si la red Admin incluye un servidor DHCP, el controlador E5600SG muestra la dirección IP asignada por DHCP en su pantalla de siete segmentos después de que se inicie. También puede determinar la dirección IP asignada por DHCP utilizando la dirección MAC para buscar la IP asignada.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Dirección IP estática que piensa usar para el nodo de almacenamiento del dispositivo en la red de administración **Nota:** Si su red no tiene una puerta de enlace, especifique la misma dirección IPv4 estática para la puerta de enlace.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Subredes de red de administración (CIDR)	

La información necesaria para conectar y configurar puertos 10-GbE en la controladora E5600SG

Los cuatro puertos de 10 GbE del controlador E5600SG se conectan a la red de grid y la red de clientes de StorageGRID.

> Consulte "conexiones de puertos de 10 GbE para la controladora E5600SG" para obtener más información acerca de las opciones de estos puertos.

Información necesaria	Su valor
Modo de enlace de puerto	Elija una opción: • Fijo (predeterminado) • Agregado
Puerto de conmutador para el puerto 1 (red cliente para modo fijo)	
Puerto de conmutador para el puerto 2 (red de cuadrícula para modo fijo)	

Información necesaria	Su valor
Puerto de conmutador para el puerto 3 (red cliente para modo fijo)	
Puerto de conmutador para el puerto 4 (red de cuadrícula para modo fijo)	

Información necesaria para conectar el controlador E5600SG a Grid Network

Grid Network para StorageGRID es una red necesaria que se utiliza para todo el tráfico interno de StorageGRID. El dispositivo se conecta a la red Grid mediante los puertos de 10 GbE en la controladora E5600SG.

> Consulte "conexiones de puertos de 10 GbE para la controladora E5600SG" para obtener más información acerca de las opciones de estos puertos.

Información necesaria	Su valor
Modo de enlace de red	Elija una opción: • Active-Backup (predeterminado) • LACP (802.3ad)
Etiquetado VLAN habilitado	Elija una opción: • No (predeterminado) • Sí
Etiqueta de VLAN (si el etiquetado de VLAN está habilitado)	Introduzca un valor entre 0 y 4095:
Dirección IP asignada por DHCP para la red de cuadrícula, si está disponible después del encendido **Nota:** Si Grid Network incluye un servidor DHCP, el controlador E5600SG muestra la dirección IP asignada por DHCP para la Red de cuadrícula en su pantalla de siete segmentos después de que se inicie.	• Dirección IPv4 (CIDR): • Puerta de enlace:
Dirección IP estática que tiene previsto usar para el nodo de almacenamiento del dispositivo en la red de grid **Nota:** Si su red no tiene una puerta de enlace, especifique la misma dirección IPv4 estática para la puerta de enlace.	• Dirección IPv4 (CIDR): • Puerta de enlace:

Información necesaria	Su valor
Subredes de red de cuadrícula (CIDR) **Nota:** Si la red de cliente no está activada, la ruta predeterminada del controlador utilizará la puerta de enlace especificada aquí.	

Información necesaria para conectar la controladora E5600SG a la red cliente

La red de cliente para StorageGRID es una red opcional que se utiliza para proporcionar acceso de protocolo de cliente a la cuadrícula. El dispositivo se conecta a la red cliente mediante los puertos 10-GbE de la controladora E5600SG.

> Consulte "conexiones de puertos de 10 GbE para la controladora E5600SG" para obtener más información acerca de las opciones de estos puertos.

Información necesaria	Su valor
Red de cliente habilitada	Elija una opción: • No (predeterminado) • Sí
Modo de enlace de red	Elija una opción: • Active-Backup (predeterminado) • LACP (802.3ad)
Etiquetado VLAN habilitado	Elija una opción: • No (predeterminado) • Sí
Etiqueta de VLAN (si el etiquetado de VLAN está habilitado)	Introduzca un valor entre 0 y 4095:
Dirección IP asignada por DHCP para la red cliente, si está disponible después del encendido	• Dirección IPv4 (CIDR): • Puerta de enlace:
Dirección IP estática que tiene previsto usar para el nodo de almacenamiento del dispositivo en la red cliente **Nota:** Si la red de cliente está activada, la ruta predeterminada del controlador utilizará la puerta de enlace especificada aquí.	• Dirección IPv4 (CIDR): • Puerta de enlace:

Información relacionada

Revisar las conexiones de red del dispositivo (SG5600)

Configurar el hardware (SG5600)

Modos de enlace de puertos para puertos de controladoras E5600SG

Instalar el hardware (SG5600)

La instalación del hardware incluye varias tareas principales, como la instalación de componentes de hardware, el cableado de esos componentes y la configuración de puertos.

Registre el hardware

El registro del hardware del dispositivo proporciona ventajas de asistencia.

Pasos

1. Busque el número de serie del chasis.

   Puede encontrar el número en el recibo de embalaje, en el correo electrónico de confirmación o en el aparato después de desembalarlo.

2. Vaya al sitio de soporte de NetApp en "mysupport.netapp.com".
3. Determine si necesita registrar el hardware:

Si usted es un…	Siga estos pasos…
Cliente existente de NetApp	a. Inicie sesión con su nombre de usuario y contraseña. b. Seleccione **Productos** > **Mis productos**. c. Confirme que el nuevo número de serie aparece en la lista. d. De lo contrario, siga las instrucciones para nuevos clientes de NetApp.
Nuevo cliente de NetApp	a. Haga clic en **Registrar ahora** y cree una cuenta. b. Seleccione **Productos** > **Registrar productos**. c. Introduzca el número de serie del producto y los detalles solicitados. Una vez aprobado el registro, puede descargar el software necesario. El proceso de aprobación puede llevar hasta 24 horas.

Instale el dispositivo en un armario o rack (SG5600)

Debe instalar rieles en su armario o rack y, a continuación, deslizar el dispositivo sobre los rieles. Si tiene un SG5660, también debe instalar las unidades después de instalar el dispositivo.

Lo que necesitará

- Ha revisado el documento de avisos de seguridad que se incluye en la caja y comprende las precauciones para mover e instalar el hardware.
- Tiene las instrucciones de instalación de E-Series para el hardware.

Instale el hardware desde la parte inferior del rack, armario o rack hasta para evitar que el equipo vuelque.

SG5612 pesa aproximadamente 27 kg (60 lb) cuando está totalmente cargado con unidades. Se requiere que dos personas o un elevador mecánico muevan de forma segura el SG5612.

SG5660 pesa aproximadamente 60 kg (132 lb) sin unidades instaladas. Se requiere que cuatro personas o un ascensor mecanizado muevan de forma segura un dispositivo SG5660 vacío.

Para evitar dañar el hardware, no mueva nunca un dispositivo SG5660 si hay unidades instaladas. Debe quitar todas las unidades antes de mover el aparato.

Acerca de esta tarea

Complete las siguientes tareas para instalar el dispositivo SG5660 en un armario o rack.

- **Instale los raíles de montaje**

  Instale los raíles de montaje en el armario o rack.

  Consulte las instrucciones de instalación de E-Series para E2700 o E5600.

- **Instale el aparato en el armario o rack**

  Deslice el aparato en el armario o rack y fíjelo.

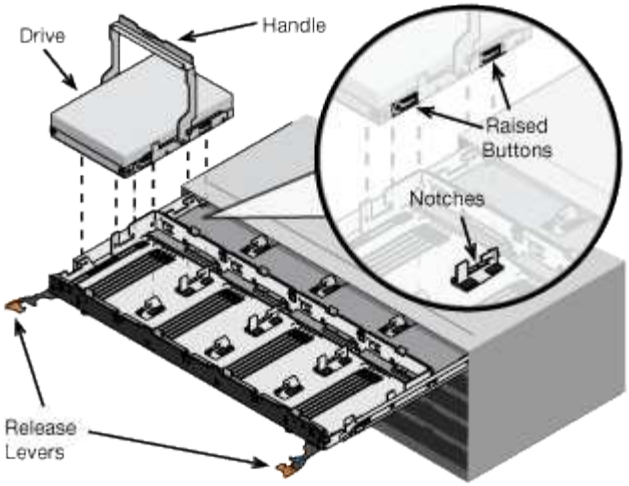
  Si está levantando el dispositivo SG5660 a mano, fije las cuatro asas a los lados del chasis. Retire estas asas mientras desliza el aparato sobre los rieles.

- **Instale las unidades**

  Si tiene un SG5660, instale 12 unidades en cada uno de los 5 cajones de unidades.

  Debe instalar las 60 unidades para garantizar que su funcionamiento es correcto.

  a. Coloque la muñequera ESD y retire los accionamientos de su embalaje.
  b. Suelte las palancas del cajón de mando superior y deslice el cajón hacia fuera con las palancas.
  c. Levante el asa de la unidad a la posición vertical y alinee los botones de la unidad con las muescas del cajón.



d. Al presionar suavemente en la parte superior de la unidad, gire la palanca de mando hacia abajo hasta que la unidad encaje en su lugar.

e. Después de instalar los primeros 12 mandos, deslice el cajón hacia atrás presionando el centro y cerrando ambas palancas con cuidado.

f. Repita estos pasos para los otros cuatro cajones.

- **Fije el bisel frontal**

  SG5612: Fije las tapas de los extremos izquierdo y derecho al frente.

  SG5660: Fije el bisel en la parte delantera.

Información relacionada

"Guía de instalación de soporte de unidades de controladora E2700 y soportes de unidades relacionadas"

"Guía de instalación de soporte de unidades de controladora E5600 y soportes de unidades relacionadas"

Dispositivo de cable (SG5600)

Debe conectar las dos controladoras entre sí mediante cables de interconexión SAS, conectar los puertos de gestión a la red de gestión adecuada y conectar los puertos de 10 GbE de la controladora E5600SG a la red de grid y la red de cliente opcional para StorageGRID.

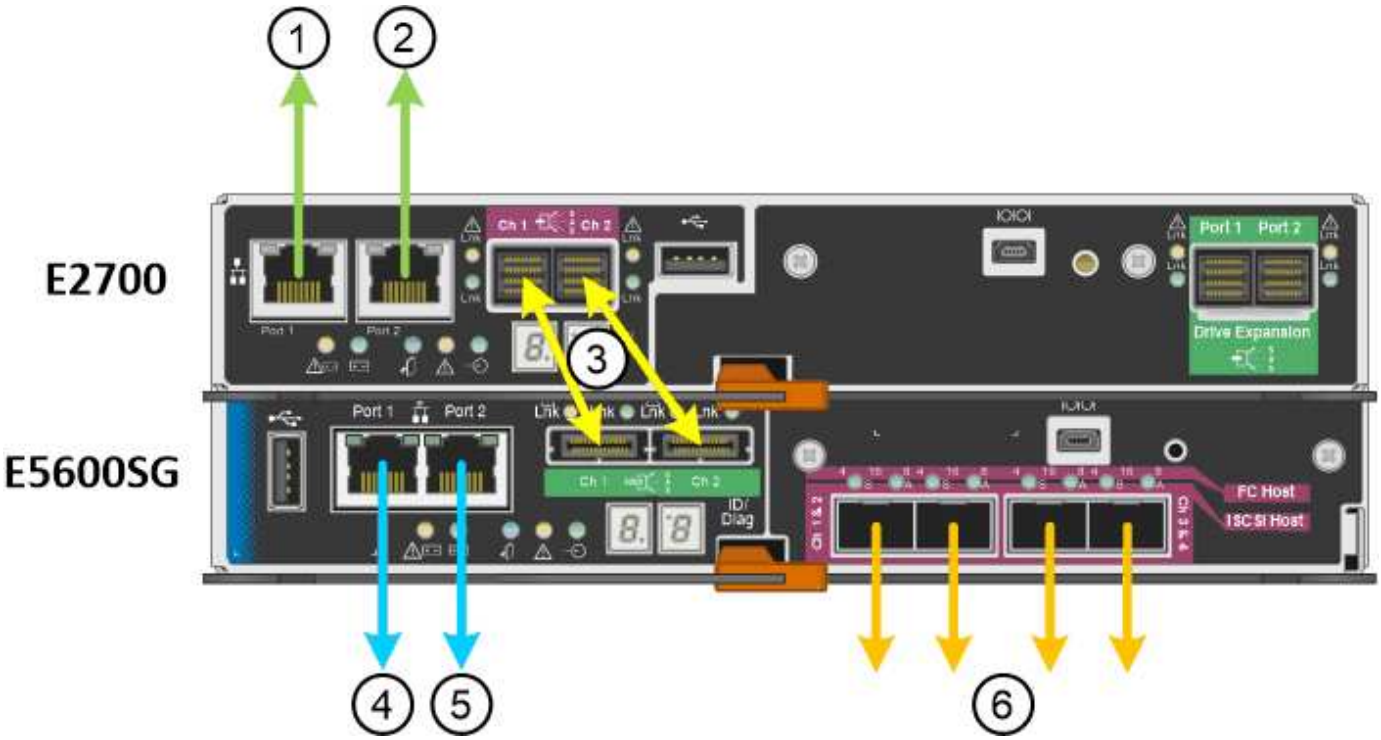
Lo que necesitará

- Tiene cables Ethernet para conectar los puertos de gestión.
- Dispone de cables ópticos para conectar los cuatro puertos de 10 GbE (no se suministran con el dispositivo).

> **Riesgo de exposición a la radiación láser** — no desmonte ni retire ninguna parte de un transceptor SFP. Puede que esté expuesto a la radiación láser.

Acerca de esta tarea

Al conectar los cables, consulte el siguiente diagrama, donde se muestra la controladora E2700 en la parte superior y la controladora E5600SG en la parte inferior. El diagrama muestra el modelo de SG5660; las controladoras del modelo SG5612 están junto a él en lugar de apilarse.



Elemento	Puerto	Tipo de puerto	Función
1	Puerto de gestión 1 en la controladora E2700	Ethernet de 1 GB (RJ-45)	Conecta la controladora E2700 a la red en la que se ha instalado SANtricity Storage Manager.
2	Puerto de gestión 2 en la controladora E2700	Ethernet de 1 GB (RJ-45)	Conecta la controladora E2700 a un portátil de servicio durante la instalación.
3	Dos puertos de interconexión SAS de cada controladora, etiquetados como Ch 1 y Ch 2	Controladora E2700: Mini-SAS-HD Controladora E5600SG: Mini-SAS	Conecte las dos controladoras entre sí.
4	Puerto de gestión 1 en la controladora E5600SG	Ethernet de 1 GB (RJ-45)	Conecta la controladora E5600SG a la red de administrador para StorageGRID.

Elemento	Puerto	Tipo de puerto	Función
5	Puerto de gestión 2 en la controladora E5600SG	Ethernet de 1 GB (RJ-45)	• Se puede unir al puerto de administración 1 si desea una conexión redundante a la red de administración. • Puede dejarse sin cables y disponible para acceso local temporal (IP 169.254.0.1). • Se puede utilizar para conectar la controladora E5600SG a un portátil de servicio durante la instalación si las direcciones IP asignadas por DHCP no están disponibles.
6	Cuatro puertos de red en la controladora E5600SG	10 GbE (óptico)	Conecte la controladora E5600SG a la red de cuadrícula y a la red de cliente (si se utiliza) para StorageGRID. Los puertos se pueden unir para proporcionar rutas redundantes a la controladora.

Pasos

1. Conecte la controladora E2700 a la controladora E5600SG mediante los dos cables de interconexión SAS.

Conectar este puerto…	A este puerto…
Puerto de interconexión SAS 1 (con la etiqueta Ch 1) en la controladora E2700	Puerto de interconexión SAS 1 (con la etiqueta Ch 1) en la controladora E5600SG
Puerto de interconexión SAS 2 (con la etiqueta Ch 2) en la controladora E2700	Puerto de interconexión SAS 2 (con la etiqueta Ch 2) en la controladora E5600SG

Utilice el conector cuadrado (mini-SAS HD) de la controladora E2700 y utilice el conector rectangular (mini-SAS) de la controladora E5600SG.

> Asegúrese de que las pestañas de los conectores SAS están en la parte inferior e inserte con cuidado cada conector hasta que encaje en su lugar. No empujar el conector si hay resistencia. Compruebe la posición de la lengüeta de tiro antes de continuar.

2. Conecte la controladora E2700 a la red de gestión donde está instalado el software SANtricity Storage Manager mediante un cable Ethernet.

Conectar este puerto…	A este puerto…
Puerto 1 de la controladora E2700 (el puerto RJ-45 de la izquierda).	Cambie el puerto de la red de gestión que utiliza SANtricity Storage Manager
Puerto 2 en la controladora E2700	Service laptop, si no utiliza DHCP

3. Si planea utilizar la red de administración para StorageGRID, conecte el controlador E5600SG mediante un cable Ethernet.

Conectar este puerto…	A este puerto…
Puerto 1 en el controlador E5600SG (el puerto RJ-45 a la izquierda)	Cambie el puerto de la red de administración para StorageGRID
Puerto 2 en el controlador E5600SG	Service laptop, si no utiliza DHCP

4. Conecte los puertos de 10 GbE de la controladora E5600SG a los switches de red adecuados, utilizando cables ópticos y transceptores SFP+.
   - Si piensa utilizar el modo de enlace de puerto fijo (predeterminado), conecte los puertos a la red de StorageGRID y a las redes de cliente, como se muestra en la tabla.

Puerto	Conecta a…
Puerto 1	Red de cliente (opcional)
Puerto 2	Red Grid
Puerto 3	Red de cliente (opcional)
Puerto 4	Red Grid

   - Si planea utilizar el modo de enlace de puerto agregado, conecte uno o varios puertos de red a uno o varios switches. Debe conectar al menos dos de los cuatro puertos para evitar tener un único punto de error. Si utiliza más de un switch para un único vínculo LACP, los switches deben ser compatibles con MLAG o equivalente.

Información relacionada

Modos de enlace de puertos para los puertos de la controladora E5600SG

Acceda al instalador de dispositivos de StorageGRID

Conexión de los cables de alimentación de CA (SG5600)

Debe conectar los cables de alimentación de CA a la fuente de alimentación externa y al conector de alimentación de CA de cada controlador. Una vez que haya conectado los

cables de alimentación, podrá encender la alimentación.

Lo que necesitará

Ambos interruptores de alimentación del aparato deben estar apagados antes de conectar la alimentación.

> **Riesgo de descarga eléctrica** — antes de conectar los cables de alimentación, asegúrese de que los dos interruptores de alimentación del aparato están apagados.

Acerca de esta tarea

- Debe utilizar fuentes de alimentación independientes para cada fuente de alimentación.

  La conexión a fuentes de alimentación independientes mantiene la redundancia de energía.

- Puede utilizar los cables de alimentación que se suministran con el controlador con tomas de corriente típicas utilizadas en el país de destino, como tomas de corriente de una fuente de alimentación ininterrumpida (UPS).

  Sin embargo, estos cables de alimentación no están diseñados para utilizarse en la mayoría de los armarios compatibles con EIA.

Pasos

1. Apague los interruptores de alimentación del compartimento o chasis.
2. Apague los switches de alimentación de las controladoras.
3. Conecte los cables de alimentación primarios del armario a las fuentes de alimentación externas.
4. Conecte los cables de alimentación al conector de alimentación de CA de cada controladora.

Encender la alimentación (SG5600)

Encender el compartimento proporciona alimentación a ambas controladoras.

Pasos

1. Encienda los dos interruptores de la fuente de alimentación situados en la parte posterior del gabinete.

   Mientras se aplica la alimentación, los LED de los controladores se encienden y se apagan intermitentemente.

   El proceso de encendido puede tardar hasta diez minutos en completarse. Las controladoras se reinician varias veces durante la secuencia de inicio inicial, lo que provoca que los ventiladores aumenten o reduzcan su capacidad y los LED parpadeen.

2. Compruebe el LED de alimentación y los LED de enlace de host activo de cada controladora para verificar que se encendió la alimentación.
3. Espere a que todas las unidades muestren un LED verde persistente, que indica que se han conectado.
4. Compruebe si hay LED verdes en la parte delantera y trasera del alojamiento.

   Si ve algún LED ámbar, anote sus ubicaciones.

5. Observe la pantalla de siete segmentos de la controladora E5600SG.

   Esta pantalla muestra **HO**, seguido de una secuencia de repetición de dos dígitos.

```
HO -- IP address for Admin Network -- IP address for Grid Network HO
```

En la secuencia, el primer conjunto de números es la dirección IP asignada por DHCP para el puerto de gestión 1 de la controladora. Esta dirección se utiliza para conectar la controladora a la red del administrador para StorageGRID. El segundo conjunto de números es la dirección IP asignada por DHCP utilizada para conectar el dispositivo a la red de cuadrícula para StorageGRID.

Si no se pudo asignar una dirección IP con DHCP, se muestra 0.0.0.0.

Ver el estado de arranque y revisar los códigos de error en controladoras SG5600

La pantalla de siete segmentos de cada controladora muestra los códigos de estado y error cuando el dispositivo se enciende, mientras el hardware se está inicializando y cuando el hardware falla y debe salir de la inicialización. Si está supervisando el progreso o solucionando problemas, debe observar la secuencia de los códigos tal como aparecen.

Acerca de esta tarea

Los códigos de estado y de error de la controladora E5600SG no son los mismos que los de la controladora E2700.

Pasos

1. Durante el arranque, consulte los códigos que se muestran en las pantallas de siete segmentos para supervisar el progreso.
2. Para revisar los códigos de error del controlador E5600SG, consulte el estado de visualización de siete segmentos e información sobre códigos de error.
3. Para revisar los códigos de error de la controladora E2700, consulte la documentación de la controladora E2700 en el sitio de soporte.

Información relacionada

códigos de visualización de siete segmentos de la controladora E5600SG

"Documentación de NetApp: Serie E2700"

códigos de visualización de siete segmentos de la controladora E5600SG

La pantalla de siete segmentos del controlador E5600SG muestra códigos de estado y error mientras el dispositivo se enciende y mientras el hardware se está inicializando. Puede utilizar estos códigos para determinar el estado y solucionar errores.

Al revisar los códigos de estado y de error en el controlador E5600SG, debe consultar los siguientes tipos de códigos:

- **códigos generales de arranque**

  Representa los eventos de inicio estándar.

- **códigos de arranque normales**

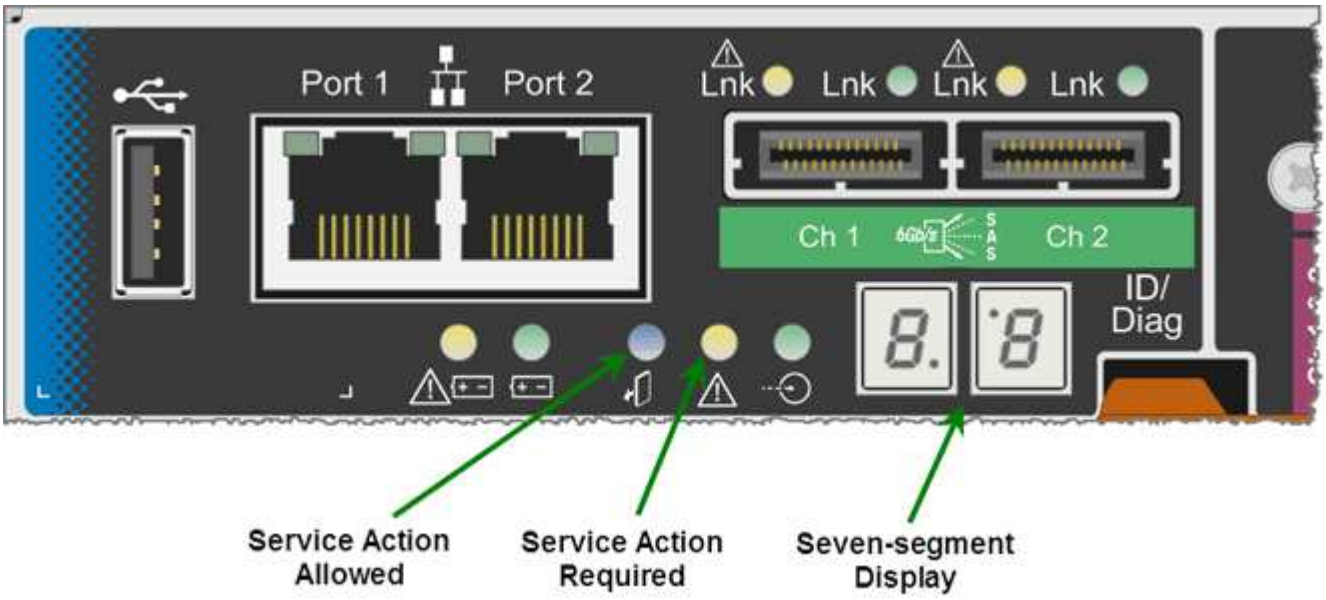
Representa los eventos de inicio normales que se producen en el dispositivo.

- **códigos de error**

  Indique los problemas durante los eventos de arranque.

StorageGRID controla únicamente los siguientes LED en el controlador E5600SG y solo después de que se haya iniciado el instalador de dispositivos StorageGRID:

- LED de permiso de acción de servicio
- LED de acción de servicio requerida
- Pantalla de siete segmentos



El dispositivo StorageGRID no utiliza los puntos decimales de la pantalla de siete segmentos:

- El punto decimal superior adyacente al dígito menos significativo es el LED de diagnóstico de la plataforma.

  Esto se activa durante el restablecimiento y la configuración inicial del hardware. De lo contrario, está desactivado.

- El punto decimal inferior adyacente al dígito más significativo se desactiva.

Para diagnosticar otros problemas, se recomienda tener en cuenta los siguientes recursos:

- Para ver toda la otra información de diagnóstico de hardware y entorno, consulte Diagnóstico de hardware del sistema operativo E-Series.

  Esto incluye la búsqueda de problemas de hardware como la alimentación, la temperatura y las unidades de disco. El dispositivo se basa en el sistema operativo E-Series para supervisar todos los Estados del entorno de la plataforma.

- Para determinar los problemas del firmware y de las unidades, observe las luces de enlace en los puertos SAS y de red.

  Para obtener más detalles, consulte la documentación de E5600 para E-Series.

códigos generales de arranque

Durante el arranque o después de un restablecimiento completo del hardware, se encienden los LED de acción de servicio permitida y acción de servicio requerida mientras el hardware se inicializa. La visualización de siete segmentos muestra una secuencia de códigos que son los mismos para el hardware de E-Series y no específicos de la controladora E5600SG.

Durante el arranque, la matriz de puertas programables en campo (FPGA, por sus siglas en inglés) controla las funciones e inicialización del hardware.

Codificación	Indicación
19	Inicialización de FPGA.
68	Inicialización de FPGA.
…	Inicialización FPGA.ésta es una sucesión rápida de códigos.
AA	Arranque del BIOS de la plataforma.
FF	Arranque del BIOS completado.se trata de un estado intermedio antes de que la controladora E5600SG inicialice y gestione los LED para indicar el estado.

Después de que aparezcan los códigos AA y FF, aparecen los códigos de arranque normales o aparecen códigos de error. Además, se apagan los LED de acción de servicio permitida y acción de servicio requerida.

códigos de arranque normales

Estos códigos representan los eventos de arranque normales que se producen en el dispositivo, en orden cronológico.

Codificación	Indicación
HOLA	Se ha iniciado la secuencia de comandos de inicio maestra.
PP	El firmware de la plataforma FPGA está buscando actualizaciones.
HP	La tarjeta de interfaz del host (HIC) está buscando actualizaciones.
RB	Después de actualizar el firmware, el sistema se está reiniciando, si es necesario.

Codificación	Indicación
P F	Se completaron las comprobaciones de actualización del firmware. Iniciar el proceso (utmagent) para comunicarse con y gestionar la controladora E2700. Este proceso facilita el aprovisionamiento de dispositivos.
ÉL	El sistema se está sincronizando con el sistema operativo E-Series.
HC	Se está realizando la comprobación de la instalación de StorageGRID.
HO	Se están produciendo la administración de la instalación y la interfaz activa.
HA	El sistema operativo Linux y StorageGRID están en ejecución.

códigos de error de la controladora E5600SG

Estos códigos representan condiciones de error que pueden mostrarse en la controladora E5600SG a medida que el dispositivo se arranca. se muestran códigos hexadecimales adicionales de dos dígitos si se producen errores específicos de hardware de bajo nivel. Si alguno de estos códigos persiste durante más de un segundo o dos, o si no puede resolver el error siguiendo uno de los procedimientos de solución de problemas prescritos, póngase en contacto con el soporte técnico.

Codificación	Indicación
22	No se ha encontrado ningún registro de arranque maestro en ningún dispositivo de arranque.
23	No hay ninguna unidad SATA instalada.
2A, 2B	Bus atascado, no se pueden leer los datos del SPD del DIMM.
40	DIMM no válidos.
41	DIMM no válidos.
42	Error en la prueba de memoria.
51	Fallo de lectura del SPD.
92 a 96	Inicialización del bus PCI.

Codificación	Indicación
A0 a A3	Inicialización de la unidad SATA.
AB	Código de inicio alternativo.
AE	So de arranque.
EA	Error de entrenamiento DDR3.
E8	No hay memoria instalada.
UE	No se ha encontrado la secuencia de comandos de instalación.
EP	El código "ManageSGA" indica que ocurrió un error en la comunicación de la pregrid con la controladora E2700.

Información relacionada

Solucionar problemas de instalación de hardware (SG5600)

"Soporte de NetApp"

Configurar el hardware (SG5600)

Después de aplicar la alimentación al dispositivo, debe configurar Storage Manager de SANtricity, que es el software que utilizará para supervisar el hardware. También debe configurar las conexiones de red que utilizará StorageGRID.

Configurar conexiones StorageGRID (SG5600)

Para poder implementar un dispositivo StorageGRID como nodo de almacenamiento en un grid StorageGRID, debe configurar las conexiones entre el dispositivo y las redes que tiene pensado utilizar. Puede configurar las redes visitando el instalador de dispositivos de StorageGRID, incluido en la controladora E5600SG (la controladora de computación del dispositivo).

Acceda al instalador de dispositivos de StorageGRID

Debe acceder al instalador de dispositivos de StorageGRID para configurar las conexiones entre el dispositivo y las tres redes StorageGRID: La red de grid, la red de administrador (opcional) y la red de cliente (opcional).

Lo que necesitará

- Está utilizando un navegador web compatible.
- El dispositivo está conectado a todas las redes StorageGRID que tiene previsto utilizar.

- Conoce la dirección IP, la puerta de enlace y la subred del dispositivo en estas redes.
- Configuró los switches de red que planea utilizar.

Acerca de esta tarea

Cuando acceda por primera vez al instalador de dispositivos de StorageGRID, puede utilizar la dirección IP asignada por DHCP para la red de administración (suponiendo que el dispositivo esté conectado a la red de administración) o la dirección IP asignada por DHCP para la red de grid. Se recomienda usar la dirección IP para la red de administración. De lo contrario, si accede al instalador de dispositivos de StorageGRID con la dirección DHCP de la red de grid, puede perder la conexión con el instalador de dispositivos de StorageGRID al cambiar la configuración de los enlaces y al introducir una IP estática.

Pasos

1. Obtenga la dirección DHCP del dispositivo en la red de administración (si está conectada) o en la red de red (si la red de administración no está conectada).

   Puede realizar una de las siguientes acciones:

   - Proporcione la dirección MAC para el puerto de gestión 1 al administrador de red, para que puedan buscar la dirección DHCP para este puerto en la red de administración. La dirección MAC está impresa en una etiqueta en el controlador E5600SG, junto al puerto.
   - Observe la pantalla de siete segmentos en la controladora E5600SG. Si los puertos 1 y 10-GbE 2 y 4 de la controladora E5600SG están conectados a redes con servidores DHCP, la controladora intenta obtener direcciones IP asignadas dinámicamente cuando se enciende en el compartimento. Una vez que el controlador ha completado el proceso de encendido, su pantalla de siete segmentos muestra **HO**, seguido de una secuencia repetida de dos números.

     ```
     HO -- IP address for Admin Network -- IP address for Grid Network HO
     ```

     En la secuencia:

     - El primer conjunto de números es la dirección DHCP para el nodo de almacenamiento del dispositivo en la red de administración, si está conectado. Esta dirección IP se asigna al puerto de gestión 1 en la controladora E5600SG.
     - El segundo conjunto de números es la dirección DHCP del nodo de almacenamiento del dispositivo en la red de grid. Esta dirección IP se asigna a los puertos 10-GbE 2 y 4 cuando se aplica la primera alimentación al dispositivo.

       Si no se pudo asignar una dirección IP con DHCP, se muestra 0.0.0.0.

2. Si pudo obtener alguna de las direcciones DHCP:

   a. Abra un explorador Web en el portátil de servicios.

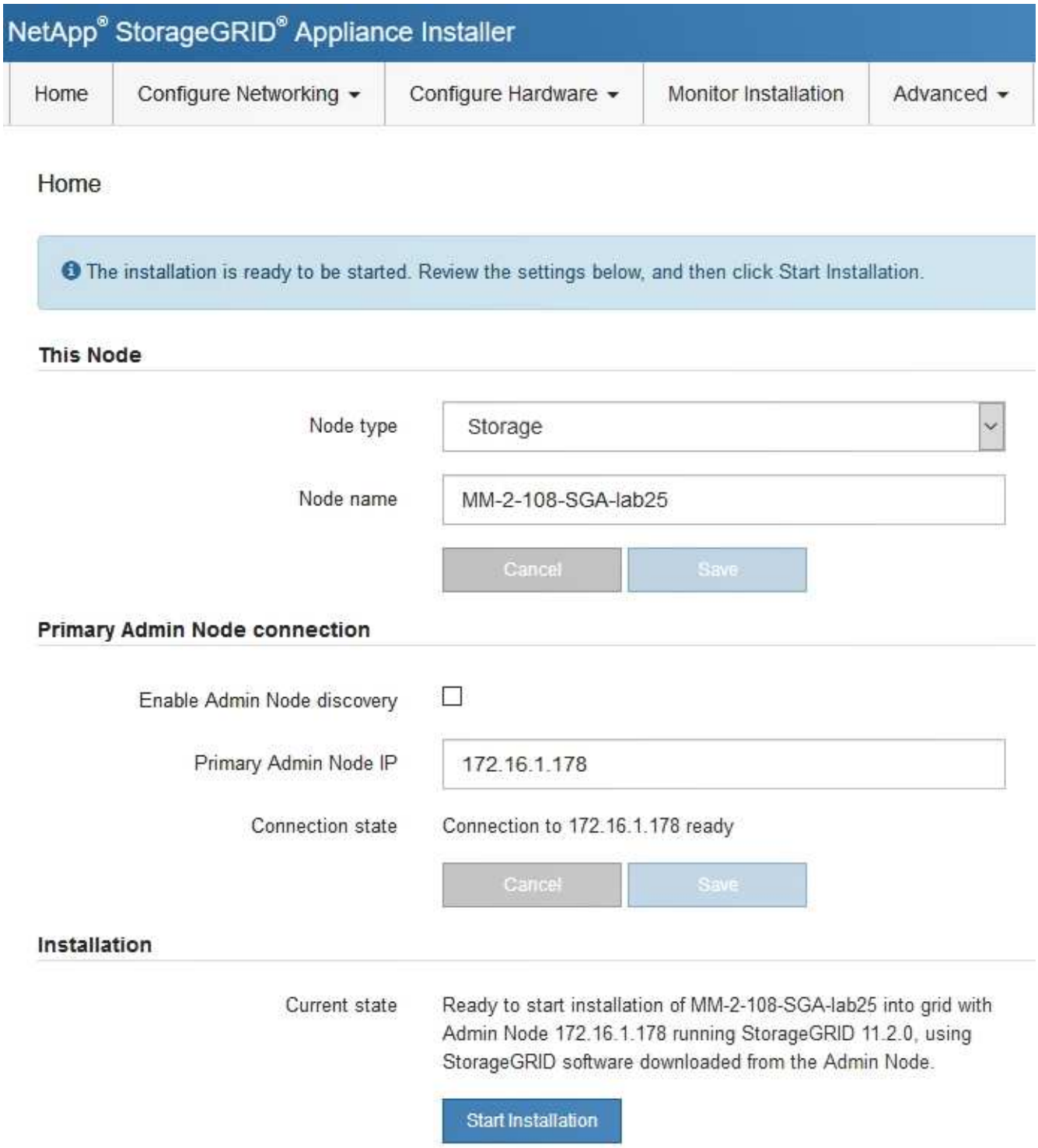
   b. Introduzca esta URL para el instalador del dispositivo StorageGRID:
      `https://E5600SG_Controller_IP:8443`

      Para *`E5600SG_Controller_IP`*, Utilice la dirección DHCP del controlador (utilice la dirección IP de la red de administración si la tiene).

   c. Si se le solicita una alerta de seguridad, vea e instale el certificado con el asistente de instalación del explorador.

La alerta no aparecerá la próxima vez que acceda a esta URL.

Aparece la página de inicio del instalador de dispositivos de StorageGRID. La información y los mensajes que se muestran cuando accede por primera vez a esta página dependen de cómo el dispositivo está conectado actualmente a redes StorageGRID. Pueden aparecer mensajes de error que se resolverán en pasos posteriores.



3. Si la controladora E5600SG no pudo adquirir una dirección IP con DHCP:

   a. Conecte el portátil de servicio al puerto de gestión 2 de la controladora E5600SG mediante un cable

Ethernet.

b. Abra un explorador Web en el portátil de servicios.

c. Introduzca esta URL para el instalador del dispositivo StorageGRID:
`https://169.254.0.1:8443`

Aparece la página de inicio del instalador de dispositivos de StorageGRID. La información y los mensajes que se muestran al acceder por primera vez a esta página dependen de cómo esté conectado el dispositivo actualmente.

> Si no puede acceder a la página de inicio a través de una conexión local de enlace, configure la dirección IP del portátil de servicio como `169.254.0.2`y vuelva a intentarlo.

4. Revise los mensajes que se muestran en la página Inicio y configure la configuración del vínculo y la configuración IP, según sea necesario.

Información relacionada

Requisitos del navegador web

Comprobar y actualizar la versión de StorageGRID Appliance Installer

La versión de instalador del dispositivo StorageGRID en el dispositivo debe coincidir con la versión de software instalada en el sistema StorageGRID para garantizar que todas las funciones de StorageGRID sean compatibles.

Lo que necesitará

Ha accedido al instalador de dispositivos de StorageGRID.

Los dispositivos StorageGRID vienen de fábrica preinstalados con el instalador de dispositivos StorageGRID. Si va a añadir un dispositivo a un sistema StorageGRID actualizado recientemente, es posible que deba actualizar manualmente el instalador de dispositivos StorageGRID antes de instalar el dispositivo como un nodo nuevo.

El instalador de dispositivos de StorageGRID se actualiza automáticamente cuando se actualiza a una nueva versión de StorageGRID. No es necesario actualizar el instalador de dispositivos StorageGRID en los nodos del dispositivo instalados. Este procedimiento sólo es necesario cuando se instala un dispositivo que contiene una versión anterior del instalador de dispositivos de StorageGRID.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Actualizar firmware**.
2. Compare la versión actual del firmware con la versión de software instalada en el sistema StorageGRID. (En la parte superior de Grid Manager, seleccione el icono de ayuda y seleccione **Acerca de**).

   El segundo dígito de las dos versiones debe coincidir. Por ejemplo, si el sistema StorageGRID está ejecutando la versión 11.**6**.*x*.*y*, la versión del instalador de dispositivos StorageGRID debe ser 3.**6**.*z*.

3. Si el dispositivo tiene una versión de nivel inferior del instalador de dispositivos de StorageGRID, vaya a.https://mysupport.netapp.com/site/products/all/details/storagegrid-appliance/downloads-tab["Descargas de NetApp: Dispositivo de StorageGRID"^].

   Inicie sesión con el nombre de usuario y la contraseña de su cuenta de NetApp.

4. Descargue la versión adecuada del archivo **Soporte para dispositivos StorageGRID** y el archivo de suma de comprobación correspondiente.

   El archivo de soporte para dispositivos StorageGRID es un `.zip` archivo que contiene las versiones de firmware actuales y anteriores para todos los modelos de dispositivos StorageGRID, en subdirectorios para cada tipo de controlador.

   Después de descargar el archivo de soporte para dispositivos StorageGRID, extraiga el `.zip` archive y consulte el archivo README para obtener información importante sobre la instalación del instalador de dispositivos StorageGRID.

5. Siga las instrucciones de la página actualización del firmware del instalador del dispositivo StorageGRID para realizar estos pasos:
   a. Cargue el archivo de soporte (imagen de firmware) apropiado para el tipo de controladora y el archivo de suma de comprobación.
   b. Actualice la partición inactiva.
   c. Reiniciar e intercambiar particiones.
   d. Actualice la segunda partición (inactiva).

Información relacionada

Acceda al instalador de dispositivos de StorageGRID

Configurar enlaces de red (SG5600)

Puede configurar los enlaces de red para los puertos utilizados para conectar el dispositivo a la red de grid, la red de cliente y la red de administración. Puede establecer la velocidad de enlace, así como los modos de enlace de red y puerto.

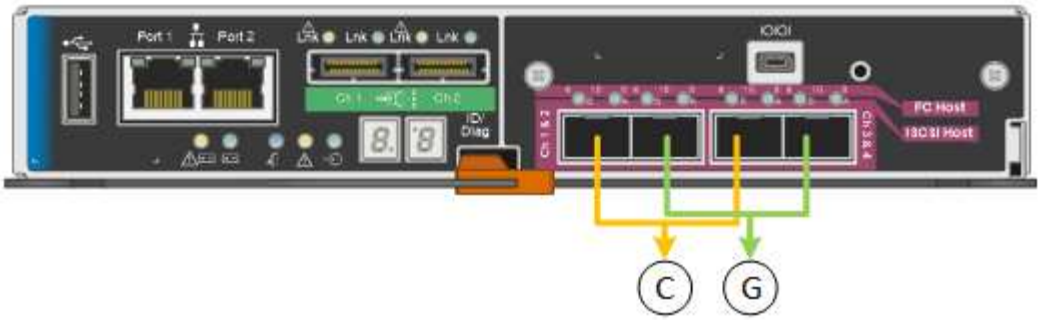
Lo que necesitará

Si planea utilizar el modo de enlace de puerto de agregado, el modo de enlace de red LACP o el etiquetado de VLAN:

- Conectó los puertos de 10-GbE del dispositivo a los switches que admiten VLAN y LACP.
- Si varios switches participan en el enlace LACP, los switches admiten grupos de agregación de enlaces de varios chasis (MLAG) o equivalente.
- Comprende cómo configurar los switches para que utilicen VLAN, LACP y MLAG o equivalente.
- Conoce la etiqueta de VLAN única que se utilizará para cada red. Esta etiqueta VLAN se añadirá a cada paquete de red para garantizar que el tráfico de red se dirija a la red correcta.

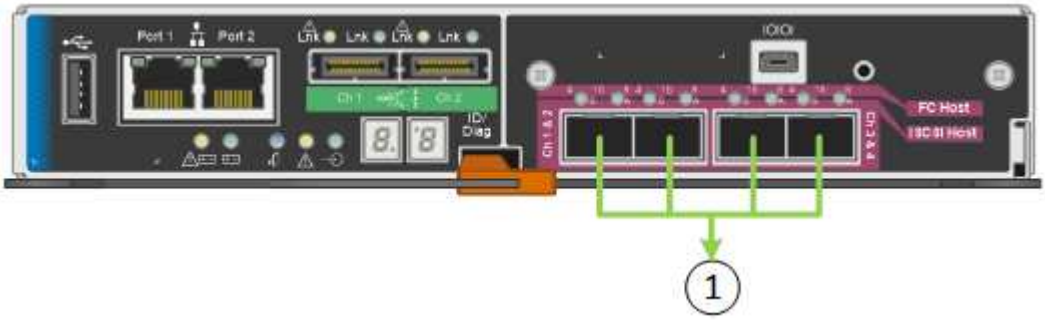
Acerca de esta tarea

En esta figura, se muestra cómo los cuatro puertos de 10 GbE se vinculan en modo de enlace de puerto fijo (configuración predeterminada).



Llamada	Qué puertos están Unidos
C	Los puertos 1 y 3 se unen para la red cliente, si se utiliza esta red.
G	Los puertos 2 y 4 están Unidos para la red de cuadrícula.

En esta figura, se muestra cómo los cuatro puertos de 10-GbE se encuentran Unidos en modo de enlace de puerto agregado.



Llamada	Qué puertos están Unidos
1	Los cuatro puertos se agrupan en un enlace LACP único, lo que permite que se usen todos los puertos para el tráfico de red de grid y de red de cliente.

La tabla resume las opciones para configurar los cuatro puertos de 10 GbE. Sólo tiene que configurar los ajustes en la página Configuración de vínculos si desea utilizar un valor no predeterminado.

- **Modo de enlace de puerto fijo (predeterminado)**

Modo de enlace de red	Red de cliente desactivada (predeterminada)	Red de cliente habilitada
Active-Backup (predeterminado)	• Los puertos 2 y 4 utilizan un vínculo de copia de seguridad activa para la red Grid. • Los puertos 1 y 3 no se usan. • Una etiqueta de VLAN es opcional.	• Los puertos 2 y 4 utilizan un vínculo de copia de seguridad activa para la red Grid. • Los puertos 1 y 3 utilizan un vínculo de backup activo para la red cliente. • Es posible especificar etiquetas de VLAN para ambas redes.
LACP (802.3ad)	• Los puertos 2 y 4 utilizan un enlace LACP para la red de grid. • Los puertos 1 y 3 no se usan. • Una etiqueta de VLAN es opcional.	• Los puertos 2 y 4 utilizan un enlace LACP para la red de grid. • Los puertos 1 y 3 utilizan un enlace LACP para la red de cliente. • Es posible especificar etiquetas de VLAN para ambas redes.

- **Modo de enlace de puerto agregado**

Modo de enlace de red	Red de cliente desactivada (predeterminada)	Red de cliente habilitada
Solo LACP (802.3ad)	• Los puertos 1-4 utilizan un enlace LACP único para la red de grid. • Una única etiqueta VLAN identifica los paquetes de red Grid.	• Los puertos 1-4 utilizan un enlace LACP único para la red de grid y la red de cliente. • Dos etiquetas VLAN permiten que los paquetes de red de cuadrícula se separen de los paquetes de red de cliente.

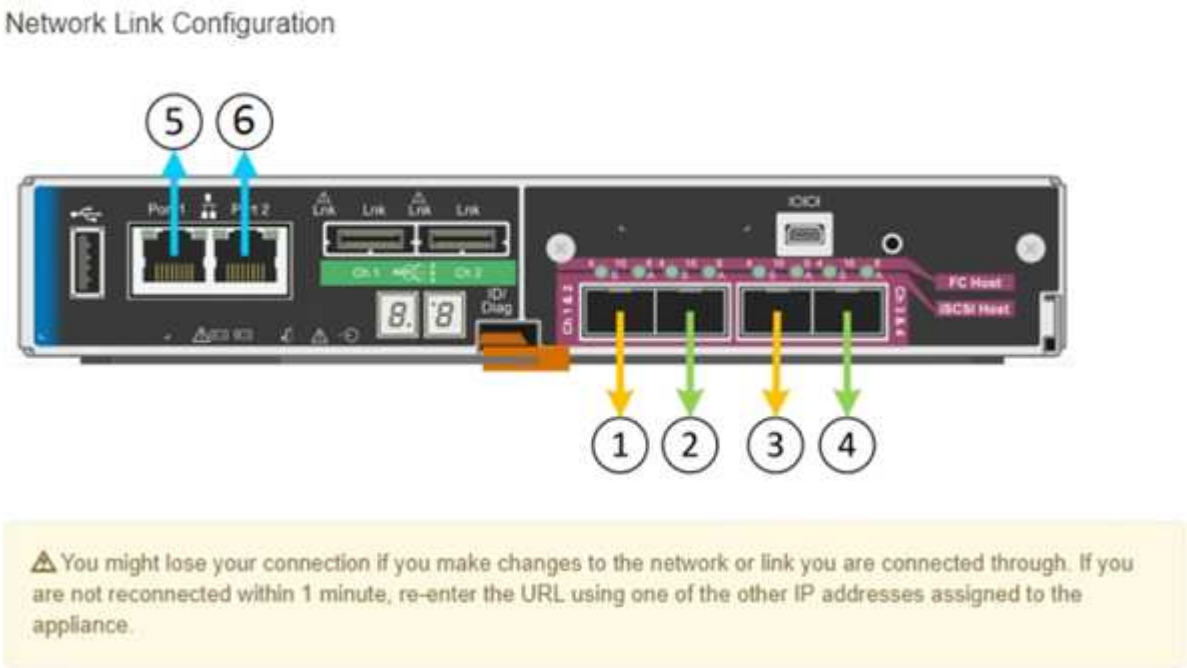
Consulte «'conexiones de puerto 10-GbE para el controlador E5600SG'» para obtener más información acerca de los modos de enlace de puerto y enlace de red.

En esta figura, se muestran cómo los dos puertos de gestión de 1-GbE de la controladora E5600SG están Unidos en el modo de enlace de red Active-Backup para la red Admin.

Pasos

1. En la barra de menús del instalador del dispositivo StorageGRID, haga clic en **Configurar redes** > **Configuración de vínculo**.

   La página Network Link Configuration muestra un diagrama del dispositivo con los puertos de red y administración numerados.



   La tabla Estado del enlace muestra el estado de los vínculos (arriba/abajo) y la velocidad (1/10/25/40/100 Gbps) de los puertos numerados.

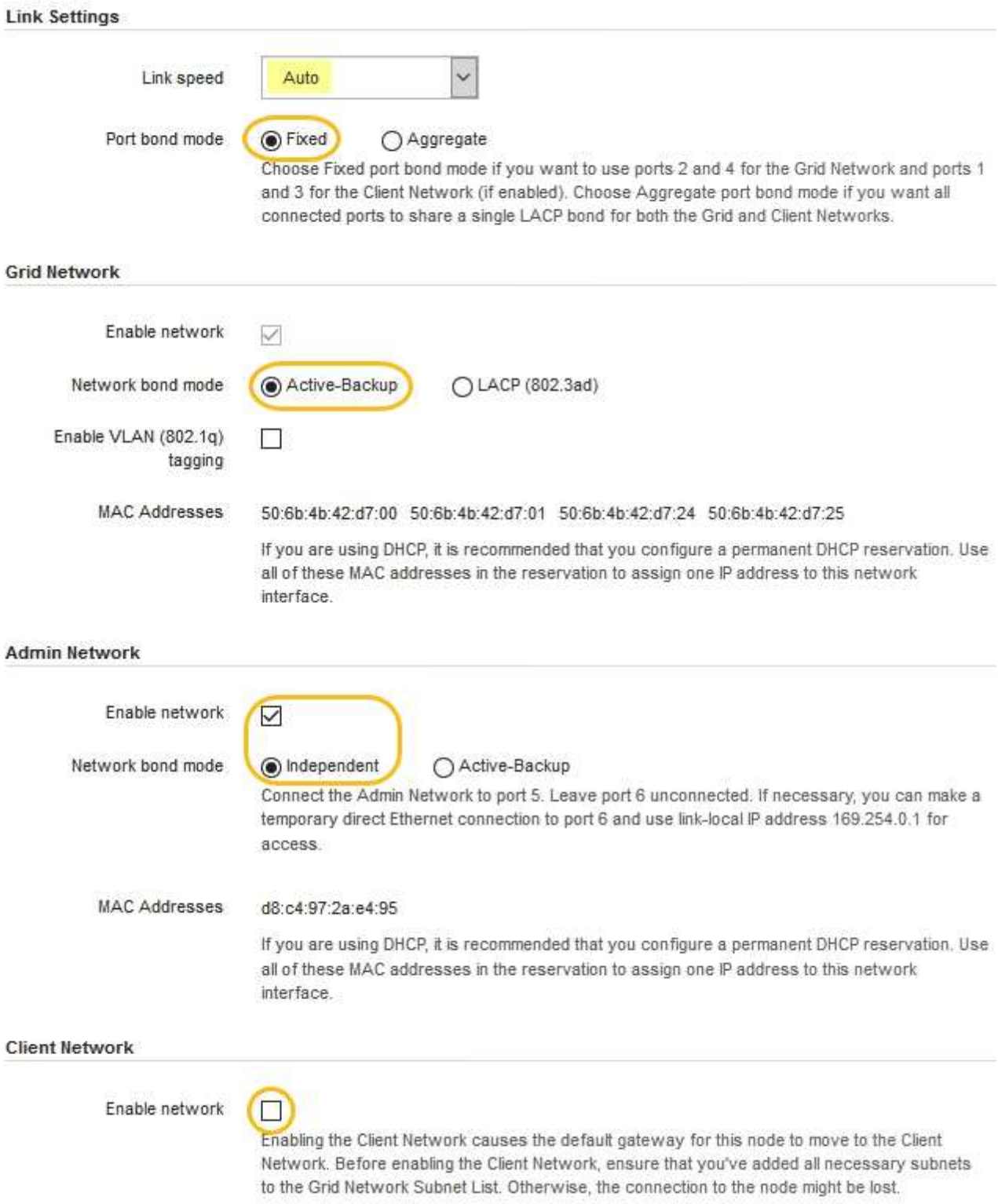
Link Status

Link	State	Speed (Gbps)
1	Down	N/A
2	Up	10
3	Up	10
4	Down	N/A
5	Up	1
6	Up	1

   La primera vez que acceda a esta página:

   - **Velocidad de enlace** se ajusta a **10 GbE**. Esta es la única velocidad de enlace disponible para el controlador E5600SG.
   - **El modo de enlace de puerto** está establecido en **fijo**.

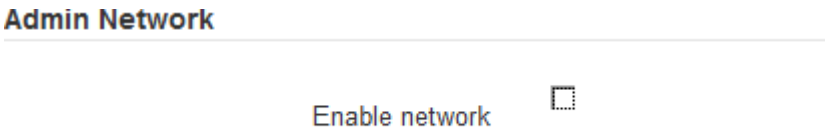
- **El modo de enlace de red** para la red Grid se establece en **Active-Backup**.
- La **Red de administración** está activada y el modo de enlace de red se establece en **independiente**.
- La **Red cliente** está desactivada.



2. Habilite o deshabilite las redes StorageGRID que tiene previsto utilizar.

   Se requiere la red de red. No se puede deshabilitar esta red.

a. Si el dispositivo no está conectado a la red de administración, anule la selección de la casilla de verificación **Activar red** para la red de administración.



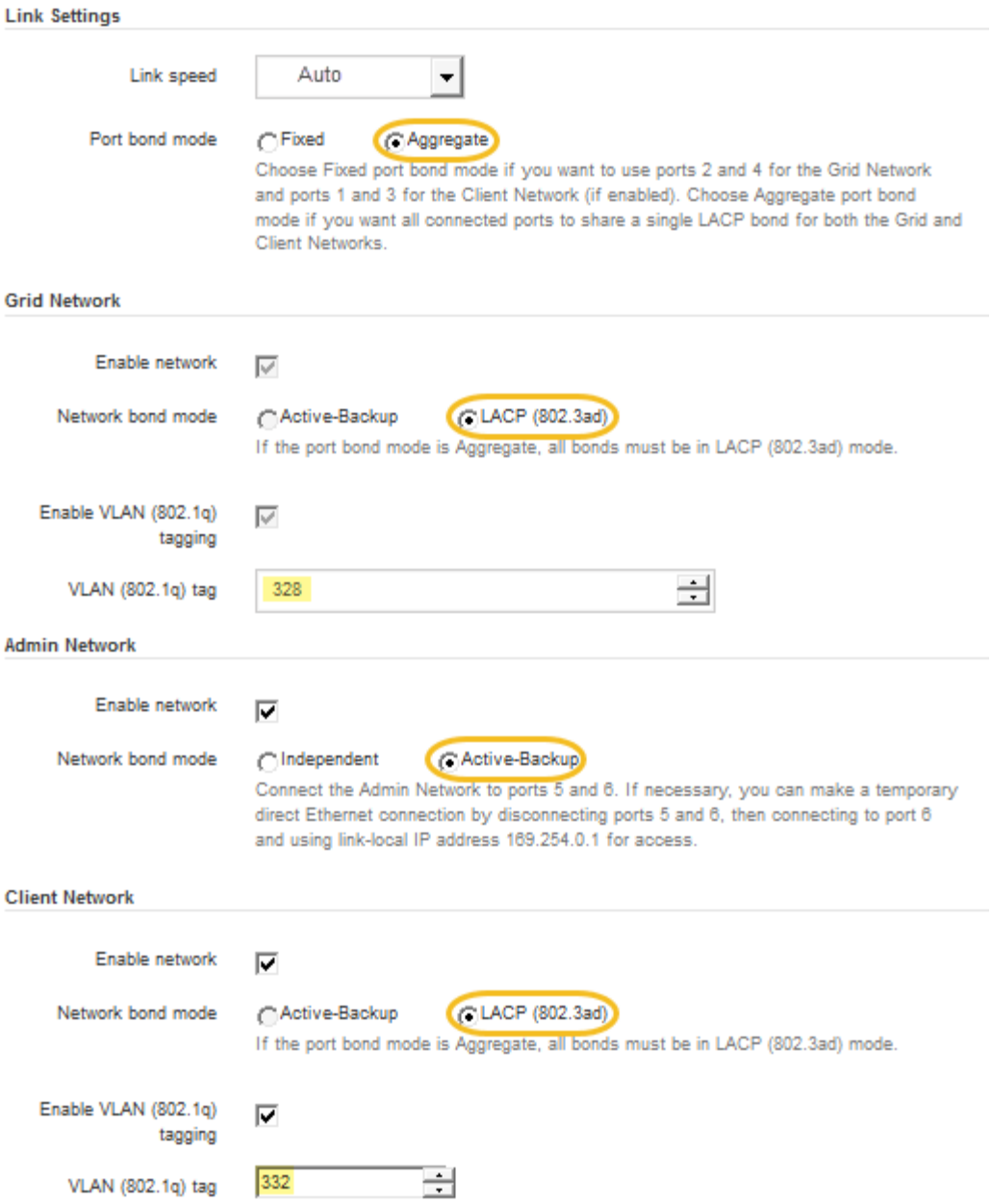
b. Si el dispositivo está conectado a la red cliente, seleccione la casilla de verificación **Activar red** de la red cliente.

   Ahora se muestran los ajustes de red de cliente para los puertos de 10-GbE.

3. Consulte la tabla y configure el modo de enlace de puerto y el modo de enlace de red.

   El ejemplo muestra:

   - **Agregado** y **LACP** seleccionados para las redes Grid y Client. Debe especificar una etiqueta de VLAN exclusiva para cada red. Puede seleccionar valores entre 0 y 4095.
   - **Active-Backup** seleccionado para la red de administración.



4. Cuando esté satisfecho con sus selecciones, haga clic en **Guardar**.

> Puede perder la conexión si ha realizado cambios en la red o el enlace que está conectado a través de. Si no vuelve a conectarse en un minuto, vuelva a introducir la URL del instalador de dispositivos StorageGRID utilizando una de las otras direcciones IP asignadas al dispositivo:
> **`https://E5600SG_Controller_IP:8443`**

Información relacionada

Modos de enlace de puertos para los puertos de la controladora E5600SG

Establezca la configuración de IP

El instalador de dispositivos StorageGRID se utiliza para configurar las direcciones IP y la información de enrutamiento utilizadas para el nodo de almacenamiento del dispositivo

en las redes de cliente, administrador y grid de StorageGRID.

Acerca de esta tarea

Debe asignar una IP estática al dispositivo en cada red conectada o asignar una concesión permanente a la dirección del servidor DHCP.

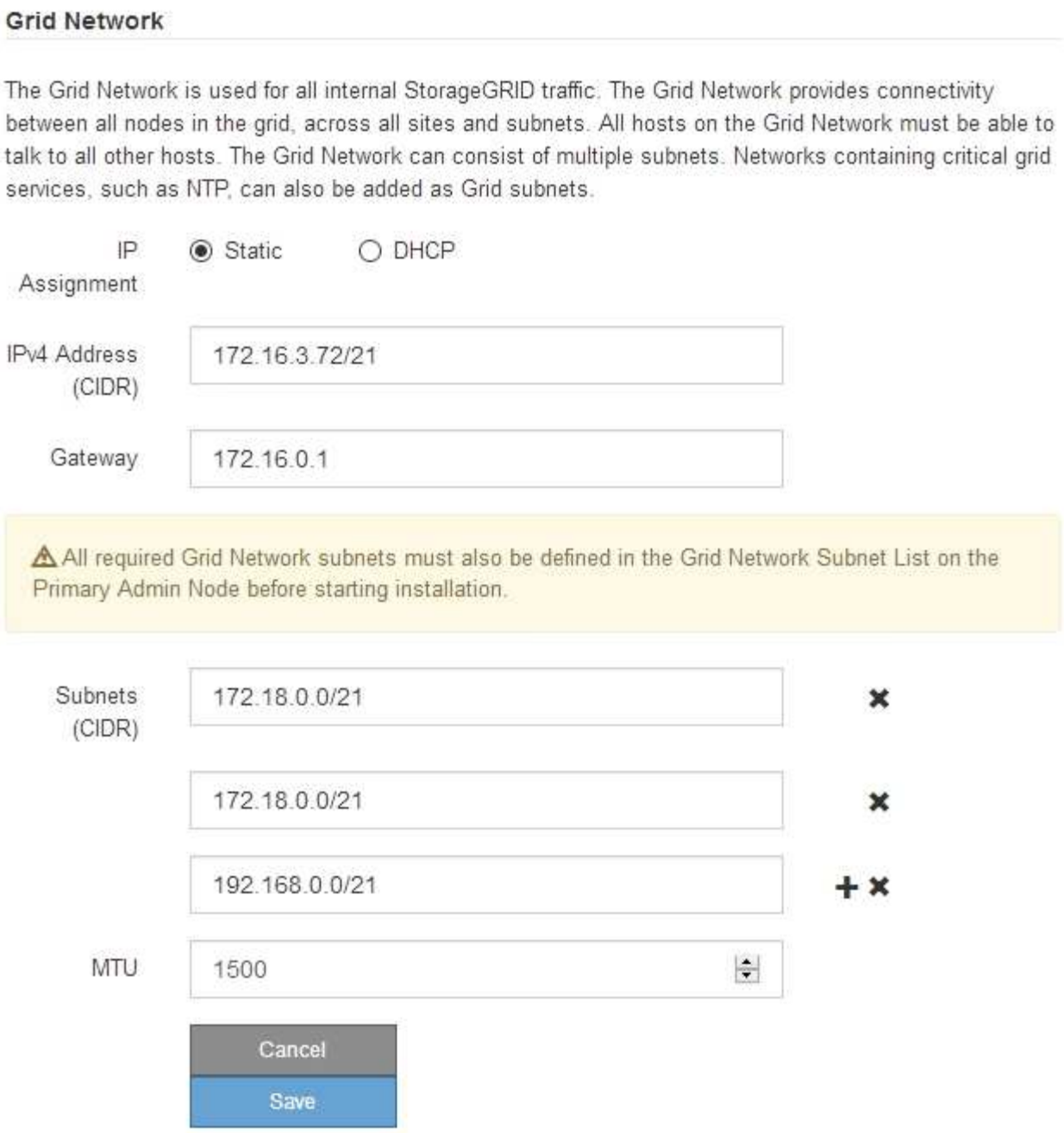
Si desea cambiar la configuración de enlaces, consulte las instrucciones para cambiar la configuración de enlaces de la controladora E5600SG.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Configurar redes** > **Configuración IP**.

   Aparece la página Configuración de IP.

2. Para configurar Grid Network, seleccione **Static** o **DHCP** en la sección **Grid Network** de la página.



3. Si ha seleccionado **estático**, siga estos pasos para configurar la red de cuadrícula:
   a. Introduzca la dirección IPv4 estática utilizando la notación CIDR.
   b. Introduzca la puerta de enlace.

      Si la red no tiene una puerta de enlace, vuelva a introducir la misma dirección IPv4 estática.

   c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

      > 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. Los valores de MTU no tienen que ser iguales para todos los tipos de red.

d. Haga clic en **Guardar**.

   Al cambiar la dirección IP, la pasarela y la lista de subredes también pueden cambiar.

   Si pierde la conexión con el instalador de dispositivos StorageGRID, vuelva a introducir la URL con la nueva dirección IP estática que acaba de asignar. Por ejemplo, `https://services_appliance_IP:8443`

e. Confirme que la lista de subredes de red es correcta.

   Si tiene 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. Estas subredes de red de cuadrícula también deben definirse en la Lista de subredes de red de cuadrícula del nodo de administración principal al iniciar la instalación de StorageGRID.

   > La ruta predeterminada no aparece en la lista. Si la red de cliente no está activada, la ruta predeterminada utilizará la puerta de enlace de red de cuadrícula.

   - Para agregar una subred, haga clic en el icono de inserción ➕ a la derecha de la última entrada.
   - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

f. Haga clic en **Guardar**.

4. Si ha seleccionado **DHCP**, siga estos pasos para configurar Grid Network:

a. Después de seleccionar el botón de opción **DHCP**, haga clic en **Guardar**.

   Los campos **Dirección IPv4**, **Puerta de enlace** y **subredes** se rellenan automáticamente. Si el servidor DHCP está configurado para asignar un valor MTU, el campo **MTU** se rellena con ese valor y el campo pasa a ser de sólo lectura.

   El navegador web se redirige automáticamente a la nueva dirección IP para el instalador de dispositivos StorageGRID.

b. Confirme que la lista de subredes de red es correcta.

   Si tiene 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. Estas subredes de red de cuadrícula también deben definirse en la Lista de subredes de red de cuadrícula del nodo de administración principal al iniciar la instalación de StorageGRID.

   > La ruta predeterminada no aparece en la lista. Si la red de cliente no está activada, la ruta predeterminada utilizará la puerta de enlace de red de cuadrícula.

   - Para agregar una subred, haga clic en el icono de inserción ➕ a la derecha de la última entrada.
   - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes,

como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

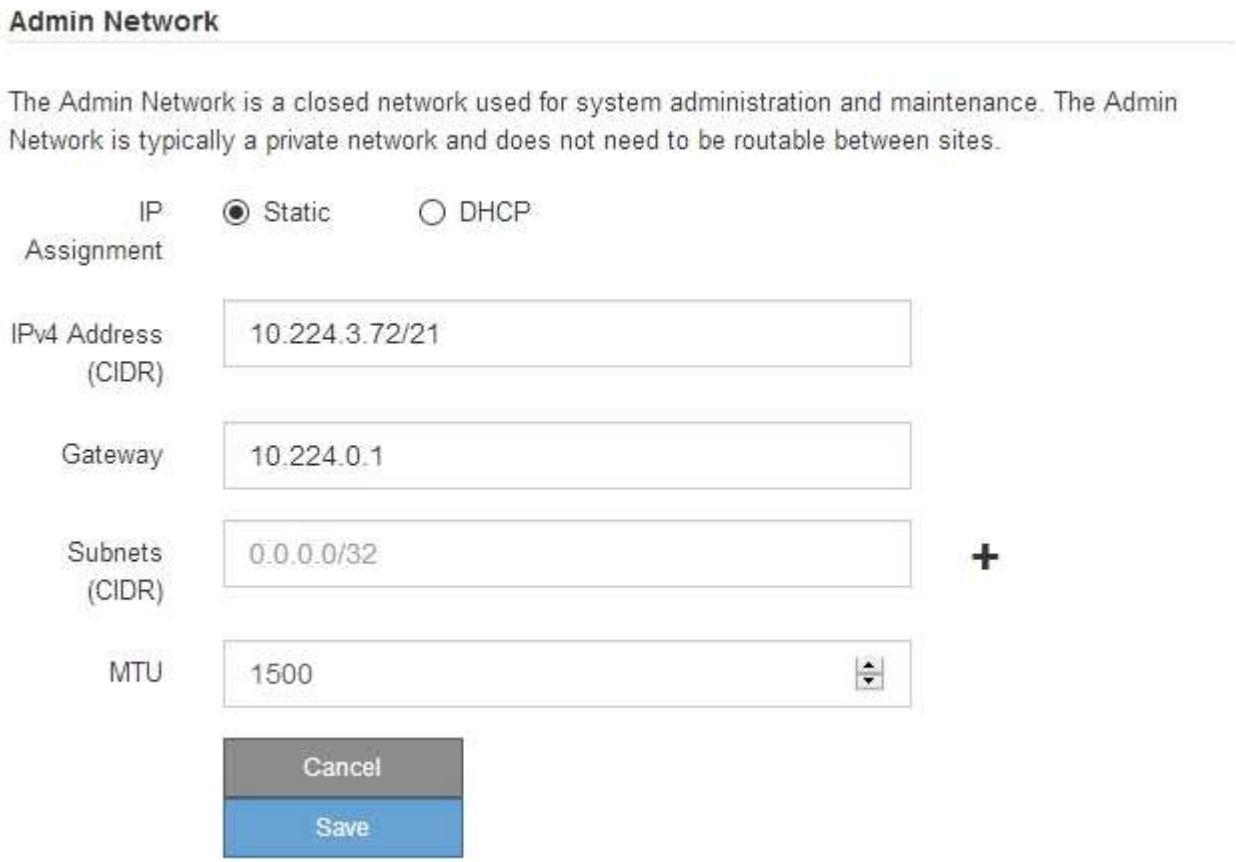
> El valor de MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, pueden ocurrir problemas de rendimiento de red o pérdida de paquetes.

> 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. Los valores de MTU no tienen que ser iguales para todos los tipos de red.

a. Haga clic en **Guardar**.

5. Para configurar la Red de administración, seleccione **estático** o **DHCP** en la sección Red de administración de la página.

> Para configurar la Red de administración, debe activar la Red de administración en la página Configuración de vínculos.



6. Si ha seleccionado **estático**, siga estos pasos para configurar la red de administración:

   a. Introduzca la dirección IPv4 estática, mediante la notación CIDR, para el puerto de gestión 1 del dispositivo.

      El puerto de gestión 1 está a la izquierda de los dos puertos RJ45 de 1-GbE del extremo derecho del dispositivo.

b. Introduzca la puerta de enlace.

   Si la red no tiene una puerta de enlace, vuelva a introducir la misma dirección IPv4 estática.

c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

   > 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.

d. Haga clic en **Guardar**.

   Al cambiar la dirección IP, la pasarela y la lista de subredes también pueden cambiar.

   Si pierde la conexión con el instalador de dispositivos StorageGRID, vuelva a introducir la URL con la nueva dirección IP estática que acaba de asignar. Por ejemplo, `https://services_appliance:8443`

e. Confirme que la lista de subredes de la red administrativa es correcta.

   Debe verificar que se pueda acceder a todas las subredes mediante la puerta de enlace que ha proporcionado.

   > No se puede realizar la ruta predeterminada para utilizar la puerta de enlace de red de administración.

   - Para agregar una subred, haga clic en el icono de inserción ➕ a la derecha de la última entrada.
   - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

f. Haga clic en **Guardar**.

7. Si ha seleccionado **DHCP**, siga estos pasos para configurar la red de administración:

   a. Después de seleccionar el botón de opción **DHCP**, haga clic en **Guardar**.

      Los campos **Dirección IPv4**, **Puerta de enlace** y **subredes** se rellenan automáticamente. Si el servidor DHCP está configurado para asignar un valor MTU, el campo **MTU** se rellena con ese valor y el campo pasa a ser de sólo lectura.

      El navegador web se redirige automáticamente a la nueva dirección IP para el instalador de dispositivos StorageGRID.

   b. Confirme que la lista de subredes de la red administrativa es correcta.

      Debe verificar que se pueda acceder a todas las subredes mediante la puerta de enlace que ha proporcionado.

      > No se puede realizar la ruta predeterminada para utilizar la puerta de enlace de red de administración.

      - Para agregar una subred, haga clic en el icono de inserción ➕ a la derecha de la última entrada.
      - Para eliminar una subred no utilizada, haga clic en el icono de eliminación ✖.

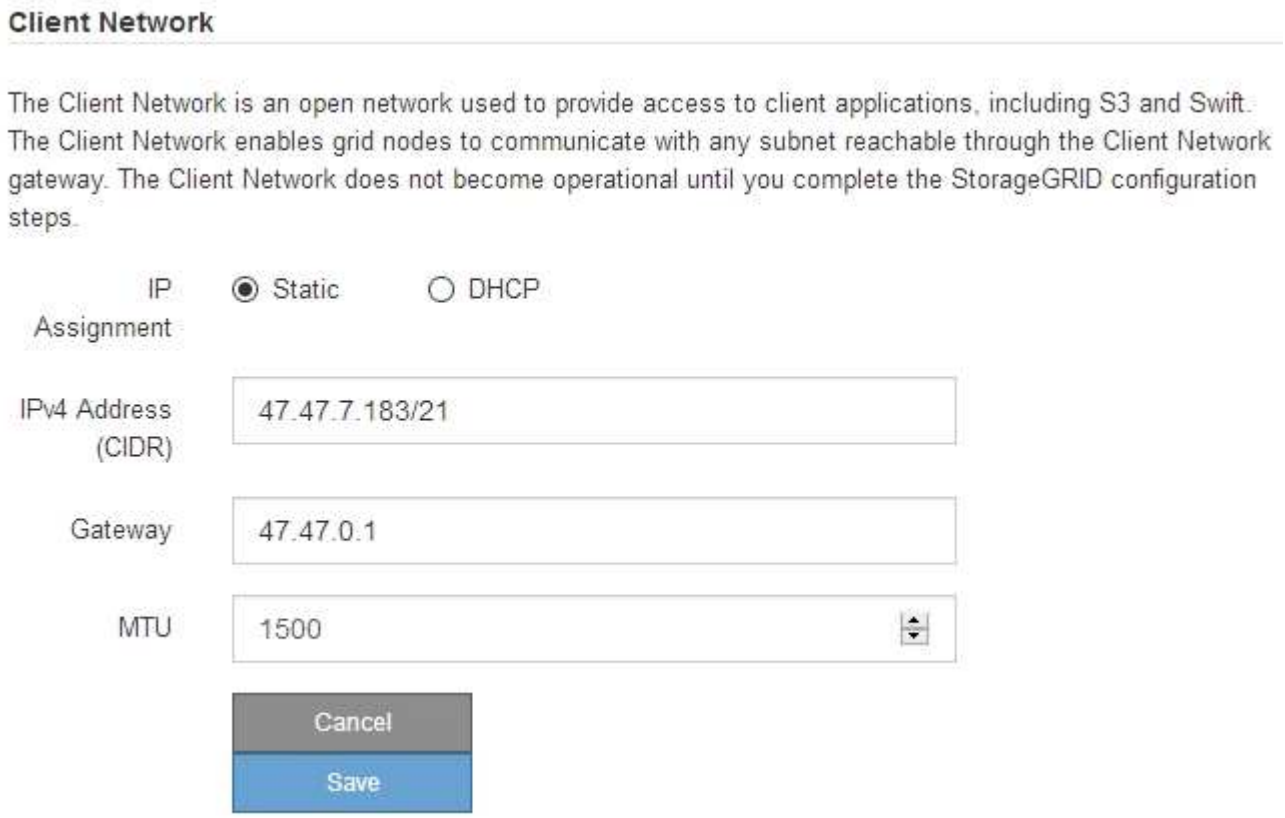
c. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

> 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.

d. Haga clic en **Guardar**.

8. Para configurar la red de cliente, seleccione **Static** o **DHCP** en la sección **Client Network** de la página.

> Para configurar la red de cliente, debe activar la red de cliente en la página Configuración de vínculos.



9. Si ha seleccionado **estático**, siga estos pasos para configurar la red de cliente:

a. Introduzca la dirección IPv4 estática utilizando la notación CIDR.

b. Haga clic en **Guardar**.

c. Confirme que la dirección IP de la puerta de enlace de red de cliente es correcta.

> Si la red de cliente está activada, se muestra la ruta predeterminada. La ruta predeterminada utiliza la puerta de enlace de red de cliente y no se puede mover a otra interfaz mientras la red de cliente está activada.

d. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

> 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.

e. Haga clic en **Guardar**.

10. Si ha seleccionado **DHCP**, siga estos pasos para configurar la red de cliente:

    a. Después de seleccionar el botón de opción **DHCP**, haga clic en **Guardar**.

    Los campos **Dirección IPv4** y **Puerta de enlace** se rellenan automáticamente. Si el servidor DHCP está configurado para asignar un valor MTU, el campo **MTU** se rellena con ese valor y el campo pasa a ser de sólo lectura.

El navegador web se redirige automáticamente a la nueva dirección IP para el instalador de dispositivos StorageGRID.

a. Confirme que la puerta de enlace es correcta.

> Si la red de cliente está activada, se muestra la ruta predeterminada. La ruta predeterminada utiliza la puerta de enlace de red de cliente y no se puede mover a otra interfaz mientras la red de cliente está activada.

b. Si desea utilizar tramas gigantes, cambie el campo MTU a un valor adecuado para tramas gigantes, como 9000. De lo contrario, mantenga el valor predeterminado de 1500.

> 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.

Información relacionada

Cambie la configuración del enlace de la controladora E5600SG

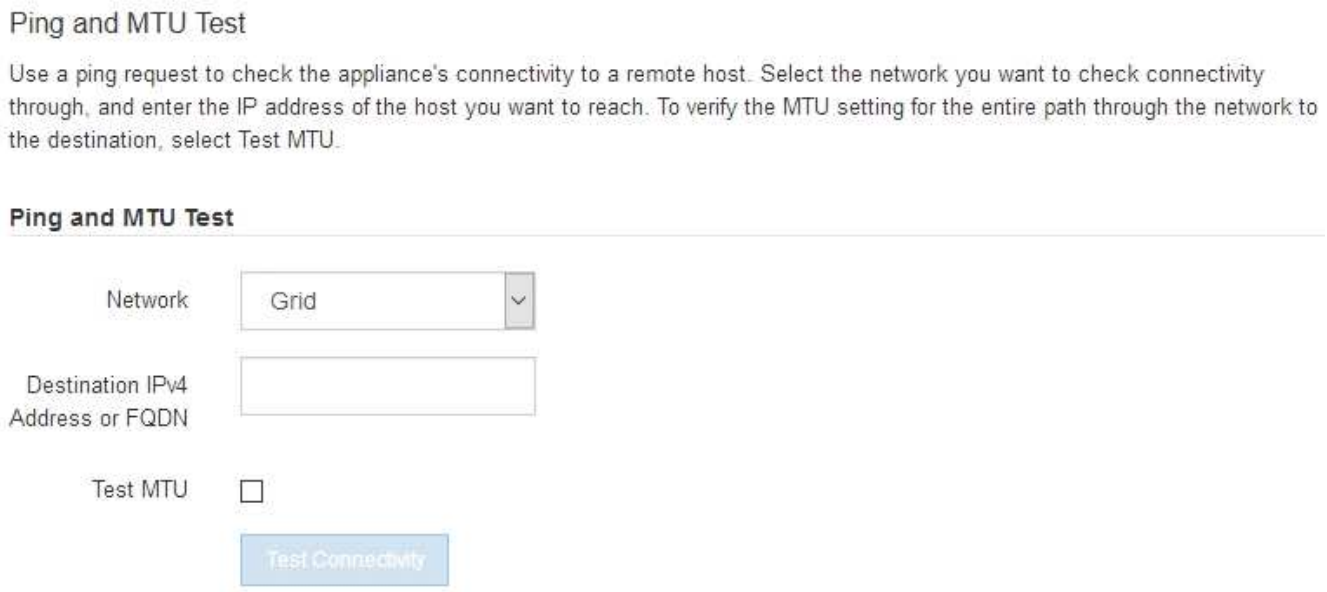
Compruebe las conexiones de red

Debe confirmar que puede acceder a las redes StorageGRID que está utilizando desde el dispositivo. Para validar el enrutamiento mediante puertas de enlace de red, debe probar la conectividad entre el instalador de dispositivos de StorageGRID y las direcciones IP en subredes diferentes. También puede verificar la configuración de MTU.

Pasos

1. En la barra de menús del instalador del dispositivo StorageGRID, haga clic en **Configurar redes** > **Ping y prueba de MTU**.

   Aparece la página pruebas de ping y MTU.



2. En el cuadro desplegable **Red**, seleccione la red que desea probar: Grid, Admin o Client.
3. Introduzca la dirección IPv4 o el nombre de dominio completo (FQDN) correspondiente a un host en esa red.

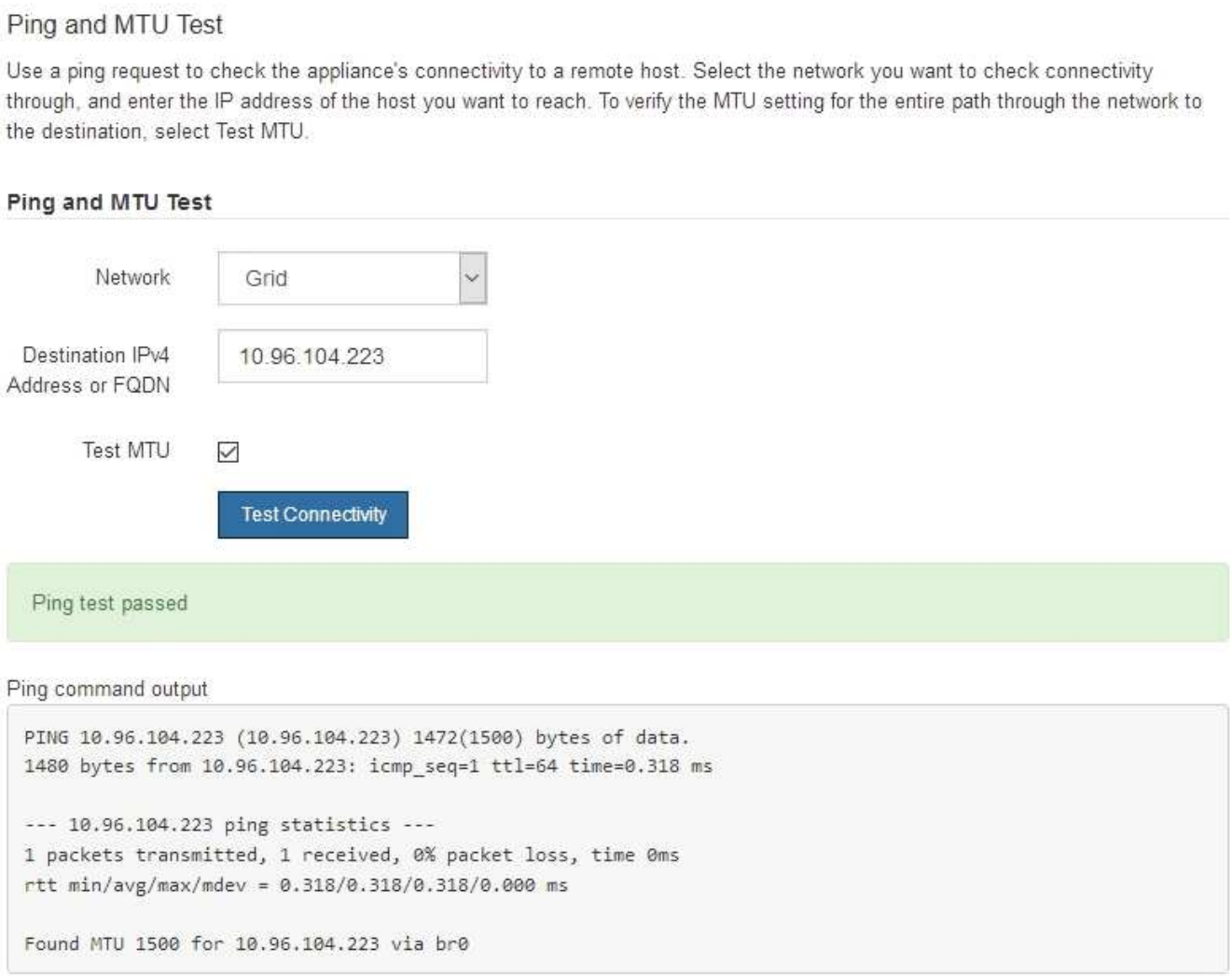
   Por ejemplo, puede hacer ping a la puerta de enlace de la red o al nodo de administración principal.

4. Opcionalmente, active la casilla de verificación **probar MTU** para comprobar la configuración de MTU para toda la ruta de acceso a través de la red hasta el destino.

   Por ejemplo, puede probar la ruta entre el nodo del dispositivo y un nodo en un sitio diferente.

5. Haga clic en **probar conectividad**.

   Si la conexión de red es válida, aparece el mensaje "Ping test pased", con la salida del comando ping en la lista.



Información relacionada

Configurar enlaces de red (SG5600)

Cambie la configuración de MTU

Verifique las conexiones de red a nivel de puerto

Para garantizar que los firewalls no obstruyan el acceso entre el instalador del dispositivo StorageGRID y otros nodos, confirme que el instalador del dispositivo StorageGRID puede conectarse a un puerto TCP o a un conjunto de puertos en la dirección IP o el rango de direcciones especificados.

Acerca de esta tarea

Con la lista de puertos que se incluye en el instalador de dispositivos de StorageGRID, puede probar la conectividad entre el dispositivo y los demás nodos de la red de grid.

Además, puede probar la conectividad en las redes de administración y cliente y en los puertos UDP, como los que se utilizan para servidores NFS o DNS externos. Para obtener una lista de estos puertos, consulte la referencia de puertos en las directrices de red de StorageGRID.

Los puertos de red de red enumerados en la tabla de conectividad de puertos sólo son válidos para StorageGRID versión 11.6.0. Para verificar qué puertos son correctos para cada tipo de nodo, siempre debe consultar las directrices de red para su versión de StorageGRID.

Pasos

1. En el instalador del dispositivo StorageGRID, haga clic en **Configurar red** > **Prueba de conectividad de puerto (nmap)**.

   Aparece la página Prueba de conectividad de puerto.

   La tabla de conectividad de puertos enumera los tipos de nodos que requieren conectividad TCP en la red de cuadrícula. Para cada tipo de nodo, la tabla enumera los puertos de red de cuadrícula a los que el dispositivo debe acceder.

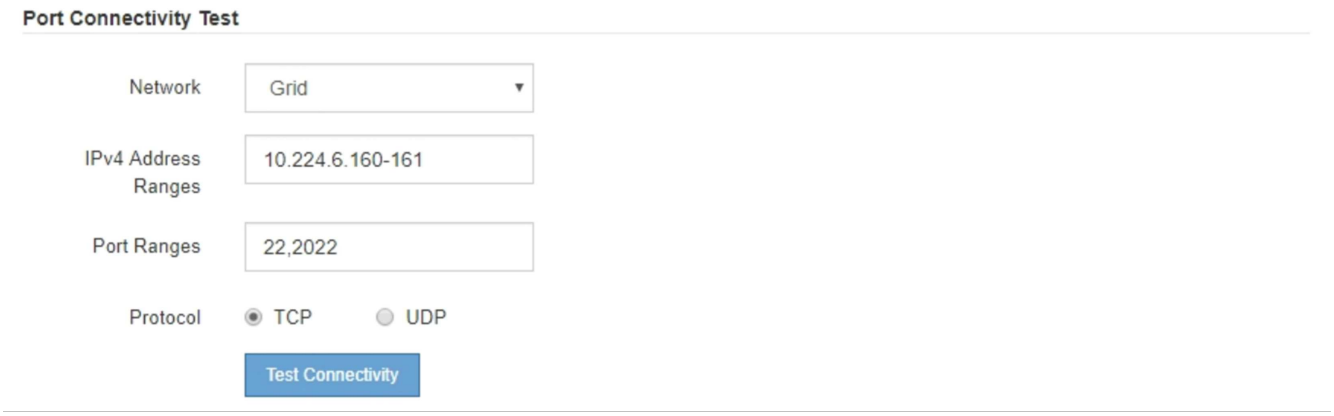
   Puede probar la conectividad entre los puertos del dispositivo que aparecen en la tabla y los demás nodos de la red de grid.

2. En el menú desplegable **Red**, seleccione la red que desea probar: **Grid**, **Admin** o **Cliente**.
3. Especifique un rango de direcciones IPv4 para los hosts en esa red.

   Por ejemplo, es posible que desee sondear la puerta de enlace en la red o en el nodo de administración principal.

   Especifique un rango utilizando un guión, como se muestra en el ejemplo.

4. Introduzca un número de puerto TCP, una lista de puertos separados por comas o un intervalo de puertos.



5. Haga clic en **probar conectividad**.

   - Si las conexiones de red a nivel de puerto seleccionadas son válidas, el mensaje "'Prueba de conectividad de puerto superada'" aparece en un banner verde. El resultado del comando nmap se muestra debajo del banner.

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
2022/tcp open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- Si se realiza una conexión de red a nivel de puerto al host remoto, pero el host no escucha en uno o más de los puertos seleccionados, el mensaje "'error de prueba de conectividad de puerto'" aparece en un banner amarillo. El resultado del comando nmap se muestra debajo del banner.

  Cualquier puerto remoto al que no esté escuchando el host tiene un estado de "'cerrado'". Por ejemplo, puede ver este banner amarillo cuando el nodo al que intenta conectarse está en estado preinstalado y el servicio NMS de StorageGRID aún no se está ejecutando en ese nodo.

Port connectivity test failed
Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
1504/tcp closed evb-elm
1505/tcp open   funkproxy
1506/tcp open   utcd
1508/tcp open   diagmond
7443/tcp open   oracleas-https
9999/tcp open   abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- Si no se puede establecer una conexión de red a nivel de puerto para uno o más puertos seleccionados, el mensaje "'Port Connectivity test failed'" aparece en un banner rojo. El resultado del comando nmap se muestra debajo del banner.

  El banner rojo indica que se ha realizado un intento de conexión TCP a un puerto en el host remoto, pero no se ha devuelto nada al remitente. Cuando no se devuelve ninguna respuesta, el puerto tiene un estado de "filtrado" y es probable que sea bloqueado por un firewall.

  ⓘ También se enumeran los puertos con «'cerrado'».

Port connectivity test failed
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT     STATE    SERVICE
22/tcp   open     ssh
79/tcp   filtered finger
80/tcp   open     http
443/tcp  open     https
1504/tcp closed   evb-elm
1505/tcp open     funkproxy
1506/tcp open     utcd
1508/tcp open     diagmond
7443/tcp open     oracleas-https
9999/tcp open     abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

Información relacionada

Directrices sobre redes

Configure el Administrador de almacenamiento de SANtricity

Puede usar Storage Manager de SANtricity para supervisar el estado de los discos de almacenamiento y los componentes de hardware del dispositivo StorageGRID. Para acceder a este software, debe conocer la dirección IP del puerto de gestión 1 de la controladora E2700 (la controladora de almacenamiento del dispositivo).

Configure la dirección IP para la controladora E2700

El puerto de gestión 1 de la controladora E2700 conecta el dispositivo a la red de gestión para SANtricity Storage Manager. Debe configurar una dirección IP estática para la controladora E2700 a fin de garantizar que no se pierda la conexión de gestión con el hardware y el firmware de la controladora en el dispositivo StorageGRID.

Lo que necesitará

Está utilizando un navegador web compatible.

Acerca de esta tarea

Las direcciones asignadas por DHCP pueden cambiar en cualquier momento. Asigne una dirección IP estática a la controladora para garantizar una accesibilidad consistente.

Pasos

1. Desde el cliente, introduzca la URL del instalador de dispositivos de StorageGRID:
   `https://E5600SG_Controller_IP:8443`

   Para *`E5600SG_Controller_IP`*, Utilice la dirección IP del dispositivo en cualquier red StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Configuración de hardware** > **Configuración de red del controlador de almacenamiento**.

Aparece la página Storage Controller Network Configuration.

3. En función de la configuración de la red, seleccione **habilitado** para IPv4, IPv6 o ambos.
4. Anote la dirección IPv4 que se muestra automáticamente.

   DHCP es el método predeterminado para asignar una dirección IP a este puerto.

   > Puede que los valores de DHCP deban tardar varios minutos en aparecer.

5. De manera opcional, configure una dirección IP estática para el puerto de gestión de la controladora E2700.

   > Debe asignar una IP estática al puerto de gestión o una concesión permanente para la dirección en el servidor DHCP.

   a. Seleccione **estático**.
   b. Introduzca la dirección IPv4 mediante la notación CIDR.
   c. Introduzca la pasarela predeterminada.

   d. Haga clic en **Guardar**.

      Puede que los cambios se apliquen en unos minutos.

   Cuando se conecta a SANtricity Storage Manager, se utiliza la nueva dirección IP estática como la URL: `https://E2700_Controller_IP`

Información relacionada

"Documentación de NetApp: SANtricity Storage Manager"

Añada el dispositivo a SANtricity Storage Manager

La controladora E2700 se conecta al dispositivo con SANtricity Storage Manager y, a continuación, añade el dispositivo como una cabina de almacenamiento.

Lo que necesitará

Está utilizando un navegador web compatible.

Acerca de esta tarea

Para obtener instrucciones detalladas, consulte la documentación de SANtricity Storage Manager.

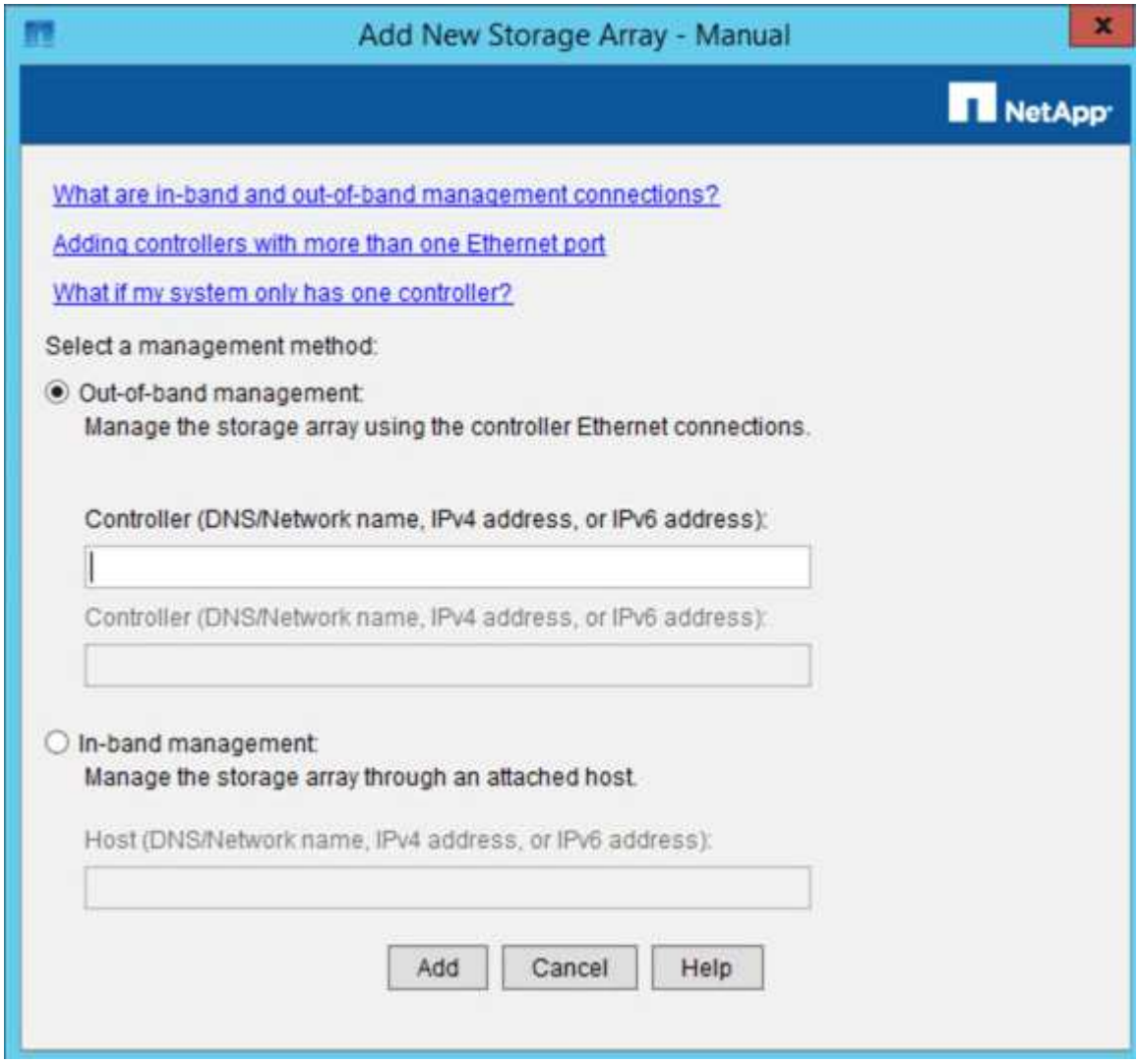
Pasos

1. Abra un explorador web y escriba la dirección IP como URL de SANtricity Storage Manager:
   `https://E2700_Controller_IP`

   Aparece la página de inicio de sesión en SANtricity Storage Manager.

2. En la página **Seleccionar método de adición**, seleccione **Manual** y haga clic en **Aceptar**.
3. Seleccione **Editar** > **Agregar matriz de almacenamiento**.

   Se mostrará la página Add New Storage Array - Manual.



4. En el cuadro **Administración fuera de banda**, introduzca uno de los siguientes valores:
   - **Usando DHCP:** la dirección IP asignada por el servidor DHCP al puerto de administración 1 del controlador E2700

- **Sin usar DHCP:** `192.168.128.101`

> Solo una de las controladoras del dispositivo está conectada a SANtricity Storage Manager, por lo que solo debe introducir una dirección IP.

5. Haga clic en **Agregar**.

Información relacionada

"Documentación de NetApp: SANtricity Storage Manager"

Configure el Administrador del almacenamiento de SANtricity

Después de acceder a Storage Manager de SANtricity, puede utilizarlo para configurar los ajustes de hardware. Normalmente, esta configuración se debe configurar antes de poner en marcha el dispositivo como nodo de almacenamiento en un sistema StorageGRID.

Configure AutoSupport

La herramienta AutoSupport recoge datos en un bundle de soporte al cliente desde el dispositivo y envía automáticamente los datos al soporte técnico. La configuración de AutoSupport ayuda al soporte técnico con la solución de problemas y el análisis de problemas de forma remota.

Lo que necesitará

- La función AutoSupport debe estar activada y activada en el dispositivo.

  La función AutoSupport se activa y desactiva globalmente en una estación de administración del almacenamiento.

- El Monitor de eventos de Storage Manager debe ejecutarse en al menos una máquina con acceso al dispositivo y, preferiblemente, en un equipo como máximo.

Acerca de esta tarea

Todos los datos se comprimen en un formato de archivo comprimido simple (.7z) en la ubicación especificada.

AutoSupport ofrece los siguientes tipos de mensajes:

Tipos de mensaje	Descripción
Mensajes de eventos	• Se envían cuando ocurre un evento de soporte en el dispositivo gestionado • Incluir información de diagnóstico y configuración del sistema

Tipos de mensaje	Descripción
Mensajes diarios	• Se envía una vez al día durante un intervalo de tiempo configurable por el usuario en la hora local del dispositivo • Incluyen los registros de eventos del sistema y los datos de rendimiento actuales
Mensajes semanales	• Se envía una vez cada semana durante un intervalo de tiempo que el usuario puede configurar en la hora local del aparato • Incluir información de estado del sistema y la configuración

Pasos

1. En la ventana de administración de empresa del Administrador de almacenamiento de SANtricity, seleccione la ficha **dispositivos** y, a continuación, seleccione **matrices de almacenamiento detectadas**.
2. Seleccione **Herramientas** > **AutoSupport** > **Configuración**.
3. Si es necesario, utilice la ayuda en línea de SANtricity Storage Manager para completar la tarea.

Información relacionada

"Documentación de NetApp: SANtricity Storage Manager"

Verifique la recepción de AutoSupport

Debe verificar que el soporte técnico recibe sus mensajes de AutoSupport. Puede encontrar el estado de AutoSupport para sus sistemas en el portal de Active IQ. Al verificar la recepción de estos mensajes se garantiza que el soporte técnico disponga de la información necesaria si necesita ayuda.

Acerca de esta tarea

AutoSupport puede mostrar uno de los siguientes Estados:

- **ON**

  Un estado DE ENCENDIDO indica que el soporte técnico está recibiendo mensajes de AutoSupport actualmente del sistema.

- **OFF**

  El estado DE APAGADO sugiere que puede haber deshabilitado AutoSupport porque el soporte técnico no ha recibido un registro semanal del sistema en los últimos 15 días naturales o puede haber un cambio en el entorno o la configuración (por ejemplo).

- **DECLINACIÓN**

  Un estado DE RECHAZO significa que ha notificado al soporte técnico que no habilitará AutoSupport.

Una vez que el soporte técnico recibe un registro semanal del sistema, el estado de AutoSupport cambia a ON.

Pasos

1. Vaya al sitio de soporte de NetApp en "mysupport.netapp.com", E inicie sesión en el portal de Active IQ.
2. Si el estado de AutoSupport es DESACTIVADO y cree que es incorrecto, complete lo siguiente:
   a. Revise la configuración del sistema para asegurarse de que ha activado AutoSupport.
   b. Compruebe el entorno de red y la configuración para garantizar que el sistema pueda enviar mensajes al soporte técnico.

Configure las notificaciones de alertas de capturas SNMP y por correo electrónico

Storage Manager de SANtricity puede notificarle en qué momento cambia el estado del dispositivo o uno de sus componentes. Esto se denomina notificación de alerta. Es posible recibir notificaciones de alerta de dos métodos diferentes: Capturas de correo electrónico y SNMP. Debe configurar las notificaciones de alerta que desee recibir.

Pasos

1. En la ventana Administración de empresas del Administrador de almacenamiento de SANtricity, seleccione la ficha **dispositivos** y, a continuación, seleccione un nodo.
2. Seleccione **Edición** > **Configurar alertas**.
3. Seleccione la ficha **correo electrónico** para configurar las notificaciones de alertas por correo electrónico.
4. Seleccione la ficha **SNMP** para configurar las notificaciones de alerta de capturas SNMP.
5. Si es necesario, utilice la ayuda en línea de SANtricity Storage Manager para completar la tarea.

Configure contraseñas para SANtricity Storage Manager

Puede configurar las contraseñas que se utilizan para el dispositivo en SANtricity Storage Manager. La configuración de contraseñas mantiene la seguridad del sistema.

Pasos

1. En Enterprise Management Window, en el Administrador de almacenamiento de SANtricity, haga doble clic en el controlador.
2. En la ventana Administración de matrices, seleccione el menú **matriz de almacenamiento** y seleccione **Seguridad** > **Configurar contraseña**.
3. Configurar las contraseñas.
4. Si es necesario, utilice la ayuda en línea de SANtricity Storage Manager para completar la tarea.

Opcional: Habilite el cifrado de nodos

Si habilita el cifrado de nodos, los discos del dispositivo pueden protegerse mediante el cifrado del servidor de gestión de claves seguro (KMS) contra la pérdida física o la eliminación del sitio. Debe seleccionar y habilitar el cifrado de nodos durante la instalación del dispositivo y no puede anular la selección del cifrado de nodos una vez que se inicia el proceso de cifrado KMS.

Lo que necesitará

Revise la información sobre KMS en las instrucciones para administrar StorageGRID.

Acerca de esta tarea

Un dispositivo con el cifrado de nodos habilitado se conecta al servidor de gestión de claves (KMS) externo que está configurado para el sitio StorageGRID. Cada KMS (o clúster KMS) administra las claves de cifrado de todos los nodos de dispositivos del sitio. Estas claves cifran y descifran los datos de cada disco de un dispositivo que tiene habilitado el cifrado de nodos.

Se puede configurar un KMS en Grid Manager antes o después de instalar el dispositivo en StorageGRID. Consulte la información sobre la configuración de KMS y del dispositivo en las instrucciones para administrar StorageGRID para obtener más detalles.

- Si se configura un KMS antes de instalar el dispositivo, el cifrado controlado por KMS comienza cuando se habilita el cifrado de nodos en el dispositivo y se lo agrega a un sitio StorageGRID donde se configura KMS.
- Si no se configura un KMS antes de instalar el dispositivo, el cifrado controlado por KMS se lleva a cabo en cada dispositivo que tenga activado el cifrado de nodos en cuanto se configure un KMS y esté disponible para el sitio que contiene el nodo del dispositivo.

> Los datos que existen antes de conectarse al KMS en un dispositivo con el cifrado de nodos habilitado se cifran con una clave temporal que no es segura. El dispositivo no está protegido de la retirada o robo hasta que la clave se configure en un valor proporcionado por el KMS.

Sin la clave KMS necesaria para descifrar el disco, los datos del dispositivo no se pueden recuperar y se pierden de forma efectiva. Este es el caso siempre que la clave de descifrado no se pueda recuperar del KMS. La clave se vuelve inaccesible si elimina la configuración de KMS, caduca una clave KMS, se pierde la conexión con el KMS o se elimina el dispositivo del sistema StorageGRID donde están instaladas sus claves KMS.

Pasos

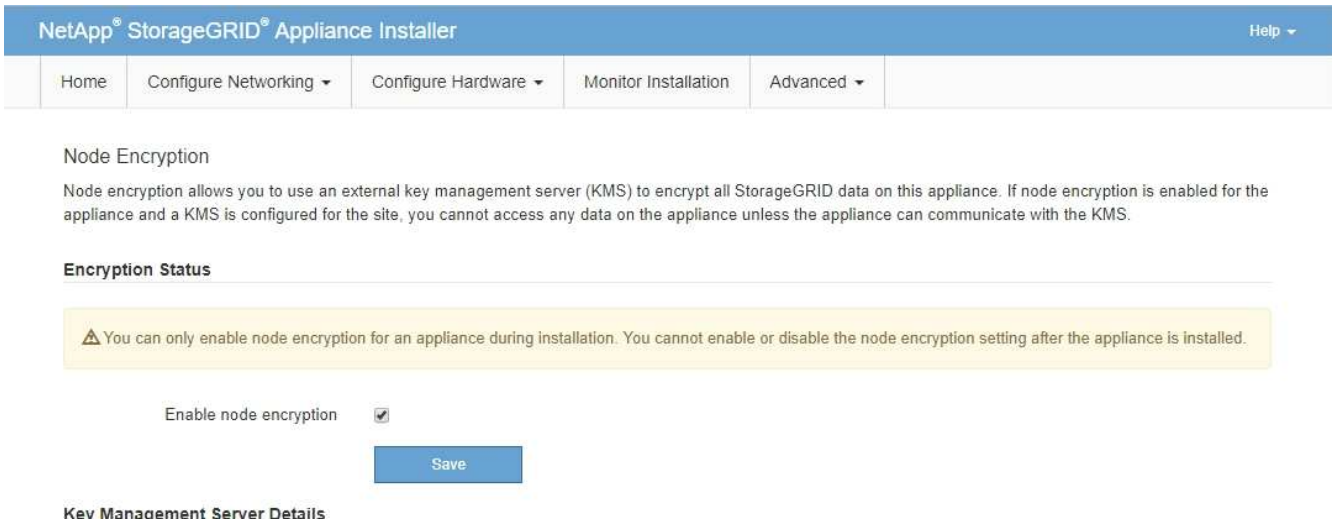
1. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.
   https://*Controller_IP*:8443

   Controller_IP Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

   > Una vez que el dispositivo se ha cifrado con una clave KMS, los discos del dispositivo no se pueden descifrar sin utilizar la misma clave KMS.

2. Seleccione **Configurar hardware** > **cifrado de nodos**.



3. Seleccione **Activar cifrado de nodo**.

   Antes de instalar el dispositivo, puede anular la selección **Activar cifrado de nodo** sin riesgo de pérdida de datos. Cuando se inicia la instalación el nodo del dispositivo, accede a las claves de cifrado de KMS en el sistema StorageGRID y comienza el cifrado de disco. No se puede deshabilitar el cifrado de nodos después de haber instalado el dispositivo.

   > Después de agregar un dispositivo que tiene habilitado el cifrado de nodos a un sitio StorageGRID que tiene un KMS, no puede detener el uso del cifrado KMS para el nodo.

4. Seleccione **Guardar**.
5. Ponga en marcha el dispositivo como nodo en su sistema StorageGRID.

   El cifrado controlado POR KMS se inicia cuando el dispositivo accede a las claves KMS configuradas para el sitio StorageGRID. El instalador muestra mensajes de progreso durante el proceso de cifrado KMS, que puede tardar unos minutos en función del número de volúmenes de disco del dispositivo.

   > Los dispositivos se configuran inicialmente con una clave de cifrado no KMS aleatoria asignada a cada volumen de disco. Los discos se cifran con esta clave de cifrado temporal, que no es segura, hasta que el dispositivo con cifrado de nodos habilitado acceda a las claves KMS configuradas para el sitio StorageGRID.

Después de terminar

Puede ver el estado de cifrado de nodo, los detalles de KMS y los certificados en uso cuando el nodo del dispositivo está en modo de mantenimiento.

Información relacionada

Administre StorageGRID

Supervisar el cifrado de nodos en modo de mantenimiento (SG5600)

Opcional: Cambiar al modo RAID6 (sólo SG5660)

Si tiene un SG5660 con 60 unidades, puede cambiar la configuración de volumen de su configuración predeterminada y recomendada, Dynamic Disk Pools (DDP) a RAID6. Solo puede cambiar el modo antes de implementar el nodo de almacenamiento del dispositivo

StorageGRID.

Lo que necesitará

- Tiene un SG5660. SG5612 no admite RAID6. Si tiene SG5612, debe usar el modo de DDP.

> Si alguno de los volúmenes ya está configurado o si StorageGRID se instaló anteriormente, al cambiar el modo RAID se quitan y se reemplazan los volúmenes. Se perderán todos los datos de estos volúmenes.

Acerca de esta tarea

Antes de implementar un nodo de almacenamiento del dispositivo StorageGRID, puede elegir entre dos opciones de configuración de volumen:

- **Dynamic Disk Pools (DDP)** — esta es la configuración predeterminada y recomendada. DDP es un esquema de protección de datos de hardware mejorado que ofrece un mejor rendimiento del sistema, menores tiempos de recompilación después de fallos de unidad y facilidad de gestión.
- **RAID6** — se trata de un esquema de protección de hardware que utiliza franjas de paridad en cada disco y permite que se produzcan dos fallos de disco dentro del conjunto RAID antes de que se pierdan datos.

> No se recomienda el uso de RAID6 en la mayoría de entornos StorageGRID. A pesar de que RAID6 puede aumentar la eficiencia del almacenamiento hasta el 88 % (frente al 80 % de los DDP), el modo DDP ofrece una recuperación más eficiente de fallos de unidad.

Pasos

1. Con el portátil de servicio, abra un explorador web y acceda al instalador de dispositivos de StorageGRID: **`https://E5600SG_Controller_IP:8443`**

   Donde *`E5600SG_Controller_IP`* Es cualquiera de las direcciones IP de la controladora E5600SG.

2. En la barra de menús, seleccione **Avanzado** > **modo RAID**.
3. En la página **Configurar el modo RAID**, seleccione **RAID6** en la lista desplegable modo.
4. Haga clic en **Guardar**.

Opcional: Reasignar puertos de red para el dispositivo

Es posible que deba reasignar los puertos internos del nodo de almacenamiento del dispositivo a diferentes puertos externos. Por ejemplo, es posible que tenga que reasignar puertos debido a un problema de firewall.

Lo que necesitará

- Ya ha accedido anteriormente al instalador de dispositivos de StorageGRID.
- No ha configurado y no planea configurar los extremos del equilibrador de carga.

> Si se reasigna algún puerto, no se pueden utilizar los mismos puertos para configurar los puntos finales del equilibrador de carga. Si desea configurar puntos finales del equilibrador de carga y ya tiene puertos reasignados, siga los pasos de Eliminar reasignaciones de puertos.

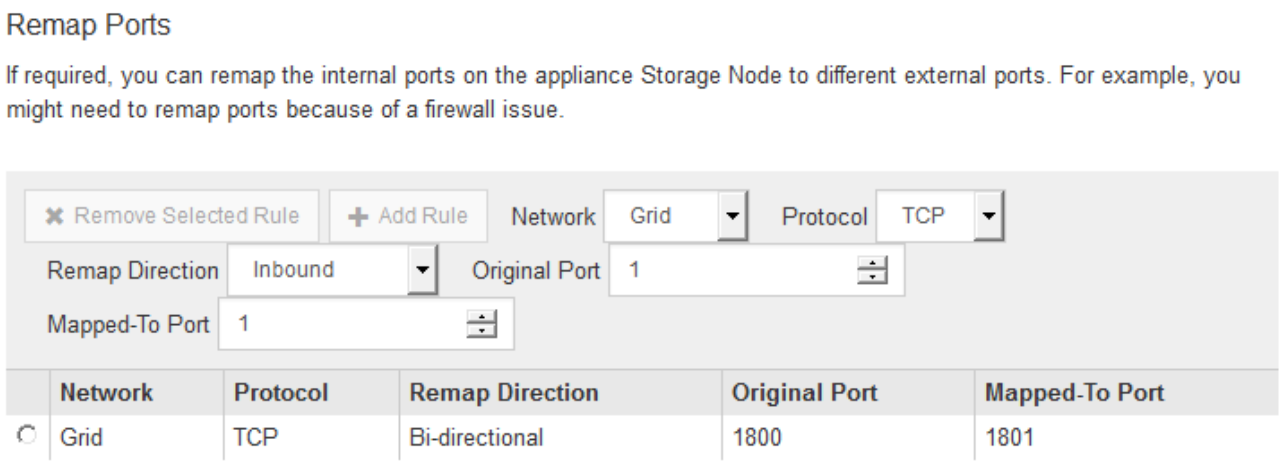
Pasos

1. En la barra de menús del instalador del dispositivo StorageGRID, haga clic en **Configurar redes** > **puertos de reasignación**.

   Aparecerá la página Remap Port.

2. En el cuadro desplegable **Red**, seleccione la red para el puerto que desea reasignar: Grid, Admin o Client.
3. En el cuadro desplegable **Protocolo**, seleccione el protocolo IP: TCP o UDP.
4. En el cuadro desplegable **Dirección de salida**, seleccione la dirección de tráfico que desea reasignar para este puerto: Entrante, saliente o bidireccional.
5. Para **Puerto original**, introduzca el número del puerto que desea reasignar.
6. En **Puerto asignado a**, introduzca el número del puerto que desea utilizar en su lugar.
7. Haga clic en **Agregar regla**.

   La nueva asignación de puertos se agrega a la tabla y la reasignación tiene efecto inmediatamente.



8. Para eliminar una asignación de puertos, seleccione el botón de opción de la regla que desea quitar y haga clic en **Eliminar regla seleccionada**.

Información relacionada

Recuperación y mantenimiento

Ponga en marcha el nodo de almacenamiento del dispositivo

Después de instalar y configurar el dispositivo de almacenamiento, puede ponerlo en marcha como un nodo de almacenamiento en un sistema StorageGRID. Al poner en marcha un dispositivo como nodo de almacenamiento, utiliza el instalador de dispositivos de StorageGRID que se incluye en el dispositivo.

Lo que necesitará

- Si va a clonar un nodo de dispositivo, continúe durante el proceso de recuperación y mantenimiento.

  Recuperación y mantenimiento

- El dispositivo se ha instalado en un rack o armario, conectado a las redes y encendido.

- Se han configurado los enlaces de red, las direcciones IP y la reasignación de puertos (si fuera necesario) para el dispositivo con el instalador de dispositivos de StorageGRID.
- Conoce una de las direcciones IP asignadas a la controladora de computación del dispositivo. Puede usar la dirección IP para cualquier red StorageGRID conectada.
- Se puso en marcha el nodo de administración principal del sistema 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.
- Tiene un portátil de servicio con un navegador web compatible.

Acerca de esta tarea

Cada dispositivo de almacenamiento funciona como un único nodo de almacenamiento. Cualquier dispositivo puede conectarse a la red de grid, a la red de administración y a la red de cliente

Para implementar un nodo de almacenamiento de dispositivos en un sistema StorageGRID, debe acceder al instalador de dispositivos StorageGRID y realizar los siguientes pasos:

- Debe especificar o confirmar la dirección IP del nodo de administrador principal y el nombre del nodo de almacenamiento.
- Se inicia la puesta en marcha y se espera a medida que se hayan configurado los volúmenes y se haya instalado el software.
- Cuando la instalación se detiene paso a paso a través de las tareas de instalación del dispositivo, se reanuda la instalación iniciando sesión en el Administrador de grid, aprobando todos los nodos de cuadrícula y completando los procesos de instalación e implementación de StorageGRID.

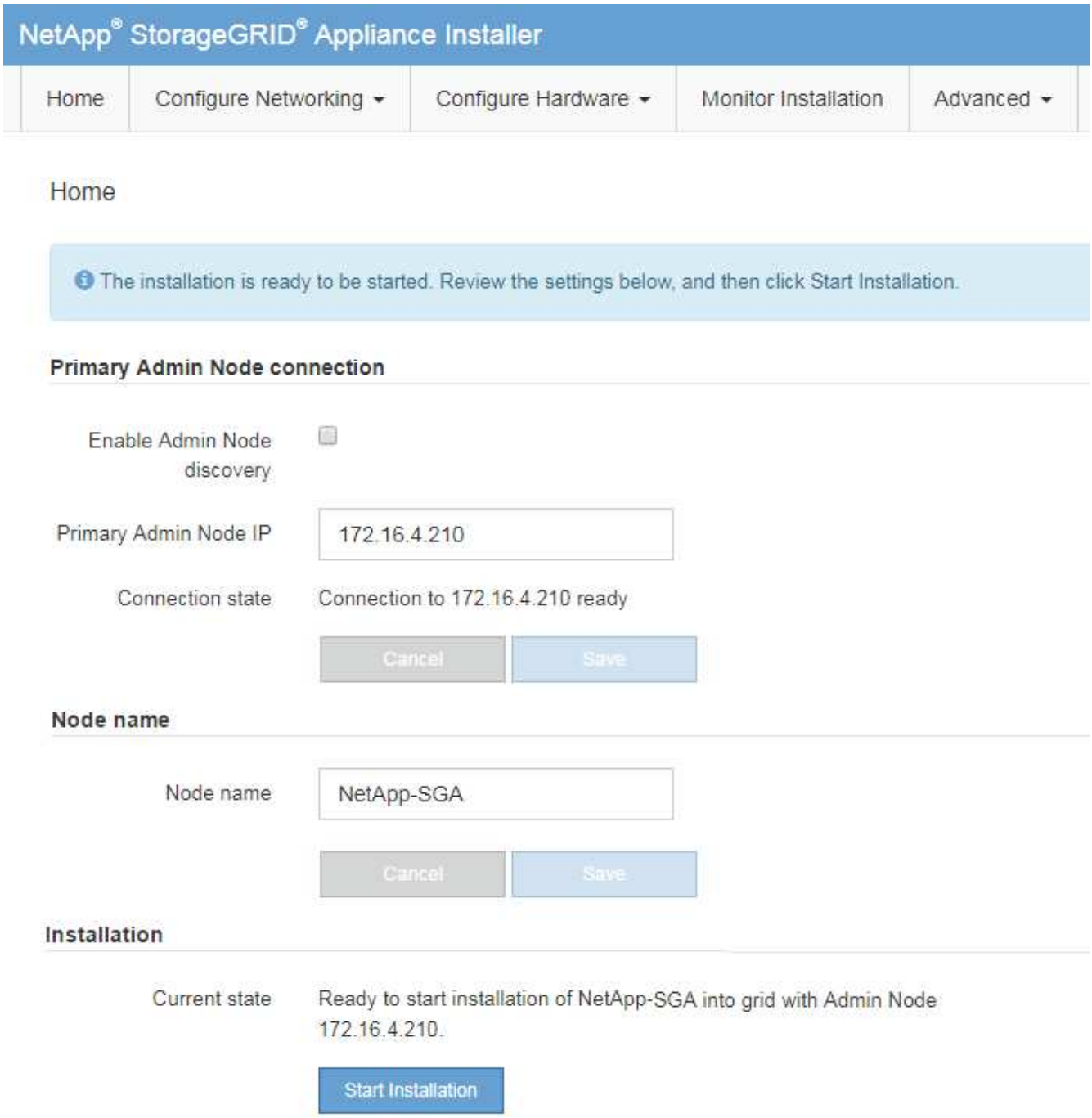
> Si necesita implementar varios nodos de dispositivos a la vez, puede automatizar el proceso de instalación mediante el `configure-sga.py` Script de instalación del dispositivo.

- Si va a realizar una operación de expansión o recuperación, siga las instrucciones correspondientes:
  - Para añadir un nodo de almacenamiento del dispositivo a un sistema StorageGRID existente, consulte las instrucciones para ampliar un sistema StorageGRID.
  - Para poner en marcha un nodo de almacenamiento del dispositivo como parte de una operación de recuperación, consulte las instrucciones de recuperación y mantenimiento.

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. Anule la selección de la casilla de verificación **Activar descubrimiento de nodo de administración**. 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.
Detección automática de todos los nodos principales de administración conectados	a. Active la casilla de verificación **Activar descubrimiento de nodos de administración**. 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 haga clic en **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 instalación, confirme que el estado actual es "Listo para iniciar la instalación de `node name` En el grid con el nodo de administrador principal `admin_ip` " Y que el botón **Iniciar instalación** 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 instalación y mantenimiento del aparato.

   > Si va a poner en marcha el dispositivo Storage Node como destino de clonado de nodos, detenga el proceso de puesta en marcha aquí y continúe con el procedimiento de clonado de nodos en recuperación y mantenimiento.

   Recuperación y mantenimiento

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**.

7. Si el grid incluye varios nodos de almacenamiento de dispositivos, repita estos pasos para cada dispositivo.

> Si necesita implementar varios nodos de almacenamiento para dispositivos a la vez, puede automatizar el proceso de instalación mediante el `configure-sga.py` script de instalación del dispositivo.

Información relacionada

Amplíe su grid

Recuperación y mantenimiento

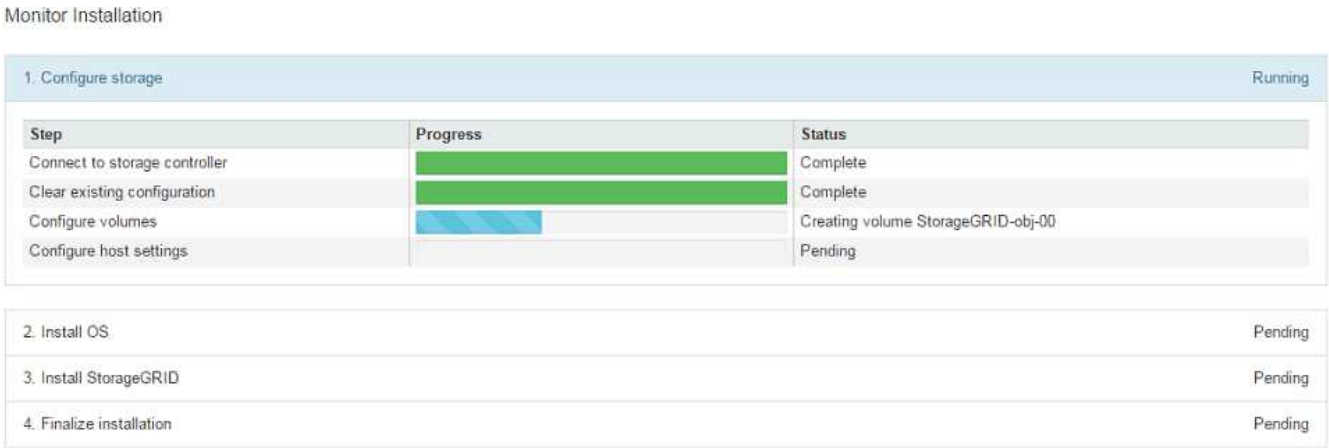
Supervise la instalación de dispositivos de almacenamiento

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**.

   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.

> El instalador garantiza que no se vuelvan a ejecutar las tareas completadas en una instalación anterior. 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 de "Shided."

2. Revise el progreso de las dos primeras etapas de instalación.

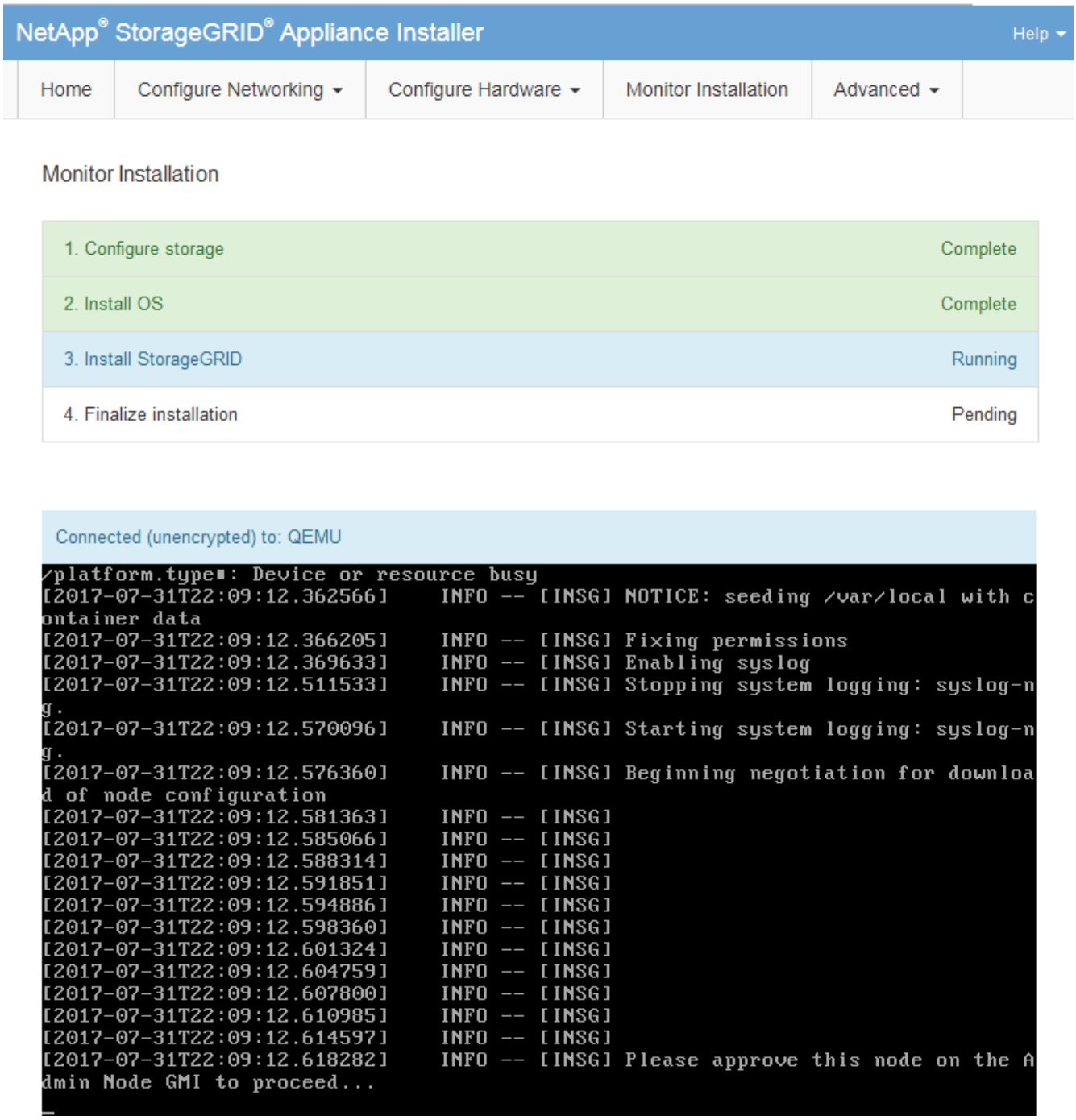
   1. Configurar almacenamiento

   Durante esta fase, el instalador se conecta al controlador de almacenamiento, borra cualquier configuración existente, se comunica con el software 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, solicitándole que apruebe este nodo en el nodo de administración mediante el Administrador de grid. Vaya al paso siguiente.



4. Vaya a Grid Manager del nodo Primary Admin, apruebe el nodo de almacenamiento pendiente y complete el proceso de instalación de StorageGRID.

   Al hacer clic en **instalar** desde Grid Manager, se completa la fase 3 y comienza la fase 4, **Finalizar instalación**. Cuando finaliza la etapa 4, se reinicia la controladora.

Automatizar la instalación y configuración del dispositivo (SG5600)

Puede automatizar la instalación y configuración de sus dispositivos y la configuración de todo el sistema StorageGRID.

Acerca de esta tarea

Automatizar la instalación y la configuración puede ser útil para poner en marcha varias instancias de StorageGRID o una instancia de StorageGRID grande y compleja.

Para automatizar la instalación y configuración, utilice una o varias de las siguientes opciones:

- Cree un archivo JSON que especifique las opciones de configuración para los dispositivos. Cargue el archivo JSON con el instalador de dispositivos StorageGRID.

  Puede usar el mismo archivo para configurar más de un dispositivo.

- Utilice la StorageGRID`configure-sga.py` Script Python para automatizar la configuración de sus dispositivos.
- Utilice scripts Python adicionales para configurar otros componentes de todo el sistema StorageGRID (la "cuadrícula").

Puede utilizar directamente los scripts Python de automatización de StorageGRID o bien puede usarlos como ejemplos de cómo utilizar la API DE REST de instalación de StorageGRID en las herramientas de puesta en marcha de grid y de configuración que desarrolla usted mismo. Consulte la información acerca de Descarga y extracción de los archivos de instalación de StorageGRID.

Automatice la configuración del dispositivo con StorageGRID Appliance Installer

Puede automatizar la configuración de un dispositivo mediante un archivo JSON que contiene la información de configuración. El archivo se carga con el instalador de dispositivos de StorageGRID.

Lo que necesitará

- El dispositivo debe tener el firmware más reciente compatible con StorageGRID 11.5 o superior.
- Debe estar conectado al instalador de dispositivos de StorageGRID en el dispositivo que esté configurando mediante un navegador web compatible.

Acerca de esta tarea

Puede automatizar las tareas de configuración de los dispositivos, como la configuración de las siguientes opciones:

- Redes de grid, red de administración y direcciones IP de red de cliente
- Interfaz BMC
- Enlaces de red
  - Modo de enlace de puerto
  - Modo de enlace de red
  - Velocidad de enlace

La configuración del dispositivo con un archivo JSON cargado suele ser más eficaz que realizar la configuración manualmente mediante múltiples páginas en el instalador del dispositivo StorageGRID, especialmente si tiene que configurar muchos nodos. Debe aplicar el archivo de configuración para cada nodo de uno en uno.

> Los usuarios con experiencia que deseen automatizar tanto la instalación como la configuración de sus dispositivos pueden utilizar el `configure-sga.py` guión. +Automatice la instalación y configuración de los nodos de los dispositivos con un script configure-sga.py

Pasos

1. Genere el archivo JSON mediante uno de los siguientes métodos:
   - Aplicación ConfigBuilder

     "ConfigBuilder.netapp.com"

   - La `configure-sga.py` script de configuración del dispositivo. Puede descargar la secuencia de comandos desde el instalador del dispositivo StorageGRID (**Ayuda** > **secuencia de comandos de configuración del dispositivo**). Consulte las instrucciones sobre cómo automatizar la configuración mediante el script configure-sga.py.

     Automatice la instalación y configuración de los nodos de los dispositivos con un script configure-sga.py

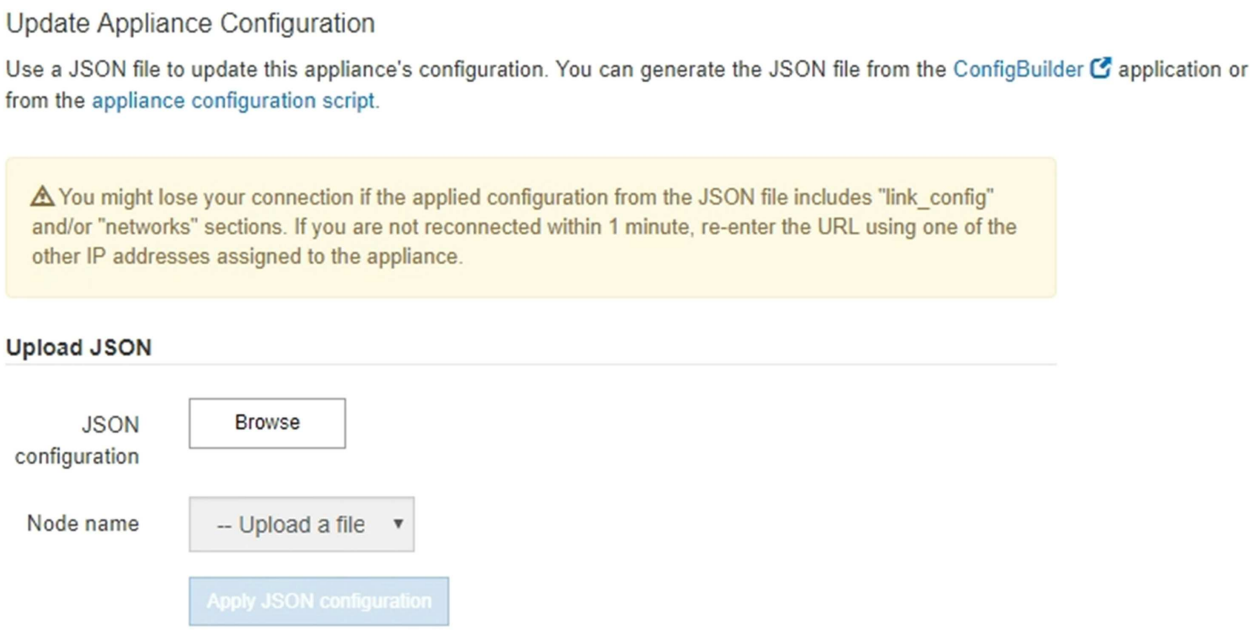
     Los nombres de nodos en el archivo JSON deben seguir estos requisitos:

     - Debe ser un nombre de host válido que contenga al menos 1 y no más de 32 caracteres
     - Puede usar letras, números y guiones
     - No se puede iniciar o finalizar con un guión
     - No puede contener solo números

     > Asegúrese de que los nombres de nodo (los nombres de nivel superior) del archivo JSON son únicos o de que no pueda configurar más de un nodo mediante el archivo JSON.

2. Seleccione **Avanzado** > **Actualizar configuración del dispositivo**.

   Aparece la página Actualizar configuración del dispositivo.



3. Seleccione el archivo JSON con la configuración que desea cargar.

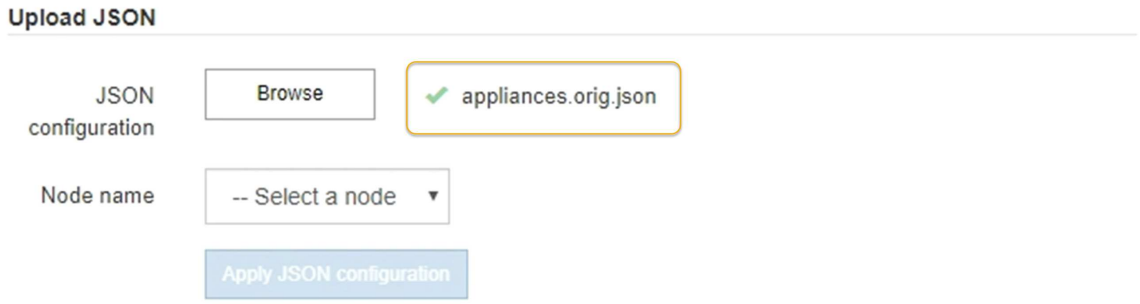
   a. Seleccione **examinar**.

   b. Localice y seleccione el archivo.

   c. Seleccione **Abrir**.

   El archivo se carga y se valida. Una vez completado el proceso de validación, se muestra el nombre del archivo junto a una Marca de verificación verde.

   > Es posible que pierda la conexión con el dispositivo si la configuración del archivo JSON incluye secciones de "link_config", "Networks" o ambas. Si no vuelve a conectarse en 1 minuto, vuelva a introducir la URL del dispositivo utilizando una de las otras direcciones IP asignadas al dispositivo.

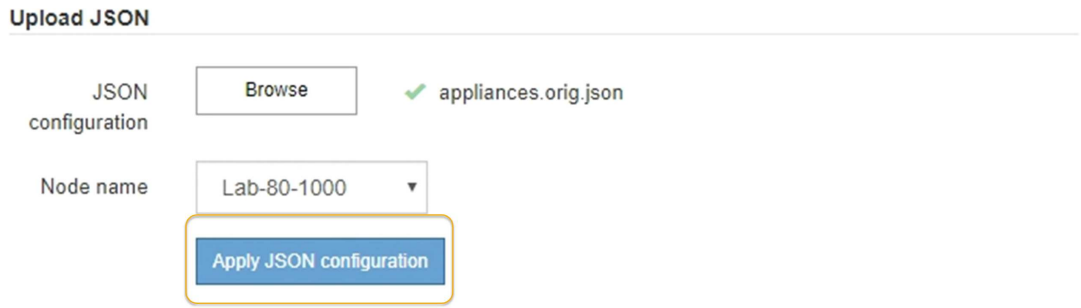


   La lista desplegable **Nombre de nodo** se rellena con los nombres de nodo de nivel superior definidos en el archivo JSON.

Si el archivo no es válido, el nombre del archivo se muestra en rojo y se muestra un mensaje de error en un banner amarillo. El archivo no válido no se ha aplicado al dispositivo. Puede utilizar ConfigBuilder para asegurarse de tener un archivo JSON válido.

4. Seleccione un nodo de la lista de la lista desplegable **Nombre de nodo**.

   El botón **aplicar configuración JSON** está activado.



5. Seleccione **aplicar configuración JSON**.

   La configuración se aplica al nodo seleccionado.

Automatice la instalación y configuración de los nodos de los dispositivos con un script configure-sga.py

Puede utilizar el `configure-sga.py` Script para automatizar muchas de las tareas de instalación y configuración para los nodos del dispositivo StorageGRID, incluida la instalación y configuración de un nodo de administración principal. Esta secuencia de comandos puede ser útil si tiene un gran número de dispositivos que configurar. También puede usar el script para generar un archivo JSON que contenga información de configuración del dispositivo.

Lo que necesitará

- 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 nodo de administración principal mediante el instalador de dispositivos de StorageGRID.
- Si está instalando el nodo de administrador principal, conoce su dirección IP.
- Si va a instalar y configurar otros nodos, el nodo de administrador principal se ha implementado y conoce su dirección IP.
- Para todos los nodos que no sean el nodo de administración principal, todas las subredes de red de cuadrícula que aparecen en la página Configuración de IP del instalador de dispositivos StorageGRID se han definido en la lista de subredes de redes de cuadrícula del nodo de administración principal.
- Ha descargado el `configure-sga.py` archivo. El archivo se incluye en el archivo de instalación o puede acceder a él haciendo clic en **Ayuda** > **secuencia de comandos de instalación del dispositivo** en el instalador del dispositivo StorageGRID.

Este procedimiento es para usuarios avanzados con cierta experiencia usando interfaces de línea de comandos. También puede usar el instalador de dispositivos de StorageGRID para automatizar la configuración. +Automatice la configuración del dispositivo con StorageGRID Appliance Installer

Pasos

1. Inicie sesión en el equipo Linux que está utilizando para ejecutar el script Python.
2. Para obtener ayuda general sobre la sintaxis de la secuencia de comandos y ver una lista de los parámetros disponibles, introduzca lo siguiente:

   ```
   configure-sga.py --help
   ```

   La `configure-sga.py` el script utiliza cinco subcomandos:

   - `advanced` Para interacciones avanzadas con dispositivos StorageGRID, incluida la configuración del BMC y la creación de un archivo JSON con la configuración actual del dispositivo
   - `configure` Para configurar los parámetros de modo RAID, nombre del nodo y red
   - `install` Para iniciar una instalación de StorageGRID
   - `monitor` Para supervisar una instalación de StorageGRID
   - `reboot` para reiniciar el dispositivo

   Si introduce un argumento de subcomando (avanzado, configure, instale, monitor o reboot) seguido del `--help` opción usted obtendrá un texto de ayuda diferente que proporciona más detalles sobre las opciones disponibles dentro de ese subcomando:
   `configure-sga.py` *`subcommand`* `--help`

3. Para confirmar la configuración actual del nodo del dispositivo, introduzca lo siguiente donde *`SGA-install-ip`* Es cualquiera de las direcciones IP del nodo del dispositivo:
   `configure-sga.py configure` *`SGA-INSTALL-IP`*

   Los resultados muestran información de IP actual del dispositivo, incluida la dirección IP del nodo de administración principal e información sobre las redes de administración, grid y cliente.

   ```
   Connecting to +https://10.224.2.30:8443+ (Checking version and
   connectivity.)
   2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
   2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
   200
   2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
   Received 200
   2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
   200
   2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
   2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
   200
   ```

```
StorageGRID Appliance
  Name:        LAB-SGA-2-30
  Node type:   storage

StorageGRID primary Admin Node
  IP:        172.16.1.170
  State:     unknown
  Message:   Initializing...
  Version:   Unknown

Network Link Configuration
  Link Status
        Link      State      Speed (Gbps)
        ----      -----      -----
        1         Up         10
        2         Up         10
        3         Up         10
        4         Up         10
        5         Up         1
        6         Down       N/A

  Link Settings
      Port bond mode:      FIXED
      Link speed:          10GBE

      Grid Network:        ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

      Admin Network:       ENABLED
          Bonding mode:    no-bond
          MAC Addresses:   00:80:e5:29:70:f4

      Client Network:      ENABLED
          Bonding mode:    active-backup
          VLAN:            novlan
          MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

Grid Network
  CIDR:      172.16.2.30/21 (Static)
  MAC:       00:A0:98:59:8E:8A
  Gateway:   172.16.0.1
  Subnets:   172.17.0.0/21
             172.18.0.0/21
             192.168.0.0/21
```

```
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

#################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#################################################################
```

4. Si necesita cambiar alguno de los valores de la configuración actual, utilice `configure` subcomando para actualizarlos. Por ejemplo, si desea cambiar la dirección IP que utiliza el dispositivo para conectarse al nodo de administración principal `172.16.2.99`, introduzca lo siguiente:
   `configure-sga.py configure --admin-ip 172.16.2.99` *`SGA-INSTALL-IP`*
5. Si desea realizar un backup de la configuración del dispositivo en un archivo JSON, utilice `advanced` y.. `backup-file` subcomandos. Por ejemplo, si desea realizar una copia de seguridad de la configuración de un dispositivo con dirección IP *`SGA-INSTALL-IP`* a un archivo llamado `appliance-SG1000.json`, introduzca lo siguiente:
   `configure-sga.py advanced --backup-file appliance-SG1000.json` *`SGA-INSTALL-IP`*

   El archivo JSON que contiene la información de configuración se escribe en el mismo directorio desde el que se ejecutó la secuencia de comandos.

   > Compruebe que el nombre del nodo de nivel superior del archivo JSON generado coincida con el nombre del dispositivo. No haga ningún cambio en este archivo a menos que sea un usuario con experiencia y que tenga una profunda comprensión de las API de StorageGRID.

6. Cuando esté satisfecho con la configuración del dispositivo, utilice `install` y.. `monitor` subcomandos para instalar el dispositivo:
   `configure-sga.py install --monitor` *`SGA-INSTALL-IP`*
7. Si desea reiniciar el dispositivo, introduzca lo siguiente:
   `configure-sga.py reboot` *`SGA-INSTALL-IP`*

Automatice la configuración de StorageGRID

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

Lo que necesitará

- 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
```

Después de terminar

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 ha especificado que se deben generar contraseñas aleatorias, debe extraer 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 general sobre la instalación de API de REST

StorageGRID proporciona dos API REST para realizar tareas de instalación: La API de instalación de StorageGRID y la API del instalador de dispositivos de StorageGRID.

Ambas API utilizan 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 (notación de objetos JavaScript).

> 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 configura inicialmente el sistema StorageGRID y en el caso de que deba realizar una recuperación de nodo de administrador principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de API, vaya a la página web de instalación del nodo de administración principal y seleccione **Ayuda** > **Documentación de 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.
- **Sites** — Operaciones de configuración a nivel de sitio. Puede crear, ver, eliminar y modificar un sitio.

API del instalador de dispositivos de StorageGRID

Se puede acceder a la API del instalador de dispositivos de StorageGRID a través de HTTPS desde `Controller_IP:8443`.

Para acceder a la documentación de la API, vaya al instalador del dispositivo StorageGRID en el dispositivo y seleccione **Ayuda** > **Documentación de la API** en la barra de menús.

La API del instalador de dispositivos de StorageGRID incluye las siguientes secciones:

- **Clone** — Operaciones para configurar y controlar la clonación de nodos.
- **Cifrado** — Operaciones para administrar el cifrado y ver el estado del cifrado.
- **Configuración del hardware** — Operaciones para configurar los ajustes del sistema en el hardware conectado.
- **Instalación** — Operaciones para iniciar la instalación del aparato y para supervisar el estado de instalación.
- **Redes** — Operaciones relacionadas con la configuración de red de Grid, Admin y Cliente para un dispositivo StorageGRID y los ajustes de puerto de dispositivo.
- **Setup** — Operaciones para ayudar con la instalación inicial del dispositivo incluyendo solicitudes para obtener información sobre el sistema y actualizar el IP principal del nodo de administración.
- **SOPORTE** — Operaciones para reiniciar el controlador y obtener registros.
- **Upgrade** — Operaciones relacionadas con la actualización del firmware del dispositivo.
- **Uploadsg** — Operaciones para cargar archivos de instalación de StorageGRID.

Solucionar problemas de instalación de hardware (SG5600)

Si encuentra problemas durante la instalación, es posible que le sea útil revisar información sobre la solución de problemas relacionados con la configuración del hardware y los problemas de conectividad.

La configuración del hardware parece que se bloquea (SG5600)

Es posible que el instalador de dispositivos StorageGRID no esté disponible si los errores de hardware o de cableado impiden que la controladora E5600SG complete su procesamiento de arranque.

Pasos

1. Compruebe el LED de atención necesaria en cualquiera de los controladores y busque un código de error parpadeante.

   Durante el encendido, los LED de acción de servicio permitida y Acción de servicio requerida se encienden mientras el hardware se está inicializando. El punto decimal superior del dígito inferior, llamado *LED* de diagnóstico, también se ilumina. La pantalla de siete segmentos recorre una secuencia de códigos que son comunes para ambos controladores. Esto es normal y no es una indicación de un error. Cuando el hardware se arranca correctamente, los LED de acción de servicio se apagan y las pantallas se basan en el firmware.

2. Revise los códigos de la pantalla de siete segmentos del controlador E5600SG.

   > La instalación y el aprovisionamiento tardan en realizarse. Algunas fases de instalación no notifican las actualizaciones del instalador de dispositivos StorageGRID durante varios minutos.

   Si se produce un error, la pantalla de siete segmentos parpadea en una secuencia, como ÉL.

3. Para comprender qué significan estos códigos, consulte los siguientes recursos:

Controladora	Referencia
Controladora E5600SG	• "'he error: Sincronización de errores con el software de sistema operativo SANtricity'" • "'códigos de visualización de siete segmentos del controlador E5600SG'"
Controladora E2700	Documentación de E-Series **Nota:** los códigos descritos para el controlador E-Series E5600 no se aplican al controlador E5600SG del aparato.

4. Si esto no se resuelve el problema, póngase en contacto con el soporte técnico.

Información relacionada

códigos de visualización de siete segmentos de la controladora E5600SG

Error: Error al sincronizar con el software de sistema operativo SANtricity

"Guía de instalación de soporte de unidades de controladora E2700 y soportes de unidades relacionadas"

"Documentación de NetApp: Serie E2700"

Error: Error al sincronizar con el software de sistema operativo SANtricity

La visualización de siete segmentos en la controladora de computación muestra un código de error HE si el instalador de dispositivos de StorageGRID no puede sincronizarse con el software de sistema operativo SANtricity.

Acerca de esta tarea

Si se muestra UN código DE error, lleve a cabo esta acción correctiva.

Pasos

1. Compruebe la integridad de los dos cables de interconexión SAS y confirme que están conectados de forma segura.
2. Según sea necesario, sustituya uno o ambos cables y vuelva a intentarlo.
3. Si esto no se resuelve el problema, póngase en contacto con el soporte técnico.

Solucionar problemas de conexión (SG5600)

Si tiene problemas de conexión durante la instalación del dispositivo StorageGRID, debe ejecutar los pasos de acción correctiva indicados.

No se puede conectar con el dispositivo StorageGRID a través de la red

Si no puede conectarse al dispositivo, puede haber un problema de red o es posible que la instalación del hardware no se haya completado correctamente.

- **Edición**

  No puede conectar al aparato.

- **Causa**

  Esto podría ocurrir si hay un problema de red o la instalación del hardware no se completó correctamente.

- **Acción Correctiva**

  a. Ping en el aparato:
  `ping E5600_controller_IP`

  b. Abra un explorador e introduzca lo siguiente para acceder al instalador de dispositivos de StorageGRID:
  `https://Management_Port_IP:8443`

  Para Management_Port_IP, introduzca la dirección IP para el puerto de gestión 1 en la controladora E5600SG (aprovisionada durante la instalación física).

  c. Haga clic en **Configurar red de administración** y compruebe la dirección IP.

  d. Si recibe una respuesta del ping, compruebe que el puerto 8443 está abierto en los firewalls.

  e. Reinicie el dispositivo.

  f. Actualice la página web de instalación.

  g. Si esto no resuelve el problema de conexión, póngase en contacto con el soporte técnico del sitio de soporte de NetApp en "mysupport.netapp.com".

Información relacionada

códigos de visualización de siete segmentos de la controladora E5600SG

Reinicie el controlador mientras el instalador de dispositivos StorageGRID está en ejecución

Es posible que deba reiniciar la controladora de computación mientras se está ejecutando el instalador de dispositivos de StorageGRID. Por ejemplo, es posible que deba reiniciar la controladora si la instalación falla.

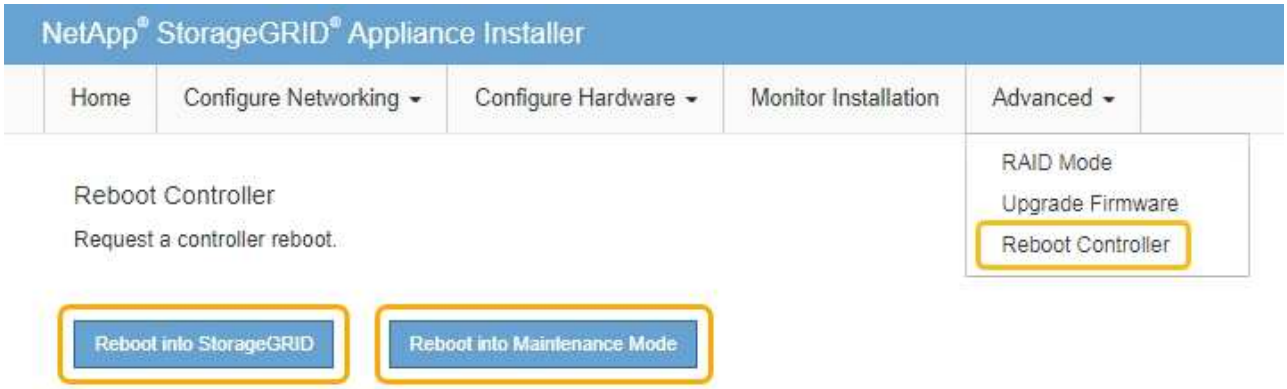
Acerca de esta tarea

Este procedimiento solo se aplica cuando la controladora de computación ejecuta el instalador de dispositivos de StorageGRID. Una vez finalizada la instalación, este paso ya no funciona porque el instalador de dispositivos StorageGRID ya no está disponible.

Pasos

1. En el instalador del dispositivo StorageGRID, haga clic en **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



   Se reinicia la controladora.

Mantenga el dispositivo SG5600

Es posible que deba actualizar el software de sistema operativo SANtricity en la controladora E2700, sustituir la controladora E2700 o la controladora E5600SG, o sustituir componentes específicos. En los procedimientos descritos en esta sección se asume que el dispositivo ya se ha puesto en marcha como nodo de almacenamiento en un sistema StorageGRID.

Coloque el dispositivo en modo de mantenimiento

Debe colocar el aparato en modo de mantenimiento antes de realizar procedimientos de mantenimiento específicos.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso de mantenimiento o acceso raíz. Para obtener más detalles, consulte las instrucciones para administrar StorageGRID.

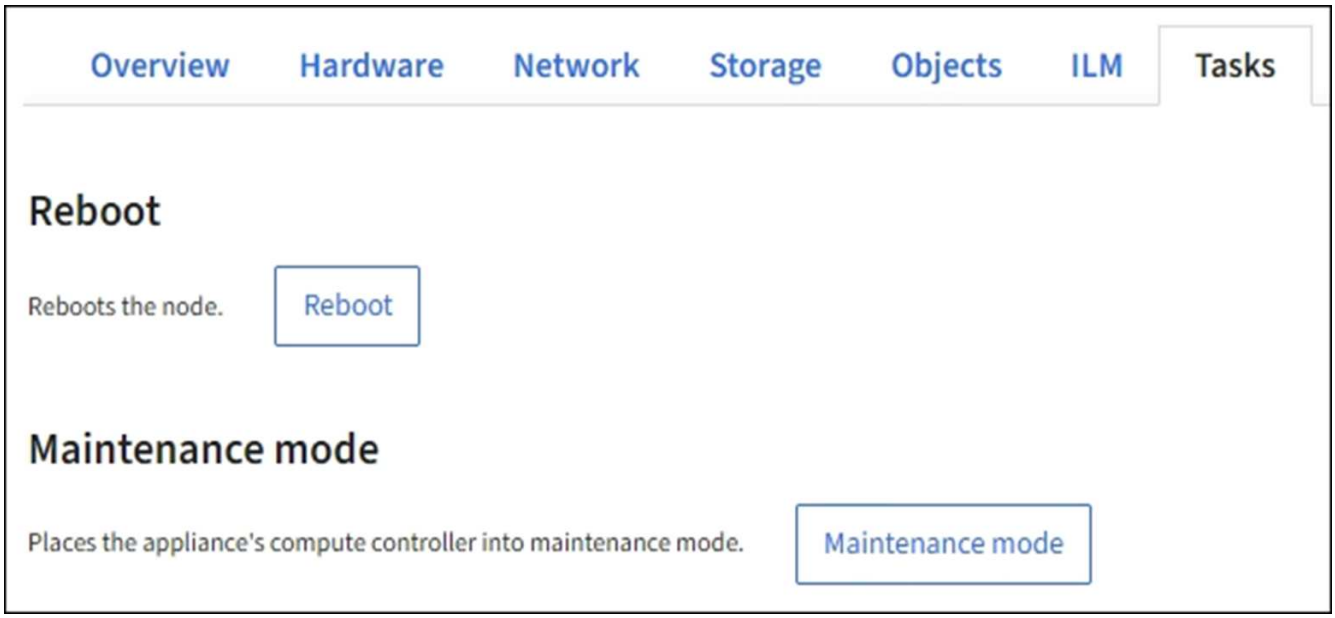
Acerca de esta tarea

En raras ocasiones, una vez que se coloca un dispositivo StorageGRID en modo de mantenimiento puede hacer que el dispositivo no esté disponible para el acceso remoto.

> La contraseña de la cuenta de administrador y las claves de host SSH para un dispositivo StorageGRID en modo de mantenimiento siguen siendo las mismas que en el momento en que el dispositivo estaba en servicio.

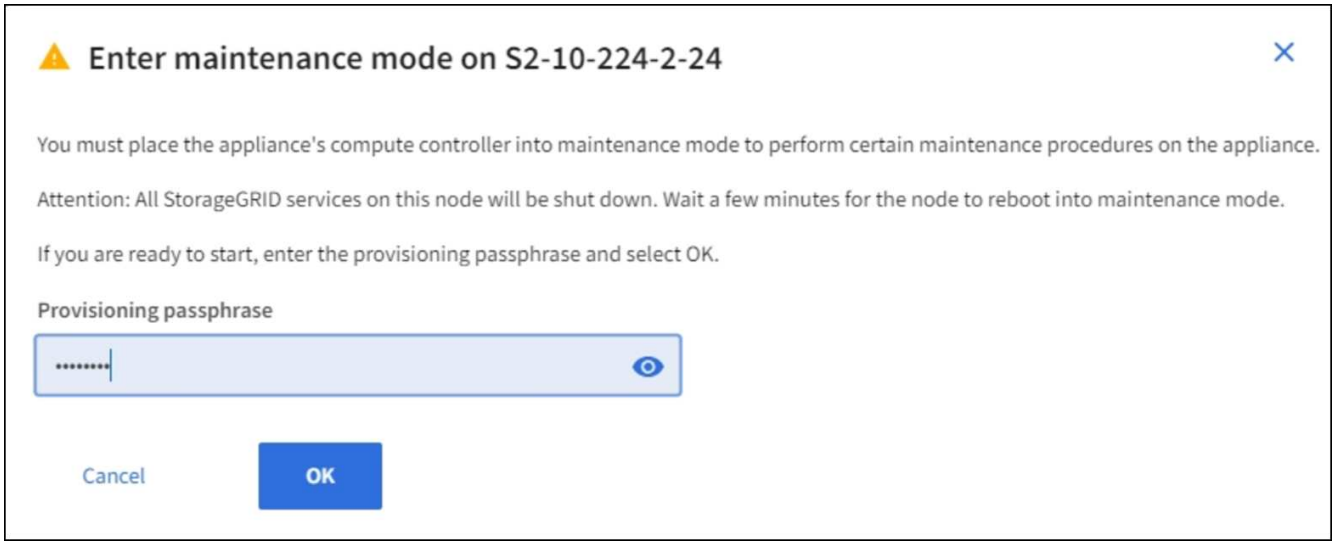
Pasos

1. En Grid Manager, seleccione **NODES**.
2. En la vista de árbol de la página Nodes, seleccione Appliance Storage Node.
3. Seleccione **tareas**.



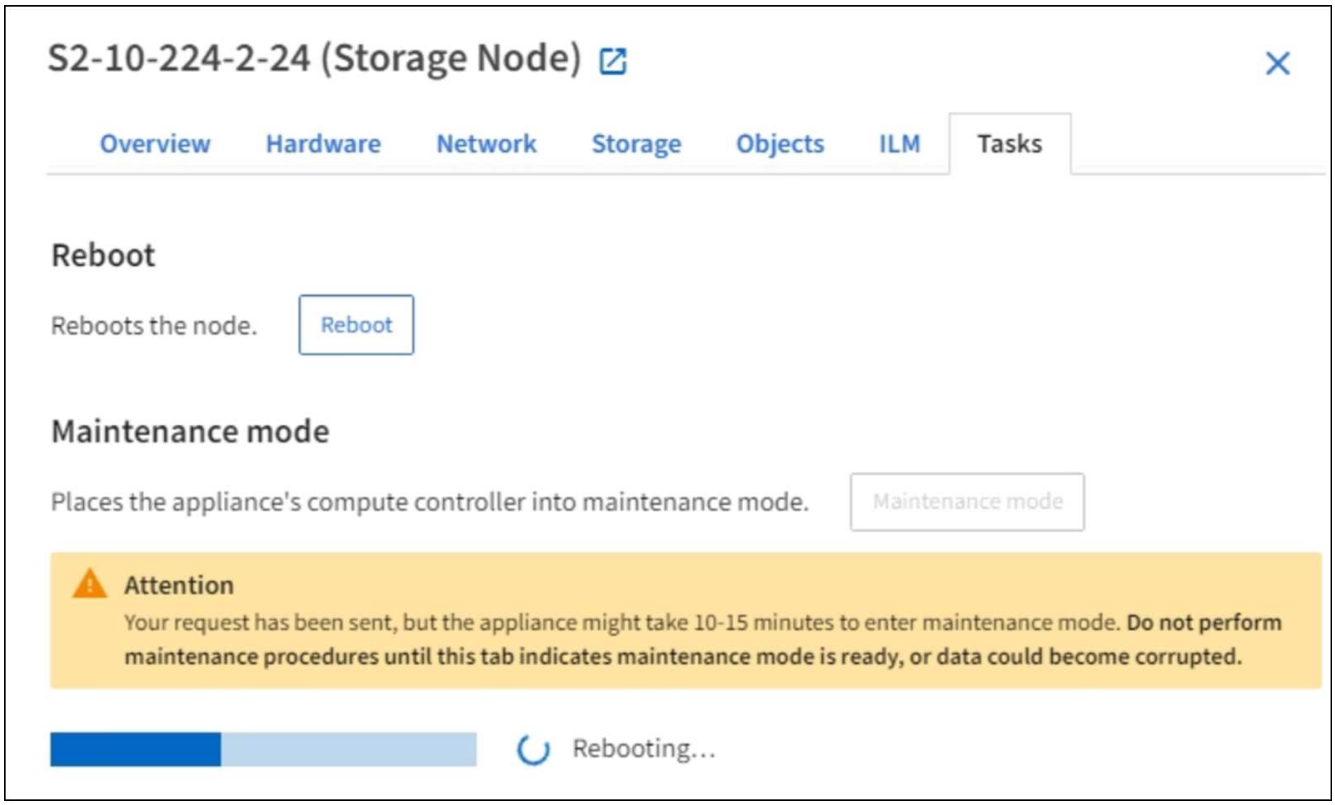
4. Seleccione **modo de mantenimiento**.

   Se muestra un cuadro de diálogo de confirmación.

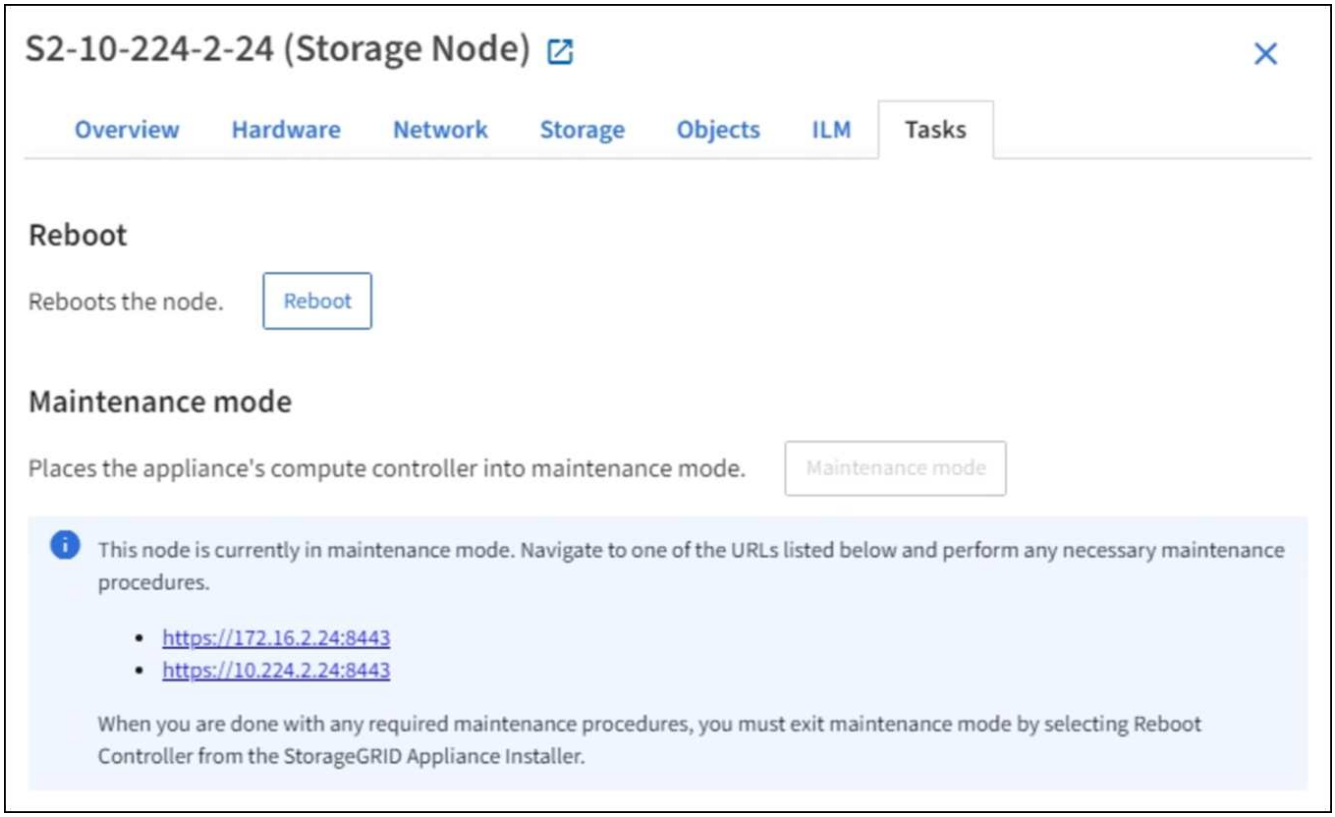


5. Introduzca la contraseña de aprovisionamiento y seleccione **Aceptar**.

   Una barra de progreso y una serie de mensajes, incluidos "solicitud enviada", "detención de StorageGRID" y "reinicio", indican que el dispositivo está llevando a cabo los pasos necesarios para entrar en el modo de mantenimiento.



   Cuando el dispositivo se encuentra en modo de mantenimiento, un mensaje de confirmación enumera las URL que puede utilizar para acceder al instalador de dispositivos de StorageGRID.



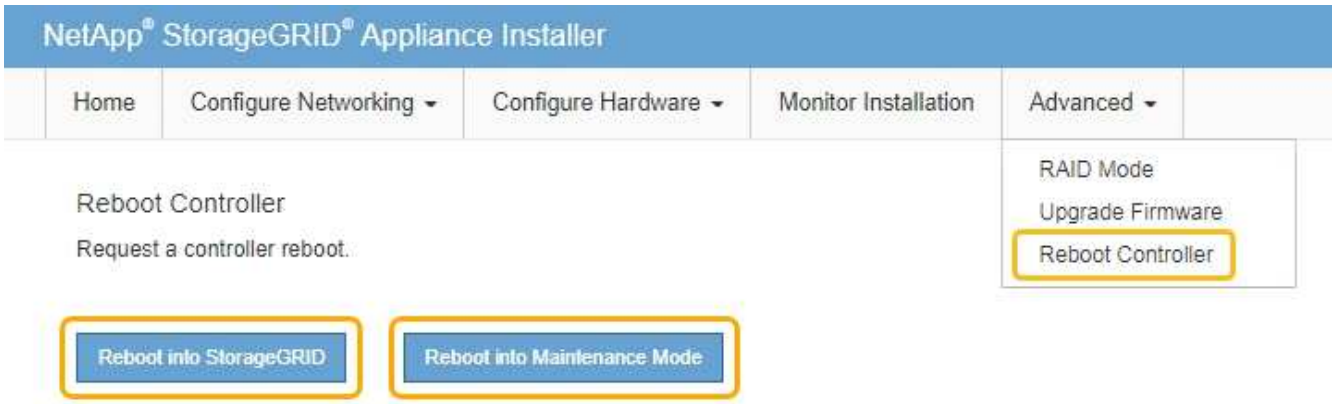
6. Para acceder al instalador de dispositivos de StorageGRID, busque cualquiera de las direcciones URL que se muestren.

   Si es posible, utilice la dirección URL que contiene la dirección IP del puerto de red de administración del dispositivo.

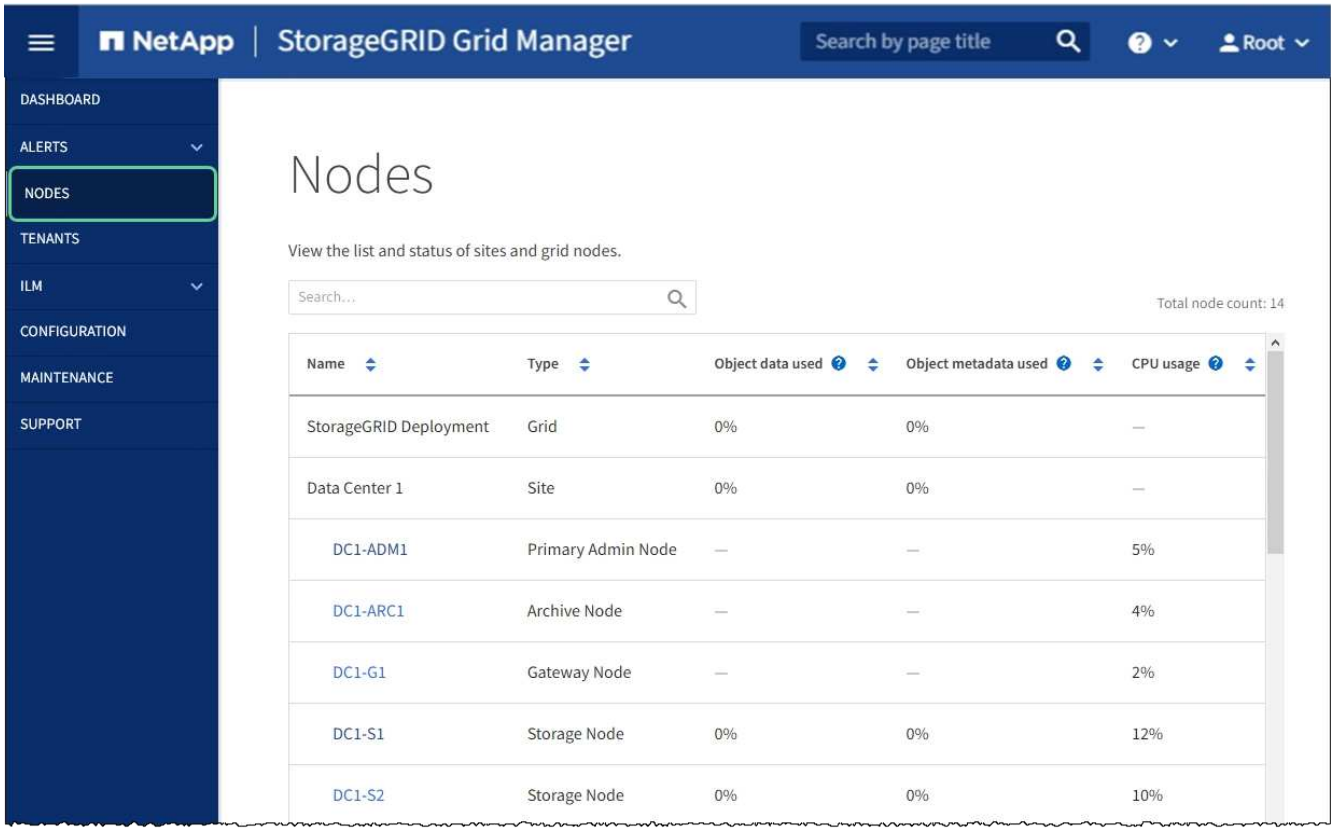
   > Si tiene una conexión directa con el puerto de gestión del dispositivo, utilice `https://169.254.0.1:8443` Para acceder a la página del instalador de dispositivos de StorageGRID.

7. En el instalador de dispositivos StorageGRID, confirme que el dispositivo está en modo de mantenimiento.

8. Realice las tareas de mantenimiento necesarias.
9. Después de completar las tareas de mantenimiento, salga del modo de mantenimiento y reanude el funcionamiento normal del nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione **Reiniciar en StorageGRID**.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante Grid Manager

Para aplicar una actualización, se deben usar Grid Manager para las controladoras de almacenamiento que actualmente utilizan SANtricity OS 08.42.20.00 (11.42) o posterior.

Lo que necesitará

- Ha consultado con la herramienta de matriz de interoperabilidad (IMT) de NetApp para confirmar que la versión del sistema operativo SANtricity que utiliza para la actualización es compatible con su dispositivo.

- Tiene el permiso de mantenimiento o acceso raíz.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene la clave de acceso de aprovisionamiento.
- Tiene acceso a la página de descargas de NetApp para SANtricity OS.

Acerca de esta tarea

No puede realizar otras actualizaciones de software (actualización de software StorageGRID o revisión) hasta que haya completado el proceso de actualización de sistema operativo SANtricity. Si intenta iniciar una revisión o una actualización de software de StorageGRID antes de que haya finalizado el proceso de actualización de SANtricity OS, se le redirigirá a la página de actualización de SANtricity OS.

No se completará el procedimiento hasta que la actualización del sistema operativo SANtricity se haya aplicado correctamente a todos los nodos aplicables seleccionados para la actualización. Es posible que tardar más de 30 minutos cargar el sistema operativo SANtricity en cada nodo (de forma secuencial) y hasta 90 minutos para reiniciar cada dispositivo de almacenamiento StorageGRID.

> Los siguientes pasos sólo son aplicables cuando se utiliza Grid Manager para realizar la actualización. No es posible actualizar las controladoras de almacenamiento en el dispositivo mediante Grid Manager cuando las controladoras utilizan SANtricity OS anteriores a 08.42.20.00 (11.42).

> Este procedimiento actualizará automáticamente la NVSRAM a la versión más reciente asociada con la actualización del sistema operativo SANtricity. No es necesario aplicar un archivo de actualización de NVSRAM aparte.

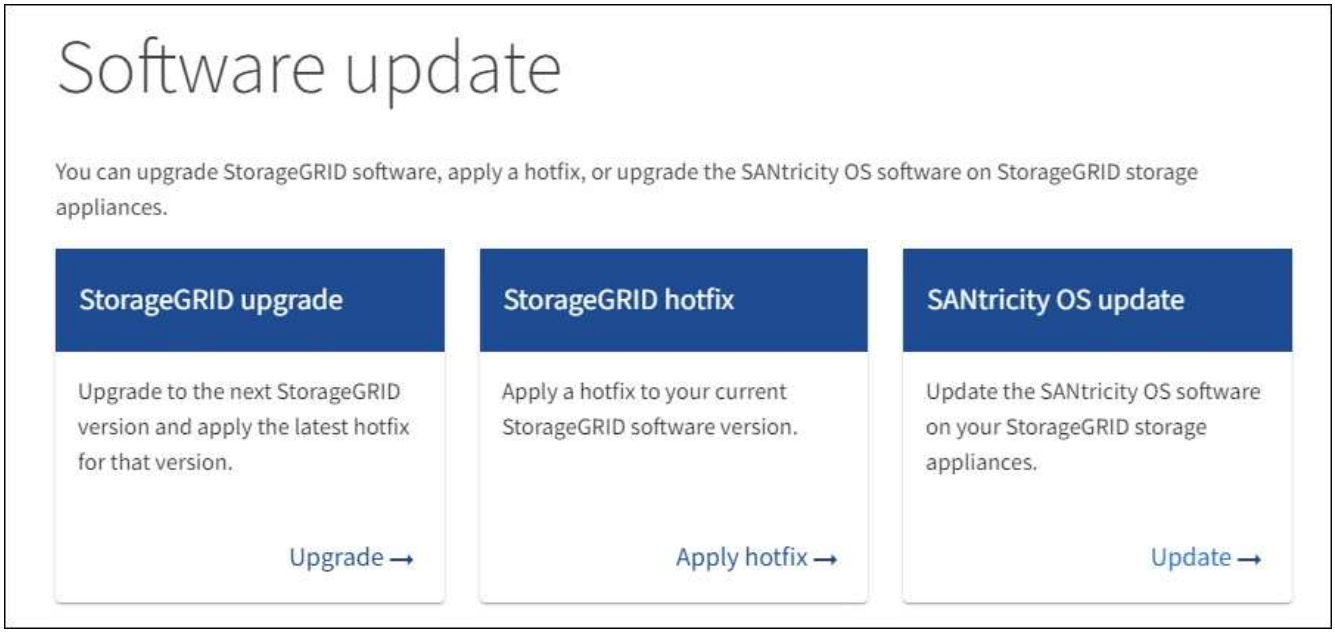
Pasos

1. Descargar el nuevo archivo de software de sistema operativo SANtricity del sitio de soporte de NetApp.

   Asegúrese de elegir la versión de sistema operativo SANtricity para las controladoras de almacenamiento.

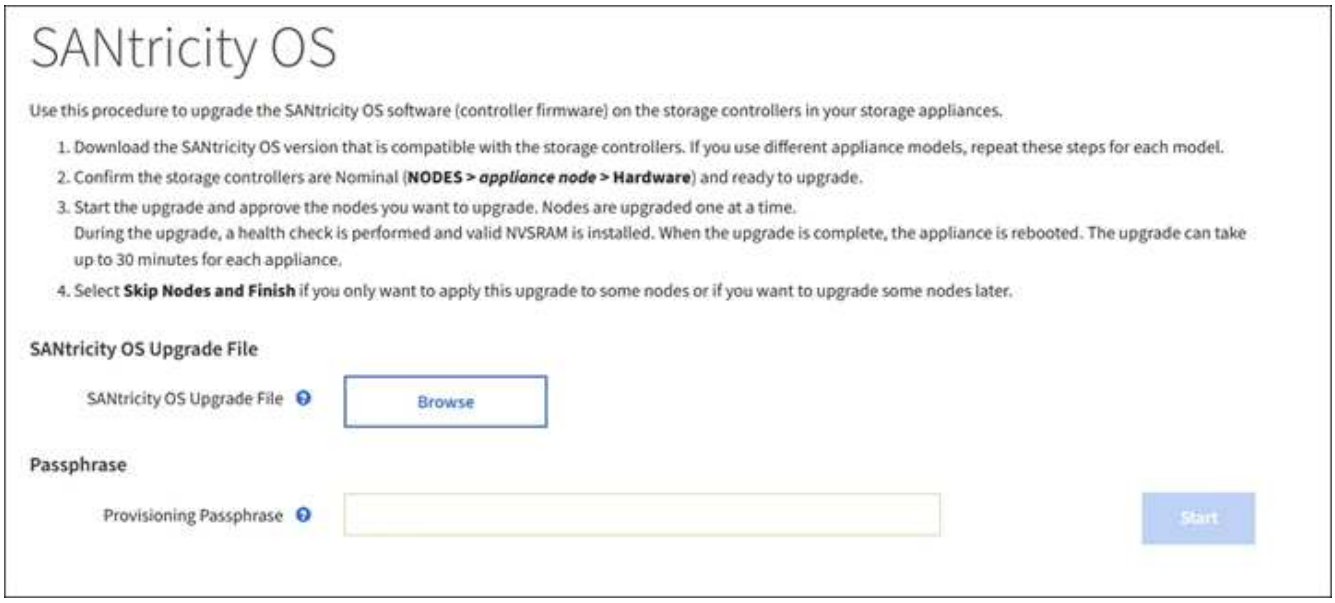
   "Descargas de NetApp: Dispositivo de StorageGRID"

2. Seleccione **MANTENIMIENTO** > **sistema** > **actualización de software**.



3. En la sección actualización del sistema operativo SANtricity, seleccione **Actualizar**.

   Se muestra la página actualización de sistema operativo SANtricity.



4. Seleccione el archivo de actualización del sistema operativo SANtricity que descargó del sitio de soporte de NetApp.

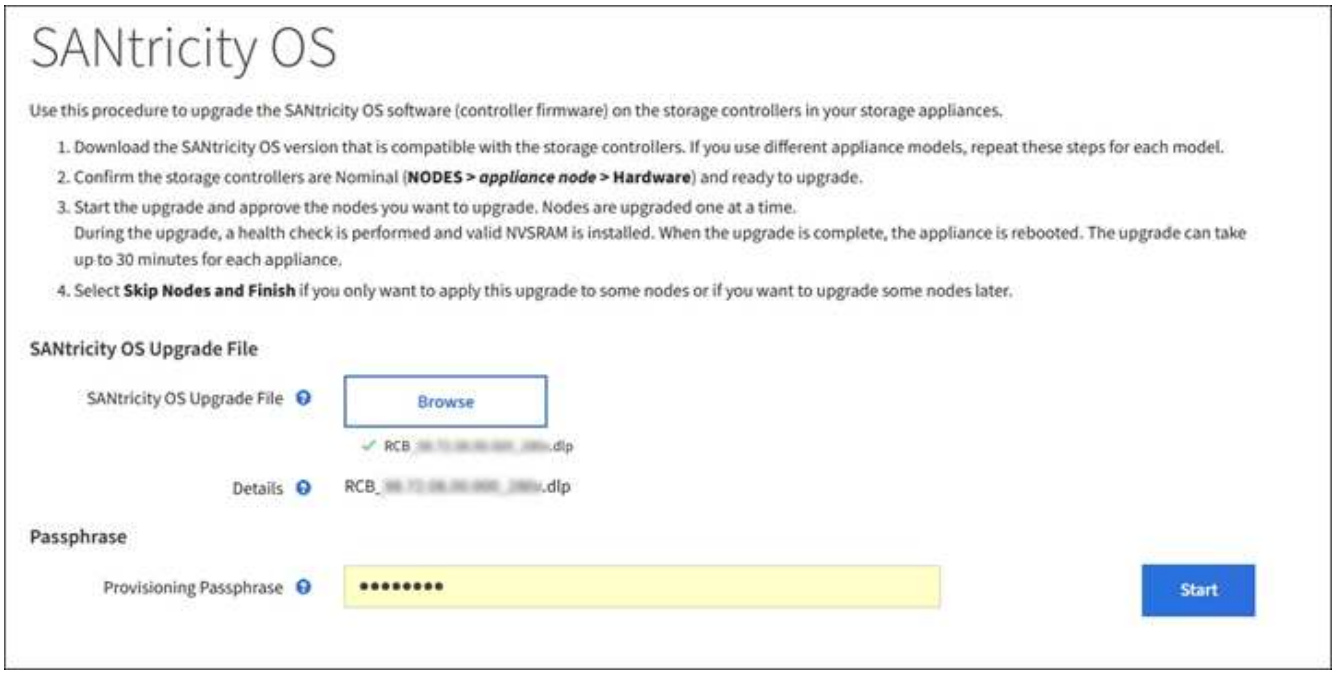
   a. Seleccione **examinar**.
   b. Localice y seleccione el archivo.
   c. Seleccione **Abrir**.

      El archivo se carga y se valida. Cuando se realiza el proceso de validación, se muestra el nombre del archivo junto al botón **examinar**.

      No cambie el nombre del archivo ya que forma parte del proceso de verificación.

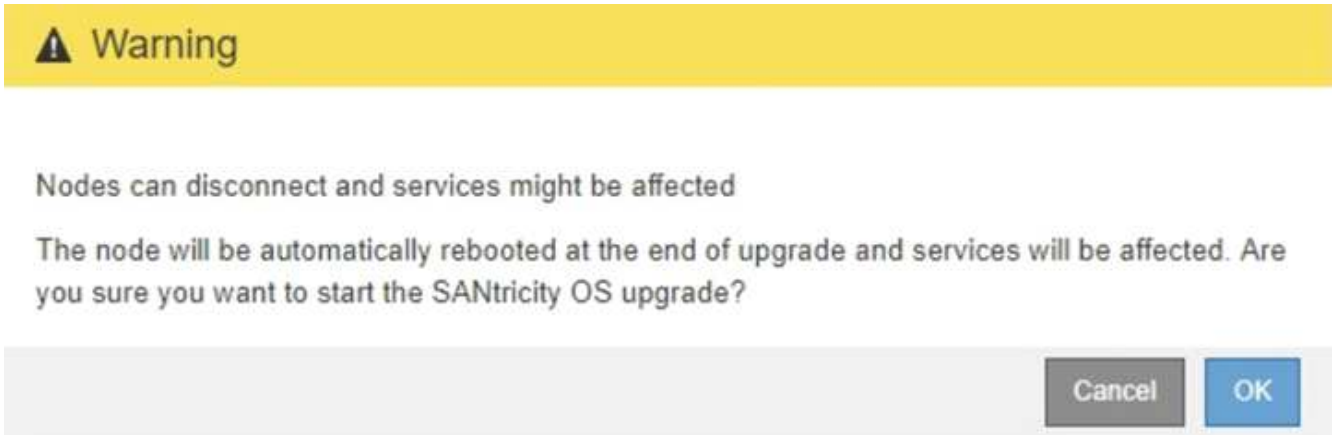
5. Introduzca la clave de acceso de aprovisionamiento.

   El botón **Iniciar** está activado.



6. Seleccione **Iniciar**.

   Aparece un cuadro de advertencia que indica que es posible que se pierda temporalmente la conexión del explorador como se reinician los servicios de los nodos actualizados.



7. Seleccione **Aceptar** para almacenar el archivo de actualización del sistema operativo SANtricity en el nodo de administración principal.

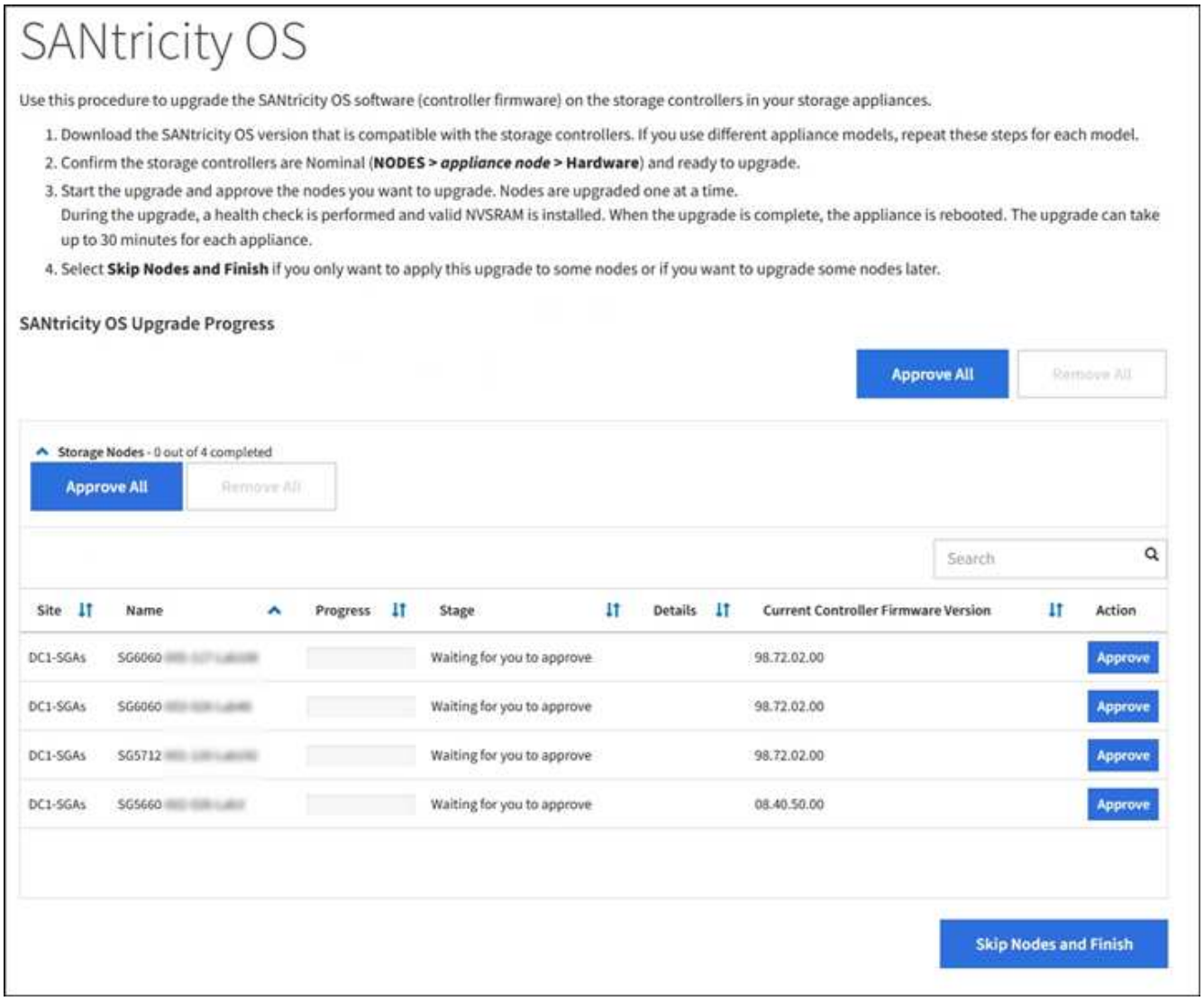
   Cuando se inicia la actualización del sistema operativo SANtricity:

   a. Se ejecuta la comprobación del estado. Este proceso comprueba que ningún nodo tenga el estado de necesita atención.

      Si se informa de algún error, solucione y seleccione **Iniciar** de nuevo.

   b. Se muestra la tabla progreso de actualización de sistema operativo SANtricity. En esta tabla se muestran todos los nodos de almacenamiento del grid y la fase actual de la actualización de cada nodo.

La tabla muestra todos los nodos de almacenamiento del dispositivo. No se muestran los nodos de almacenamiento basados en software. Seleccione **aprobar** para todos los nodos que requieran la actualización.



8. Opcionalmente, ordene la lista de nodos en orden ascendente o descendente por **Sitio**, **Nombre**, **progreso**, **etapa**, **Detalles**, O **Versión actual del firmware de la controladora**. O bien, introduzca un término en el cuadro **Buscar** para buscar nodos específicos.

   Puede desplazarse por la lista de nodos utilizando las flechas izquierda y derecha de la esquina inferior derecha de la sección.

9. Apruebe los nodos de cuadrícula que está listo para agregar a la cola de actualización. Los nodos aprobados del mismo tipo se actualizan de uno en uno.

No apruebe la actualización de SANtricity OS para un nodo de almacenamiento de dispositivos a menos que esté seguro de que el nodo esté listo para detenerse y reiniciar. Cuando la actualización de SANtricity OS se aprueba en un nodo, los servicios de ese nodo se detienen y comienza el proceso de actualización. Más tarde, cuando el nodo finaliza la actualización, el nodo del dispositivo se reinicia. Estas operaciones pueden provocar interrupciones del servicio en los clientes que se comunican con el nodo.

- Seleccione uno de los botones **aprobar todo** para agregar todos los nodos de almacenamiento a la cola de actualización de SANtricity OS.

  > 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 uno o más botones **aprobar** para agregar uno o más nodos a la cola de actualización de SANtricity OS.

  Después de seleccionar **aprobar**, el proceso de actualización determina si se puede actualizar el nodo. Si se puede actualizar un nodo, se agrega a la cola de actualización.

En algunos nodos, el archivo de actualización seleccionado no se aplica de forma intencional, y se puede completar el proceso de actualización sin actualizar estos nodos específicos. Los nodos no actualizados intencionalmente muestran una etapa de completado (intento de actualización) y muestran el motivo por el que el nodo no se actualizó en la columna Details.

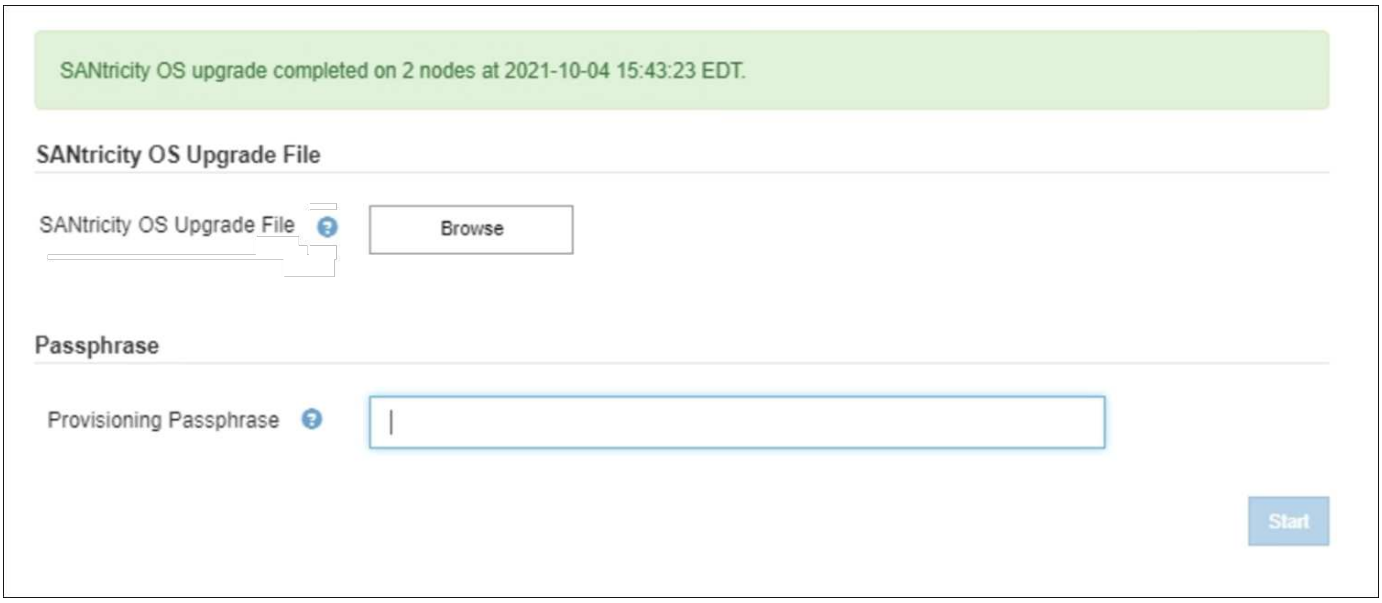
10. Si necesita eliminar un nodo o todos los nodos de la cola de actualización de SANtricity OS, seleccione **Quitar** o **Quitar todo**.

    Cuando la etapa avanza más allá de la cola, el botón **Quitar** está oculto y ya no puede quitar el nodo del proceso de actualización de SANtricity OS.

11. Espere mientras la actualización del SO SANtricity se aplica a cada nodo de grid aprobado.

    - Si alguno de los nodos muestra una etapa de error mientras se aplica la actualización del sistema operativo SANtricity, se produjo un error en la actualización del nodo. Con la ayuda del soporte técnico, es posible que deba colocar el dispositivo en modo de mantenimiento para recuperarlo.
    - Si el firmware del nodo es demasiado antiguo para actualizarse con Grid Manager, el nodo muestra una etapa de error con los detalles: "'debe utilizar el modo de mantenimiento para actualizar SANtricity OS en este nodo. Consulte las instrucciones de instalación y mantenimiento del aparato. Tras la actualización, puede utilizar esta utilidad para futuras actualizaciones». Para resolver el error, haga lo siguiente:
      i. Utilice el modo de mantenimiento para actualizar SANtricity OS en el nodo que muestre una etapa de error.
      ii. Utilice el Administrador de grid para reiniciar y completar la actualización de SANtricity OS.

    Una vez completada la actualización de SANtricity OS en todos los nodos aprobados, la tabla de progreso de la actualización de SANtricity OS se cierra y un banner verde muestra la fecha y la hora en que se completó la actualización de SANtricity OS.



1. Si no se puede actualizar un nodo, tenga en cuenta el motivo que se muestra en la columna Details y realice la acción adecuada:
   - «Ya se ha actualizado el nodo de almacenamiento». No es necesario realizar ninguna otra acción.
   - «'la actualización de SANtricity OS no es aplicable a este nodo». El nodo no tiene una controladora de almacenamiento que pueda gestionar el sistema StorageGRID. Complete el proceso de actualización sin actualizar el nodo que muestra este mensaje.
   - «'el archivo del sistema operativo SANtricity no es compatible con este nodo». El nodo requiere un archivo de SANtricity OS diferente al que seleccionó. Después de completar la actualización actual, descargue el archivo de sistema operativo SANtricity correcto para el nodo y repita el proceso de actualización.

> El proceso de actualización del sistema operativo SANtricity no se completará hasta que apruebe la actualización del sistema operativo SANtricity en todos los nodos de almacenamiento enumerados.

1. Si desea finalizar la aprobación de nodos y volver a la página de SANtricity OS para permitir la carga de un nuevo archivo de SANtricity OS, haga lo siguiente:
   a. Seleccione **Omitir nodos y Finalizar**.

      Aparece una advertencia en la que se pregunta si está seguro de que desea finalizar el proceso de actualización sin actualizar todos los nodos.

   b. Seleccione **Aceptar** para volver a la página **SANtricity OS**.
   c. Cuando esté listo para continuar aprobando nodos, vaya a. Descargue el sistema operativo SANtricity para reiniciar el proceso de actualización.

      > Los nodos ya aprobados y actualizados sin errores siguen actualizando.

2. Repita este procedimiento de actualización para todos los nodos con una etapa de finalización que requieran un archivo de actualización de sistema operativo SANtricity diferente.

   > Para cualquier nodo con el estado necesita atención, utilice el modo de mantenimiento para realizar la actualización.

Cuando repita el procedimiento de actualización, deberá aprobar los nodos actualizados anteriormente.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Actualice el sistema operativo SANtricity en la controladora E2700 mediante modo de mantenimiento

Actualice el sistema operativo SANtricity en la controladora E2700 mediante modo de mantenimiento

Si no puede actualizar el software del sistema operativo SANtricity mediante el administrador de grid, utilice el procedimiento del modo de mantenimiento para aplicar la actualización.

Lo que necesitará

- Ha consultado con la herramienta de matriz de interoperabilidad (IMT) de NetApp para confirmar que la versión del sistema operativo SANtricity que utiliza para la actualización es compatible con su dispositivo.
- Debe colocar la controladora E5600 en modo de mantenimiento Si no está utilizando Grid Manager. Si una controladora se coloca en modo de mantenimiento, se interrumpe la conexión con la controladora E2700.

En raras ocasiones, una vez que se coloca un dispositivo StorageGRID en modo de mantenimiento puede hacer que el dispositivo no esté disponible para el acceso remoto.

Acerca de esta tarea

No actualice el sistema operativo SANtricity ni NVSRAM en la controladora E-Series en más de un dispositivo StorageGRID a la vez.

Actualizar más de un dispositivo StorageGRID a la vez puede provocar la falta de disponibilidad de los datos, según el modelo de puesta en marcha y las políticas de ILM.

Pasos

1. Confirme que el aparato está en modo de mantenimiento.
2. Desde un portátil de servicio, acceda a Storage Manager de SANtricity e inicie sesión.
3. Descargue el nuevo archivo de NVSRAM y de software de sistema operativo SANtricity en el cliente de gestión.

   La NVSRAM es específica del dispositivo StorageGRID. No use la descarga estándar de NVSRAM.

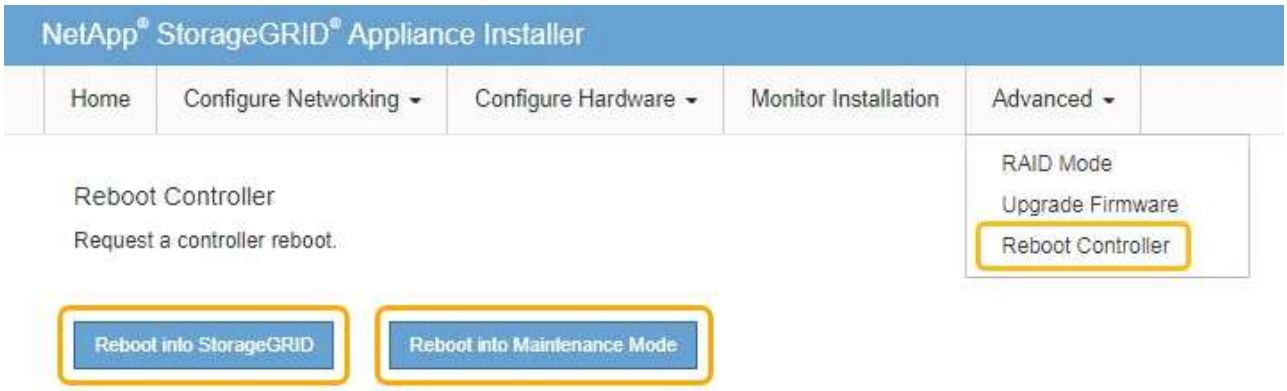
4. Siga las instrucciones de actualización de software y firmware de SANtricity *E2700 y E5600* o de la ayuda en línea de Administrador de almacenamiento de SANtricity, y actualice el firmware de la controladora E2700, NVSRAM o ambos.

   Si necesita actualizar NVSRAM en la controladora E2700, debe confirmar que el archivo del sistema operativo SANtricity que descargó se ha designado como compatible con los dispositivos StorageGRID.

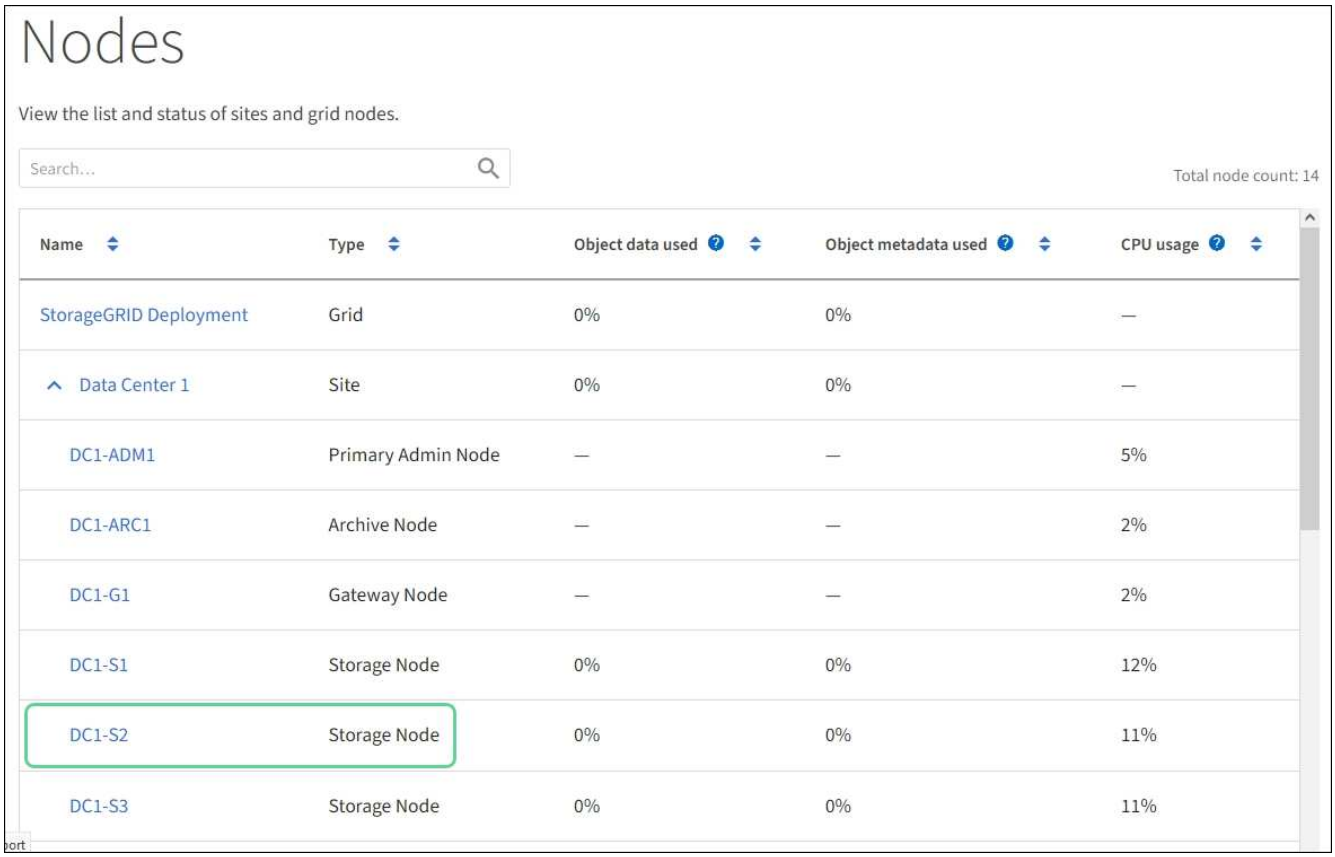
Active los archivos de actualización inmediatamente. No aplace la activación.

5. Si este procedimiento se completó correctamente y tiene procedimientos adicionales que realizar mientras el nodo se encuentra en modo de mantenimiento, realice ahora. Cuando haya terminado, o si ha experimentado algún fallo y desea volver a empezar, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID**
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. Seleccione esta opción si ha experimentado algún error durante el procedimiento y desea volver a empezar. Cuando el nodo termine de reiniciarse en el modo de mantenimiento, reinicie desde el paso adecuado del procedimiento en que falló.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página nodos debe mostrar el estado normal (no hay iconos a la izquierda del nombre del nodo) para el nodo de dispositivo, lo que indica que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Actualizar el firmware de la unidad mediante SANtricity Storage Manager

El firmware de la unidad se actualiza para asegurarse de tener todas las funciones y correcciones de errores más recientes.

Lo que necesitará

- El dispositivo de almacenamiento tiene el estado Optimal.
- Todas las unidades tienen el estado Optimal.
- Tiene instalada la última versión de SANtricity Storage Manager que es compatible con la versión de StorageGRID.

  Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante Grid Manager

  Actualice el sistema operativo SANtricity en la controladora E2700 mediante modo de mantenimiento

- Ya tienes Colocó el dispositivo StorageGRID en modo de mantenimiento.

> El modo de mantenimiento interrumpe la conexión a la controladora de almacenamiento, al detener toda la actividad de I/o y colocar todas las unidades en estado sin conexión.

> No actualice el firmware de la unidad en más de un dispositivo StorageGRID a la vez. Si lo hace, puede provocar la falta de disponibilidad de los datos, según el modelo de puesta en marcha y las políticas de ILM.

Pasos

1. Confirme que el aparato está en modo de mantenimiento.
2. Abra un explorador web y escriba la dirección IP como URL de SANtricity Storage Manager: **`https://E2700_Controller_IP`**
3. Si es necesario, introduzca el nombre de usuario y la contraseña del administrador de SANtricity Storage Manager.
4. En Administración de empresa de SANtricity, seleccione la ficha **dispositivos**.

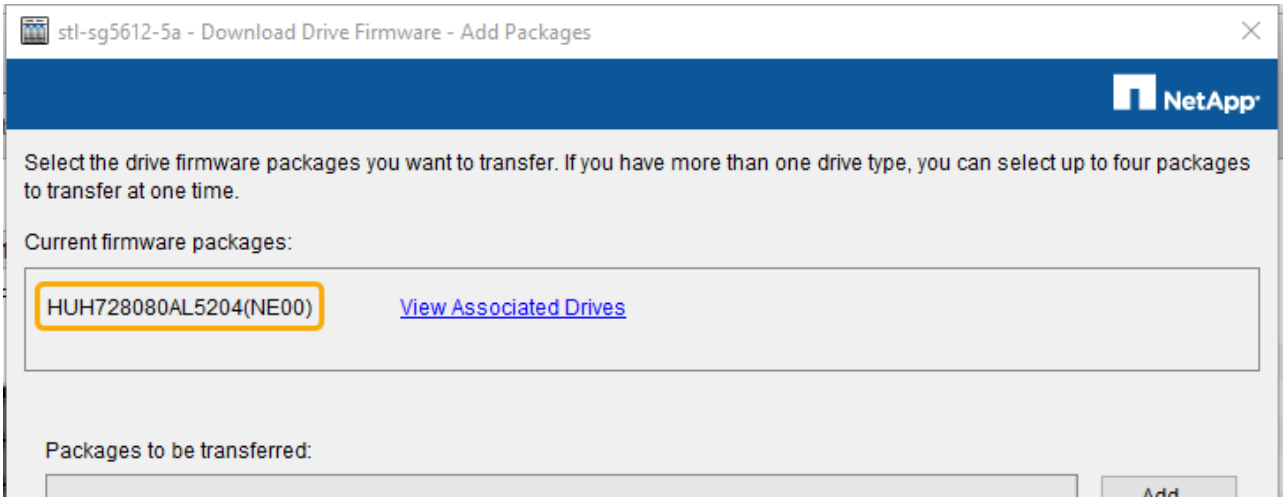
   Se abrirá la ventana Gestión de cabinas SANtricity.

5. En Gestión de cabinas de SANtricity, haga doble clic en la cabina de almacenamiento con las unidades que desea actualizar.
6. Verifique que tanto la cabina de almacenamiento como las unidades tengan el estado Optimal.
7. Compruebe la versión de firmware de la unidad instalada actualmente en el dispositivo de almacenamiento:

   a. En SANtricity Enterprise Management, seleccione **actualización** > **firmware de la unidad**.

      La ventana Descargar firmware de la unidad - Añadir paquetes muestra los archivos de firmware de la unidad que están en uso actualmente.

   b. Tenga en cuenta las revisiones de firmware de la unidad actuales y los identificadores de unidades con los paquetes de firmware actuales.



      En este ejemplo:

      - La revisión del firmware de la unidad es **NE00**.
      - El identificador de la unidad es **HUH7280AL5204**.

   Seleccione **Ver unidades asociadas** para mostrar dónde están instaladas estas unidades en el dispositivo de almacenamiento.

8. Descargue y prepare la actualización del firmware de la unidad disponible:

   a. Abra el explorador web, desplácese hasta el sitio web de soporte de NetApp e inicie sesión con su ID y contraseña.

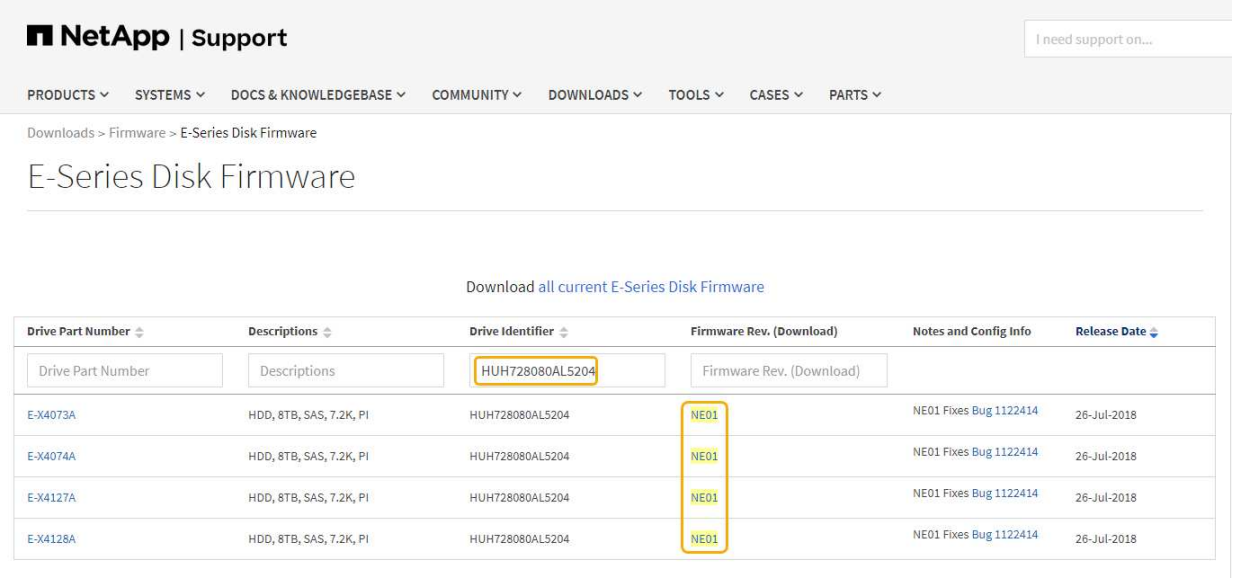
      "Soporte de NetApp"

b. En el sitio de soporte de NetApp, seleccione la pestaña **Descargas** y, a continuación, seleccione **firmware de las unidades de disco E-Series**.

   Se muestra la página firmware del disco E-Series.

c. Busque cada **Identificador de unidad** instalado en el dispositivo de almacenamiento y compruebe que cada identificador de unidad tiene la última revisión de firmware.

   - Si la revisión del firmware no es un enlace, este identificador de unidad tiene la revisión de firmware más reciente.
   - Si se enumeran uno o varios números de pieza de unidad para un identificador de unidad, estas unidades tienen disponible una actualización de firmware. Puede seleccionar cualquier enlace para descargar el archivo de firmware.



d. Si aparece una revisión posterior del firmware, seleccione el enlace en la revisión del firmware (Descargar) para descargar una `.zip` archivo que contiene el archivo de firmware.

e. Extraiga (descomprima) los archivos de almacenamiento del firmware de la unidad que descargó del sitio de soporte.

9. Instale la actualización del firmware de la unidad:

   a. En la ventana Descargar firmware de la unidad de SANtricity Storage Manager - Agregar paquetes, seleccione **Agregar**.

   b. Desplácese hasta el directorio que contiene los archivos de firmware y seleccione hasta cuatro archivos de firmware.

      Los archivos de firmware de la unidad tienen un nombre de archivo similar a `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`

      Si se selecciona más de un archivo de firmware para actualizar el firmware de la misma unidad, se puede producir un error de conflicto de archivo. Si se produce un error de conflicto de archivo, aparece un cuadro de diálogo de error. Para resolver este error, seleccione **Aceptar** y elimine todos los demás archivos de firmware excepto el que desee utilizar para actualizar el firmware de la unidad. Para eliminar un archivo de firmware, seleccione el archivo de firmware en el área de información Paquetes a transferir y seleccione **Quitar**. Además, solo es posible seleccionar hasta cuatro paquetes de firmware de la unidad a la vez.

c. Seleccione **OK**.

   El sistema actualiza el área de información Paquetes a transferir con los archivos de firmware seleccionados.

d. Seleccione **Siguiente**.

   Se abre la ventana Descargar firmware de la unidad: Seleccionar unidades.

   - Se analizan todas las unidades del dispositivo para obtener información sobre la configuración y poder actualizar.
   - Se presenta con una selección (según la variedad de unidades de la cabina de almacenamiento) de unidades compatibles que se pueden actualizar con el firmware seleccionado. De manera predeterminada, se muestran las unidades que pueden actualizarse como una operación en línea.
   - El firmware seleccionado para la unidad aparece en el área de información firmware propuesto. Si debe cambiar el firmware, seleccione **Atrás** para volver al cuadro de diálogo anterior.

e. En la capacidad de actualización de la unidad, seleccione la operación de descarga **paralelo** o **todo**.

   Es posible usar cualquiera de estos métodos de actualización porque el dispositivo está en modo de mantenimiento, donde se detiene la actividad de I/o de todas las unidades y todos los volúmenes.

f. En unidades compatibles, seleccione las unidades para las que desea actualizar los archivos de firmware seleccionados.

   - Para una o varias unidades, seleccione cada unidad que desee actualizar.
   - Para todas las unidades compatibles, seleccione **Seleccionar todo**.

     La práctica recomendada es actualizar todas las unidades del mismo modelo a la misma revisión de firmware.

g. Seleccione **Finalizar**; a continuación, escriba `yes` Y seleccione **OK**.

   - Comienza la descarga y la actualización del firmware de la unidad, con Download firmware de la unidad: Progreso que indica el estado de la transferencia del firmware en todas las unidades.
   - El estado de cada unidad que participa en la actualización aparece en la columna progreso de transferencia de dispositivos actualizados.

     Una operación de actualización del firmware de una unidad paralela puede tardar hasta 90 segundos en completarse si todas las unidades se actualizan en un sistema de 24 unidades. En un sistema más grande, el tiempo de ejecución es ligeramente más largo.

h. Durante el proceso de actualización del firmware, puede: +

   - Seleccione **Detener** para detener la actualización del firmware en curso. Se completa cualquier actualización de firmware actualmente en curso. Cualquier unidad que haya intentado actualizar el firmware muestra su estado individual. Las unidades restantes se enumeran con el estado no se intenta.

     > Si se detiene la actualización del firmware de la unidad en el proceso, podrían producirse la pérdida de datos o la falta de disponibilidad de las unidades.

   - Seleccione **Guardar como** para guardar un informe de texto del resumen de progreso de la actualización del firmware. El informe se guarda con una extensión de archivo .log predeterminada. Si desea cambiar la extensión o el directorio, cambie los parámetros en Guardar

registro de descarga de unidad.

i. Utilice Descargar firmware de la unidad: Progreso para supervisar el progreso de las actualizaciones del firmware de la unidad. El área Drives Updated contiene una lista de unidades programadas para la actualización de firmware y el estado de transferencia de cada unidad que se descarga y actualización.

   El progreso y el estado de cada unidad que está participando en la actualización se muestran en la columna progreso de la transferencia. Realice la acción recomendada si se producen errores durante la actualización.

   - **Pendiente**

     Este estado se muestra para una operación de descarga de firmware en línea programada, pero aún no se inició.

   - **En curso**

     El firmware se está transfiriendo a la unidad.

   - **Reconstrucción en curso**

     Este estado se muestra si tiene lugar una transferencia de volumen durante la reconstrucción rápida de una unidad. Por lo general, esto se debe a un restablecimiento o un fallo de la controladora y el propietario de la controladora transfiere el volumen.

El sistema iniciará una reconstrucción completa de la unidad.

- **Fallo - parcial**

  El firmware solo se transfirió parcialmente a la unidad antes de que un problema impidió que se transfiriera el resto del archivo.

- **Error: Estado no válido**

  El firmware no es válido.

- **Error - otro**

  No se pudo descargar el firmware, posiblemente debido a un problema físico con la unidad.

- **No se ha intentado**

  El firmware no se descargó, lo que puede deberse a diversos motivos diferentes, como la descarga se detuvo antes de que pudiera producirse, o la unidad no cumple los requisitos para la actualización. O la descarga no pudo ocurrir debido a un error.

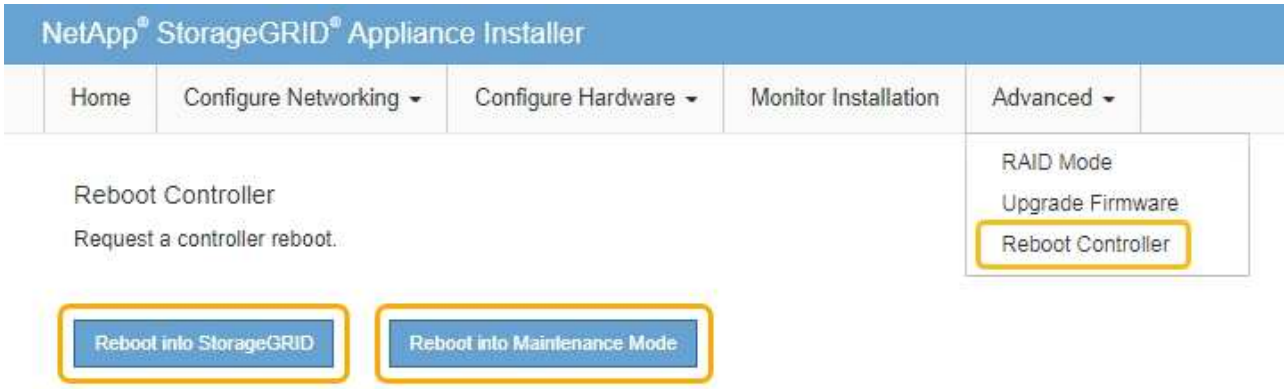
- **Correcto**

  El firmware se ha descargado correctamente.

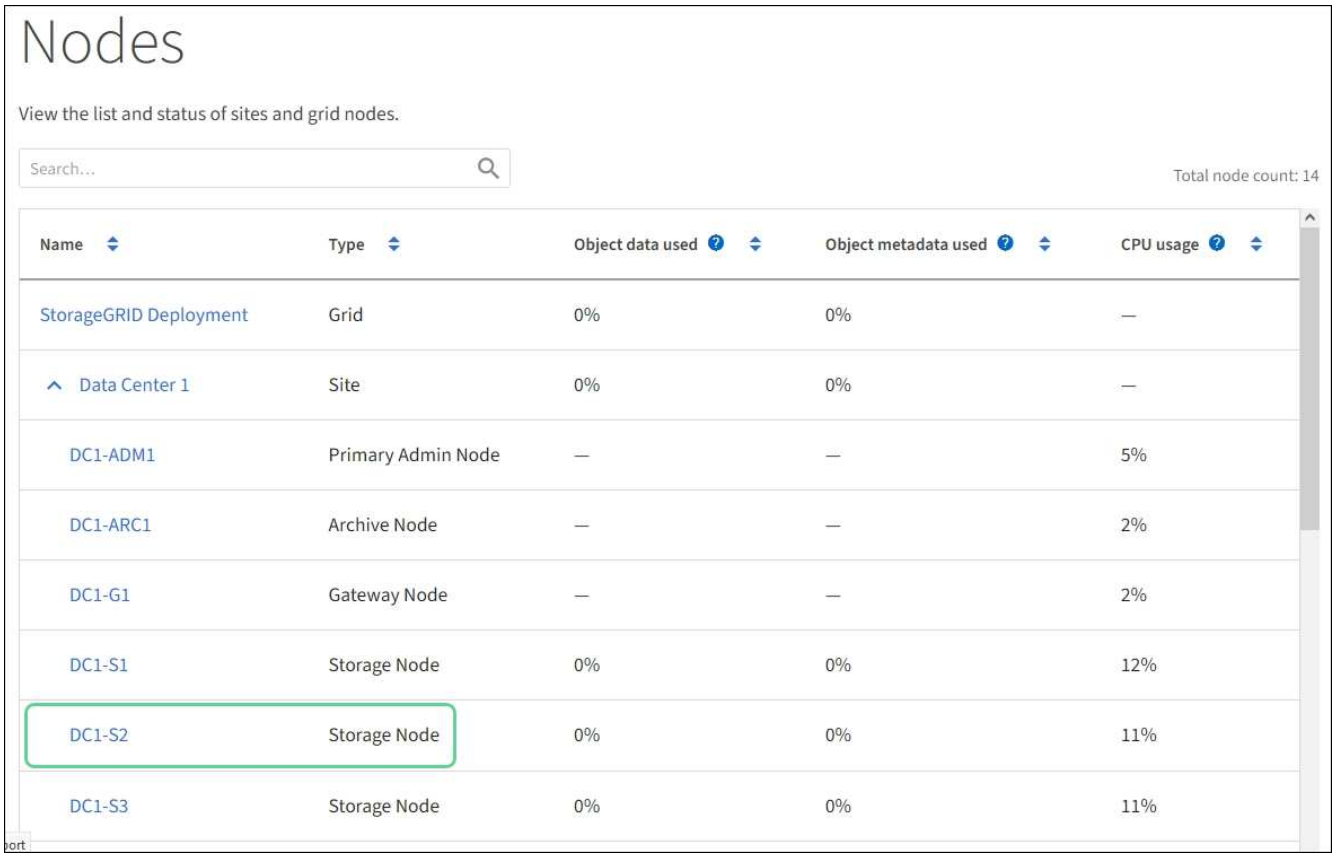
10. Una vez completada la actualización del firmware de la unidad:
    - Para cerrar el Asistente para descargar firmware de la unidad, seleccione **Cerrar**.
    - Para volver a iniciar el asistente, seleccione **transferir más**.
11. Si este procedimiento se completó correctamente y tiene procedimientos adicionales que realizar mientras

el nodo se encuentra en modo de mantenimiento, realice ahora. Cuando haya terminado, o si ha experimentado algún fallo y desea volver a empezar, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

- Seleccione **Reiniciar en StorageGRID**
- Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. Seleccione esta opción si ha experimentado algún error durante el procedimiento y desea volver a empezar. Cuando el nodo termine de reiniciarse en el modo de mantenimiento, reinicie desde el paso adecuado del procedimiento en que falló.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **Nodes** debe mostrar un estado normal (no hay iconos a la izquierda del nombre del nodo) para el nodo del dispositivo, lo que indica que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Sustituya la controladora E2700

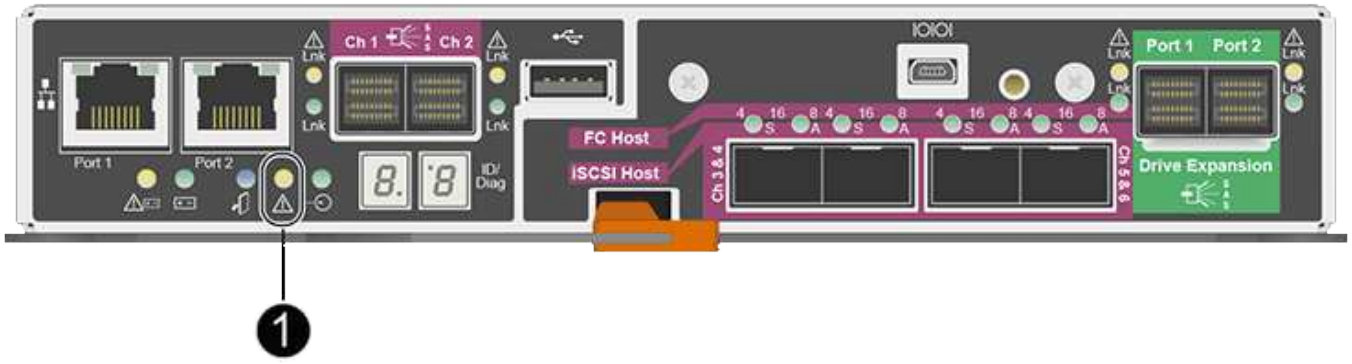
Tal vez deba sustituir la controladora E2700 si no funciona de forma óptima o ha fallado.

Lo que necesitará

- Tiene una controladora de sustitución con el mismo número de pieza que la controladora que desea sustituir.
- Tiene etiquetas para identificar cada cable conectado a la controladora.
- Tiene protección antiestática.
- Debe tener los permisos de mantenimiento o acceso raíz. Para obtener más detalles, consulte las instrucciones para administrar StorageGRID.

Acerca de esta tarea

Puede determinar si tiene un controlador que ha fallado comprobando el LED ámbar de acción de servicio requerida en el controlador (se muestra como 1 en la ilustración). Si este LED está encendido, se debe sustituir el controlador.



No se podrá acceder al nodo de almacenamiento del dispositivo cuando se sustituye la controladora. Si la controladora E2700 funciona lo suficiente, puede colocar la controladora E5600SG en modo de mantenimiento.

Al sustituir una controladora, debe quitar la batería de la controladora original e instalarla en la controladora de reemplazo.

Pasos

1. Prepárese para quitar el controlador.

   El administrador del almacenamiento de SANtricity se utiliza para realizar estos pasos.

   a. Anote en qué versión del software de sistema operativo SANtricity está instalada actualmente en la controladora.

   b. Anote en qué versión de NVSRAM está instalada actualmente.

   c. Si la función Drive Security está habilitada, asegúrese de que existe una clave guardada y de que conoce la frase de contraseña necesaria para instalarla.

   > **Posible pérdida de acceso a datos y#8212;** Si todas las unidades del dispositivo tienen la seguridad habilitada, el nuevo controlador no podrá acceder al dispositivo hasta que desbloquee las unidades seguras mediante la ventana de administración empresarial de SANtricity Storage Manager.

   d. Realice un backup de la base de datos de configuración.

      Si se produce un problema al quitar una controladora, puede usar el archivo guardado para restaurar la configuración.

   e. Recopile datos de soporte del dispositivo.

   > La recogida de datos de soporte antes y después de reemplazar un componente garantiza que se pueda enviar un conjunto completo de registros al soporte técnico en caso de que el reemplazo no resuelva el problema.

2. Si el dispositivo StorageGRID se ejecuta en un sistema StorageGRID, Coloque la controladora E5600SG en modo de mantenimiento.

3. Si la controladora E2700 funciona lo suficiente para permitir un apagado controlado, confirme que todas las operaciones se han completado.

a. En la barra de título de Array Management Window, seleccione **Monitor** > **Informes** > **Operaciones en curso**.

b. Confirmar que se han completado todas las operaciones.

4. Siga las instrucciones del procedimiento de sustitución para una controladora E2700 simple a fin de completar los siguientes pasos:

   a. Etiquete los cables y desconecte los cables.

   > Para evitar un rendimiento degradado, no gire, pliegue, pellizque ni pellizque los cables.

   b. Retire el controlador que ha fallado del dispositivo.

   c. Retire la cubierta del controlador.

   d. Desenrosque el tornillo de ajuste manual y retire la batería del controlador que ha fallado.

   e. Instale la batería en el controlador de repuesto y vuelva a colocar la cubierta del controlador.

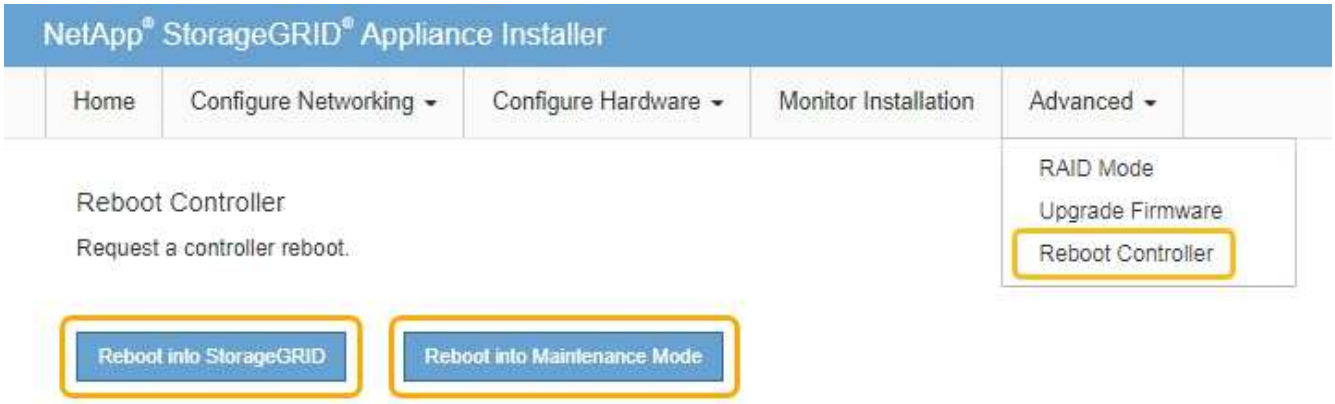
   f. Instale el controlador de repuesto en el aparato.

   g. Sustituya los cables.

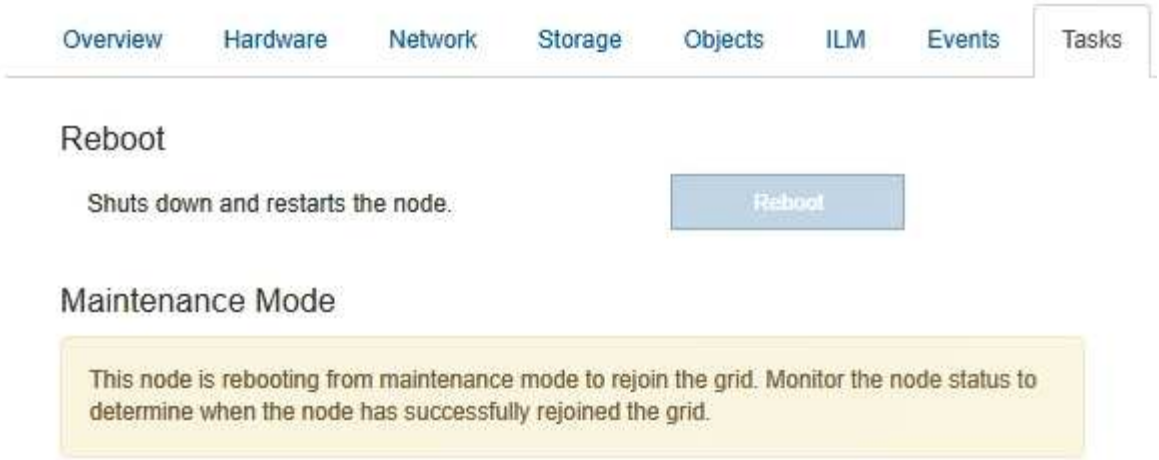
   h. Espere a que se reinicie la controladora E2700. Compruebe que la pantalla de siete segmentos muestra el estado de `99`.

5. Si el dispositivo utiliza unidades seguras, importe la clave de seguridad de la unidad.

6. Vuelva a poner el aparato en modo de funcionamiento normal. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione **Reiniciar en StorageGRID**.

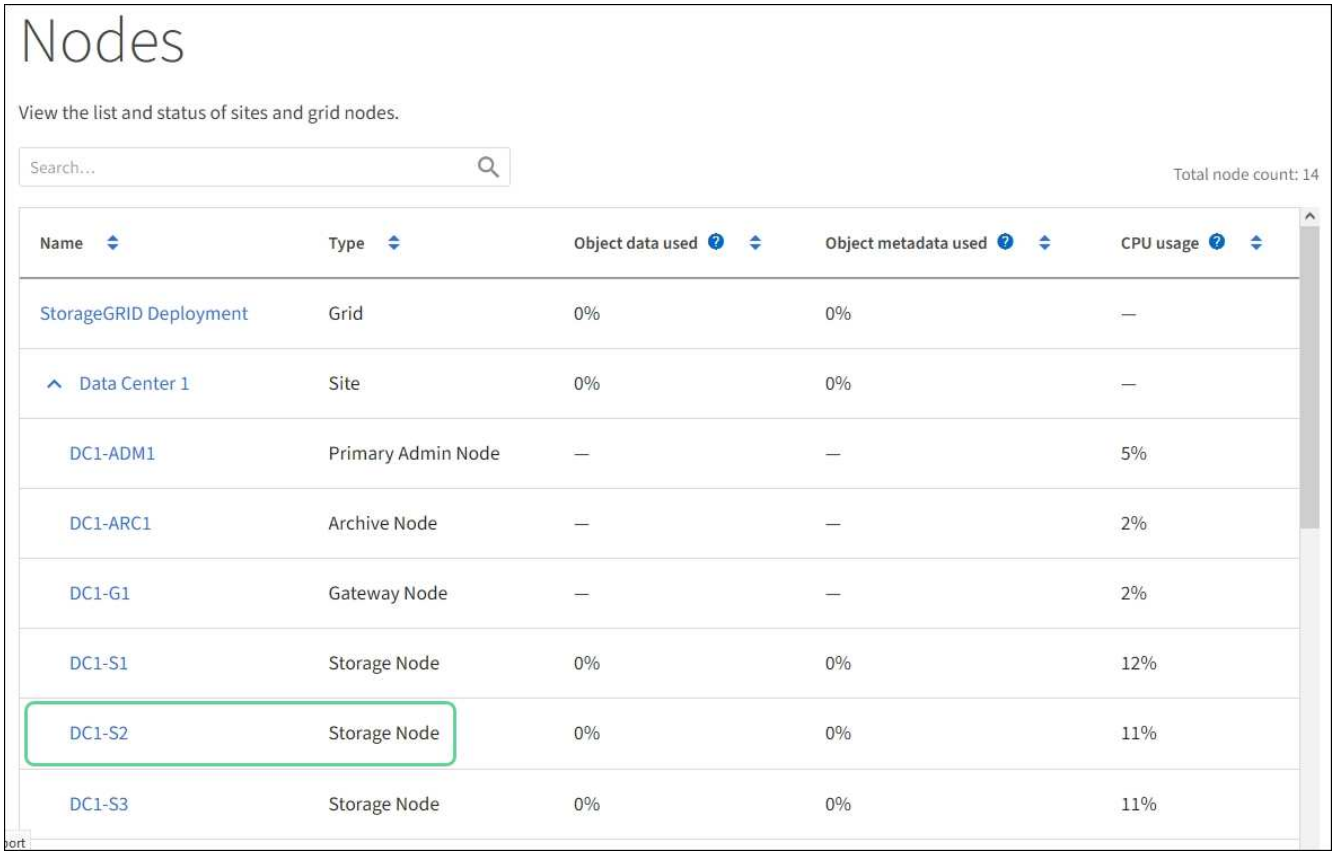


Durante el reinicio, aparece la siguiente pantalla:



El dispositivo se reinicia y vuelve a unir la cuadrícula. Este proceso puede llevar hasta 20 minutos.

7. Confirme que el reinicio ha finalizado y que el nodo se ha vuelto a unir a la cuadrícula. En Grid Manager, compruebe que la página Nodes muestra un estado normal (sin iconos a la izquierda del nombre del nodo) del nodo de dispositivo, lo que indica que no hay alertas activas y que el nodo está conectado a la cuadrícula.



8. En SANtricity Storage Manager, confirme que el estado de la nueva controladora es óptimo y recoja datos de soporte.

Información relacionada

"Procedimientos para reemplazar hardware E-Series y EF-Series de NetApp"

"Documentación de NetApp: Serie E2700"

Sustituya la controladora E5600SG

Es posible que deba sustituir la controladora E5600SG.

Lo que necesitará

Debe tener acceso a los siguientes recursos:

- Información para la sustitución del hardware E-Series en el sitio de soporte de NetApp en +http://mysupport.netapp.com/["mysupport.netapp.com"^]
- Documentación de E5600 en el sitio de soporte
- El aparato se ha estado se colocó en modo de mantenimiento.

Acerca de esta tarea

Si ambas controladoras funcionan lo suficiente como para permitir un apagado controlado, puede apagar la controladora E5600SG primero para interrumpir la conectividad con la controladora E2700.

> Si va a sustituir la controladora antes de instalar el software StorageGRID, es posible que no pueda acceder al instalador de dispositivos de StorageGRID inmediatamente después de completar este procedimiento. Aunque puede acceder al instalador del dispositivo StorageGRID desde otros hosts de la misma subred que el dispositivo, no puede acceder al mismo desde hosts de otras subredes. Esta condición debe resolverse dentro de los 15 minutos (cuando se agota cualquier entrada de caché ARP para el tiempo de espera original de la controladora); asimismo, puede borrar la condición de inmediato mediante la purga manual de todas las entradas antiguas de la caché ARP desde el enrutador o la puerta de enlace local.

Pasos

1. Use protección antiestática.
2. Etiquete cada cable conectado a la controladora E5600SG, de modo que pueda volver a conectar los cables correctamente.

   > Para evitar un rendimiento degradado, no gire, pliegue, pellizque ni pellizque los cables. No doble los cables más apretados que un radio de 5 cm (2 pulg).

3. Una vez colocado el dispositivo en modo de mantenimiento, apague el controlador E5600SG.
   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. Apague el controlador E5600SG:
      `shutdown -h now`
4. Apague el compartimento y espere a que se hayan detenido todos los LED y la actividad de visualización de siete segmentos de la parte posterior del controlador.

5. Quite los cables.
6. Quite la controladora, como se describe en la documentación de la controladora E5600SG.
7. Inserte la nueva controladora, como se describe en la documentación de la controladora E5600SG.
8. Sustituya todos los cables.
9. Vuelva a encender el compartimento.
10. Supervise los códigos de siete segmentos.
    - Controladora E2700:

      El estado del LED final es `99`.

    - Controladora E5600SG:

      El estado del LED final es `HA`.

11. Supervise el estado del nodo de almacenamiento del dispositivo en Grid Manager.

    Compruebe que los nodos de almacenamiento del dispositivo vuelven al estado esperado.

Información relacionada

"Procedimientos para reemplazar hardware E-Series y EF-Series de NetApp"

"Documentación de NetApp: Serie E5600"

Sustituir otros componentes de hardware

Es posible que deba sustituir una unidad, un ventilador, una fuente de alimentación o una batería en el dispositivo StorageGRID.

Lo que necesitará

- Tiene el procedimiento de sustitución del hardware E-Series.
- El aparato se ha estado se pone en modo de mantenimiento si el procedimiento de sustitución de componentes requiere que apague el aparato.

Acerca de esta tarea

Para sustituir una unidad, un contenedor de alimentación/ventilador, un contenedor de ventilador, un contenedor de alimentación, una batería, O el cajón de unidades, consulte los procedimientos estándar de las cabinas de almacenamiento E2700 y E5600. Céntrese en las instrucciones paso a paso para extraer y sustituir el hardware en sí; muchos de los procedimientos de Administrador de almacenamiento de SANtricity no se aplican a un dispositivo.

Instrucciones de sustitución de componentes de SG5612

FRU	Consulte
Unidad	Siga los pasos de las instrucciones E-Series para reemplazar una unidad en los soportes de 12 o 24 unidades E2600, E2700, E5400, E5500, E5600.

FRU	Consulte
Contenedor de alimentación/ventilador	Siga los pasos de las instrucciones de E-Series para reemplazar una batería de alimentación/ventilador con error en el soporte de controladoras E5612 o E5624
Batería en la controladora E2700 (requiere la extracción de la controladora)	Siga los pasos de Sustituya la controladora E2700, pero instale la batería nueva en el controlador existente.

Instrucciones para la sustitución de componentes SG5660

FRU	Consulte
Unidad	Siga los pasos de las instrucciones E-Series para reemplazar una unidad en las bandejas E2660, E2760, E5460, E5560 o E5660.
Contenedor de alimentación	Siga los pasos de las instrucciones de E-Series para reemplazar un contenedor de alimentación con error en el soporte de controladoras E5660
Contenedor de ventilador	Siga los pasos de las instrucciones de E-Series para reemplazar un contenedor de ventilador con error en el soporte de controladoras E5660
Batería en la controladora E2700 (requiere la extracción de la controladora)	Siga los pasos de Sustituya la controladora E2700, pero instale la batería nueva en el controlador existente.

Información relacionada

"Procedimientos para reemplazar hardware E-Series y EF-Series de NetApp"

"Documentación de NetApp: Serie E2700"

"Documentación de NetApp: Serie E5600"

Cambiar la configuración de los enlaces de la controladora E5600SG

Es posible cambiar la configuración del enlace Ethernet de la controladora E5600SG. Puede cambiar el modo de enlace de puerto, el modo de enlace de red y la velocidad del enlace.

Lo que necesitará

Coloque la controladora E5600SG en modo de mantenimiento.

> En raras ocasiones, una vez que se coloca un dispositivo StorageGRID en modo de mantenimiento puede hacer que el dispositivo no esté disponible para el acceso remoto.

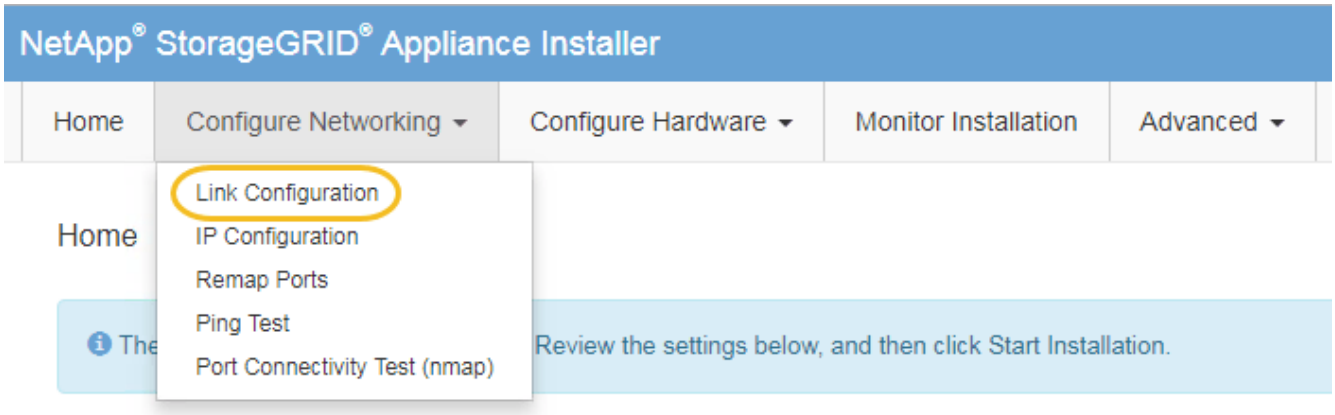
Acerca de esta tarea

Entre las opciones para cambiar la configuración del enlace Ethernet de la controladora E5600SG se incluyen:

- Cambiando **modo de enlace de puerto** de fijo a agregado, o de agregado a fijo
- Cambio del **modo de enlace de red** de Active-Backup a LACP o de LACP a Active-Backup
- Habilitar o deshabilitar el etiquetado de VLAN, o cambiar el valor de una etiqueta de VLAN
- Cambio de la velocidad de enlace de 10-GbE a 25-GbE, o de 25-GbE a 10-GbE

Pasos

1. Seleccione **Configurar red** > **Configuración de enlace** en el menú.



2. realice los cambios deseados en la configuración del enlace.

   Para obtener más información sobre las opciones, consulte «"Configuración de enlaces de red".

3. Cuando esté satisfecho con sus selecciones, haga clic en **Guardar**.

   > Puede perder la conexión si ha realizado cambios en la red o el enlace que está conectado a través de. Si no vuelve a conectarse en un minuto, vuelva a introducir la URL del instalador de dispositivos StorageGRID utilizando una de las otras direcciones IP asignadas al dispositivo:
   > **`https://E5600SG_Controller_IP:8443`**

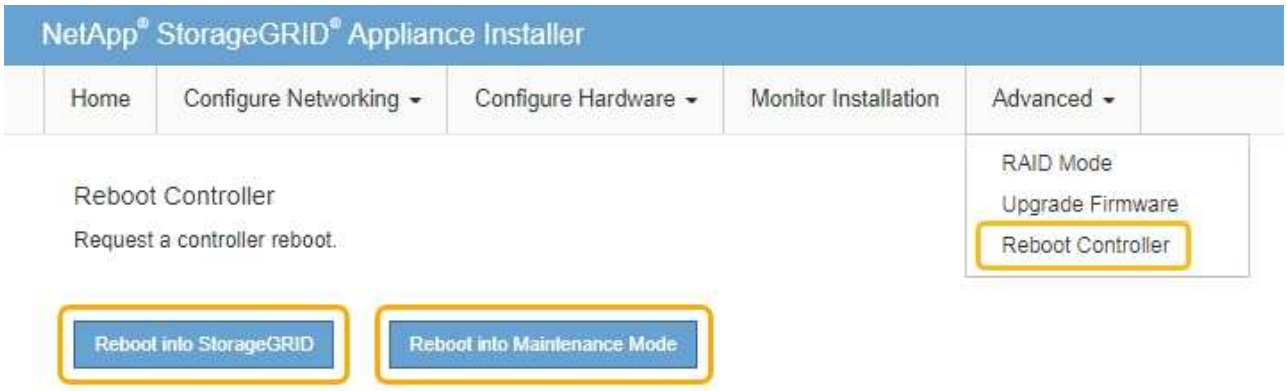
   Si ha realizado cambios en la configuración de VLAN, es posible que la subred del dispositivo haya cambiado. Si necesita cambiar las direcciones IP del dispositivo, siga el Establezca la configuración de IP instrucciones.

4. En el instalador del dispositivo StorageGRID, seleccione **Configurar redes** > **Prueba de ping**.
5. Utilice la herramienta Ping Test para comprobar la conectividad a las direcciones IP en cualquier red que pueda haber sido afectada por los cambios de configuración de vínculos realizados en Cambiar la configuración del enlace paso.

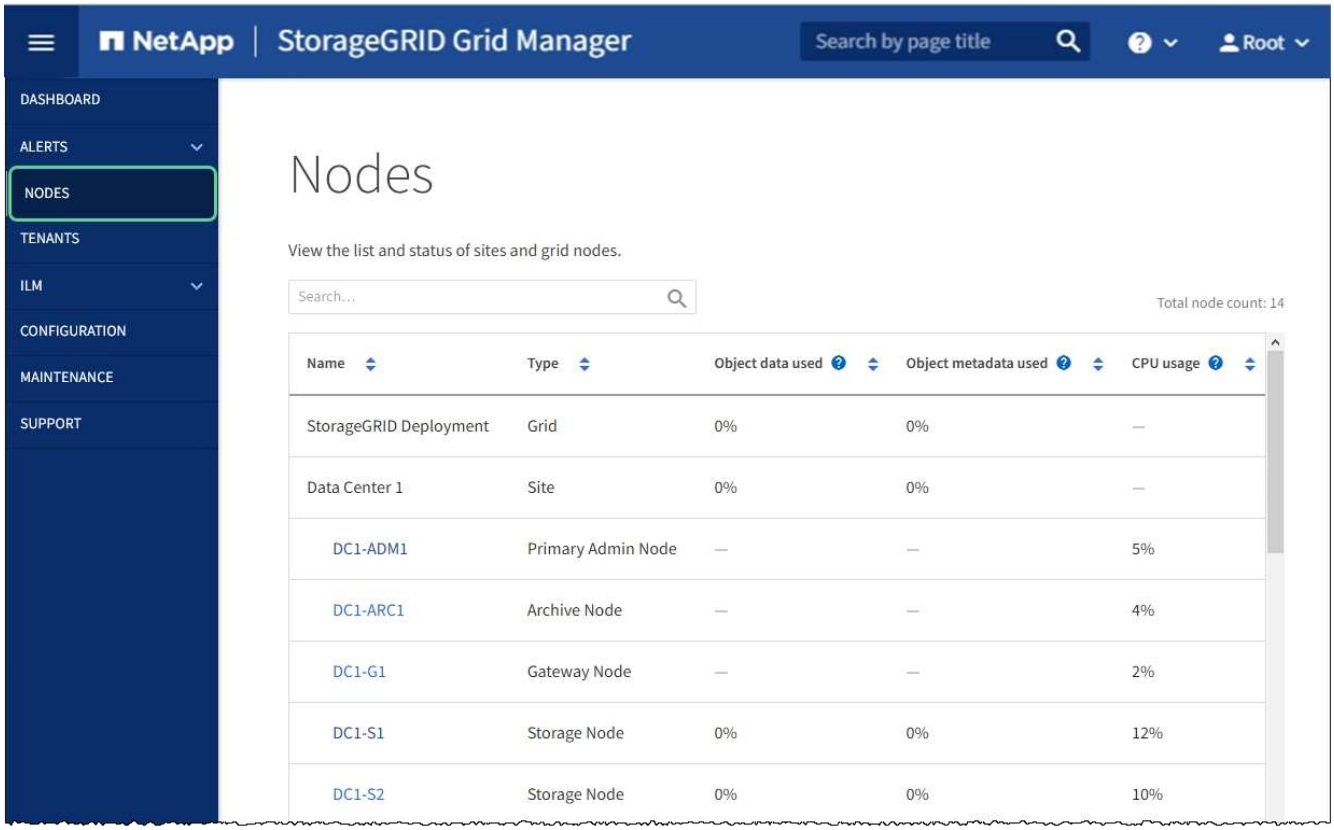
   Además de todas las pruebas que elija realizar, confirme que puede hacer ping a la dirección IP de grid del nodo de administración principal y a la dirección IP de grid del al menos otro nodo de almacenamiento. Si es necesario, corrija los problemas de configuración de los enlaces.

6. Una vez que esté satisfecho de que los cambios en la configuración del enlace funcionan, reinicie el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

- Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
- Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Configurar enlaces de red (SG5600)

Cambie la configuración de MTU

Puede cambiar la configuración de MTU que asigne al configurar las direcciones IP para el nodo del dispositivo.

Acerca de esta tarea

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. Los valores de MTU no tienen que ser iguales para todos los tipos de red.

Para cambiar la configuración de MTU sin reiniciar el nodo del dispositivo, Utilice la herramienta Cambiar IP.

Si la red de cliente o administrador no se configuró en el instalador de dispositivos de StorageGRID durante la instalación inicial, Cambie la configuración de MTU con el modo de mantenimiento.

Cambie la configuración de MTU mediante la herramienta Cambiar IP

Lo que necesitará

Usted tiene la `Passwords.txt` Archivo para utilizar la herramienta Cambiar IP.

Pasos

Acceda a la herramienta Cambiar IP y actualice la configuración de MTU como se describe en Cambie la configuración de red de los nodos.

Cambie la configuración de MTU con el modo de mantenimiento

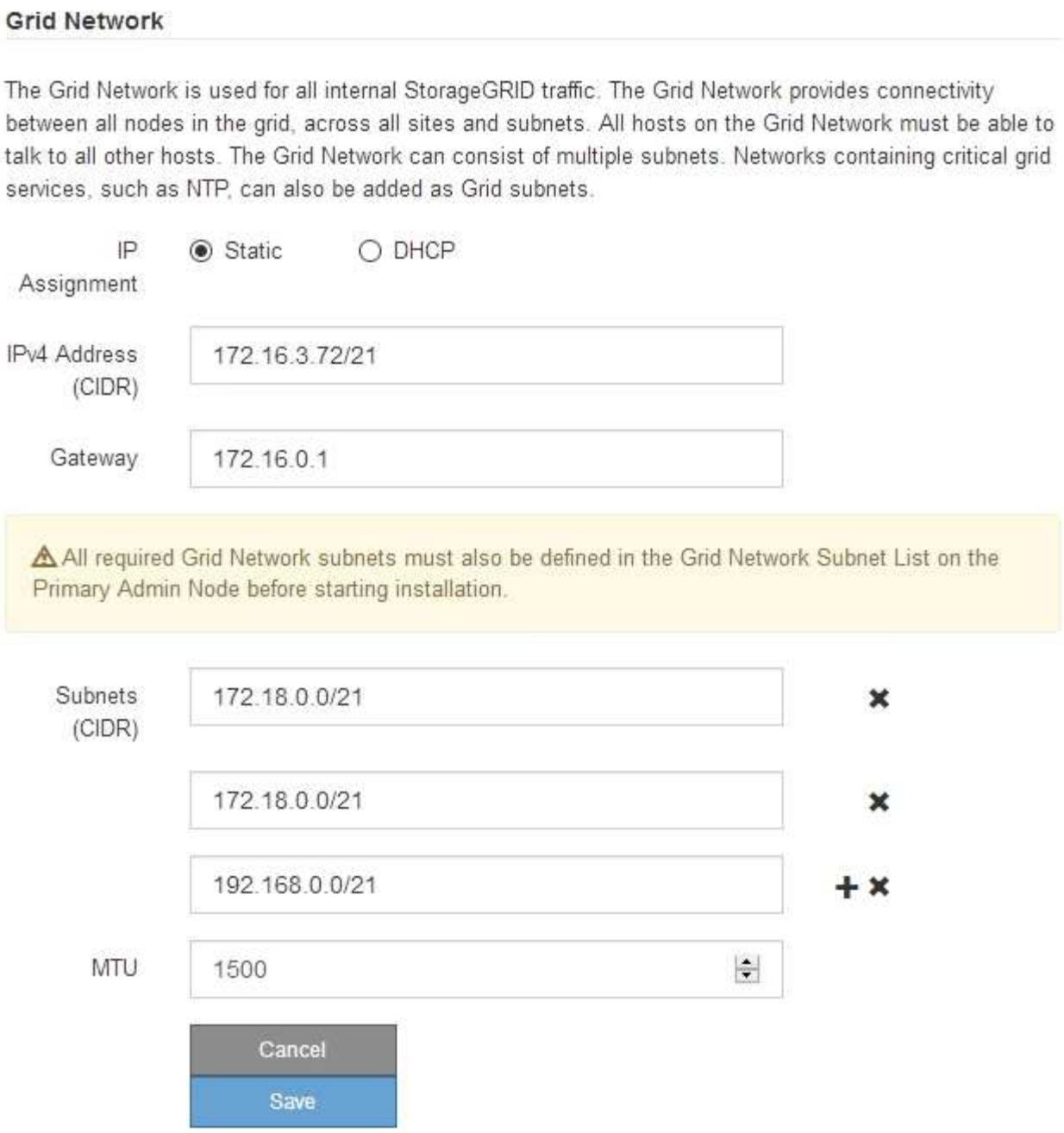
Cambie la configuración de MTU mediante el modo de mantenimiento si no puede acceder a estas opciones con la herramienta Cambiar IP.

Lo que necesitará

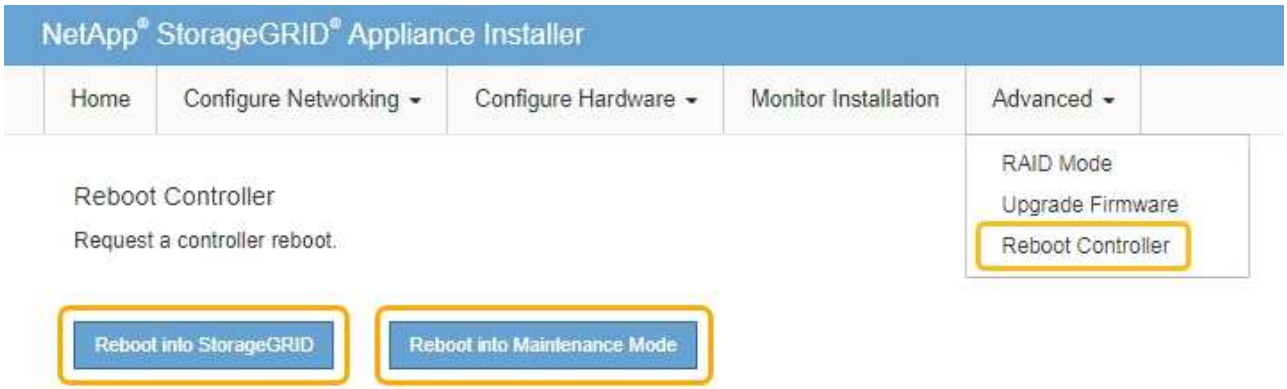
El aparato se ha estado se colocó en modo de mantenimiento.

Pasos

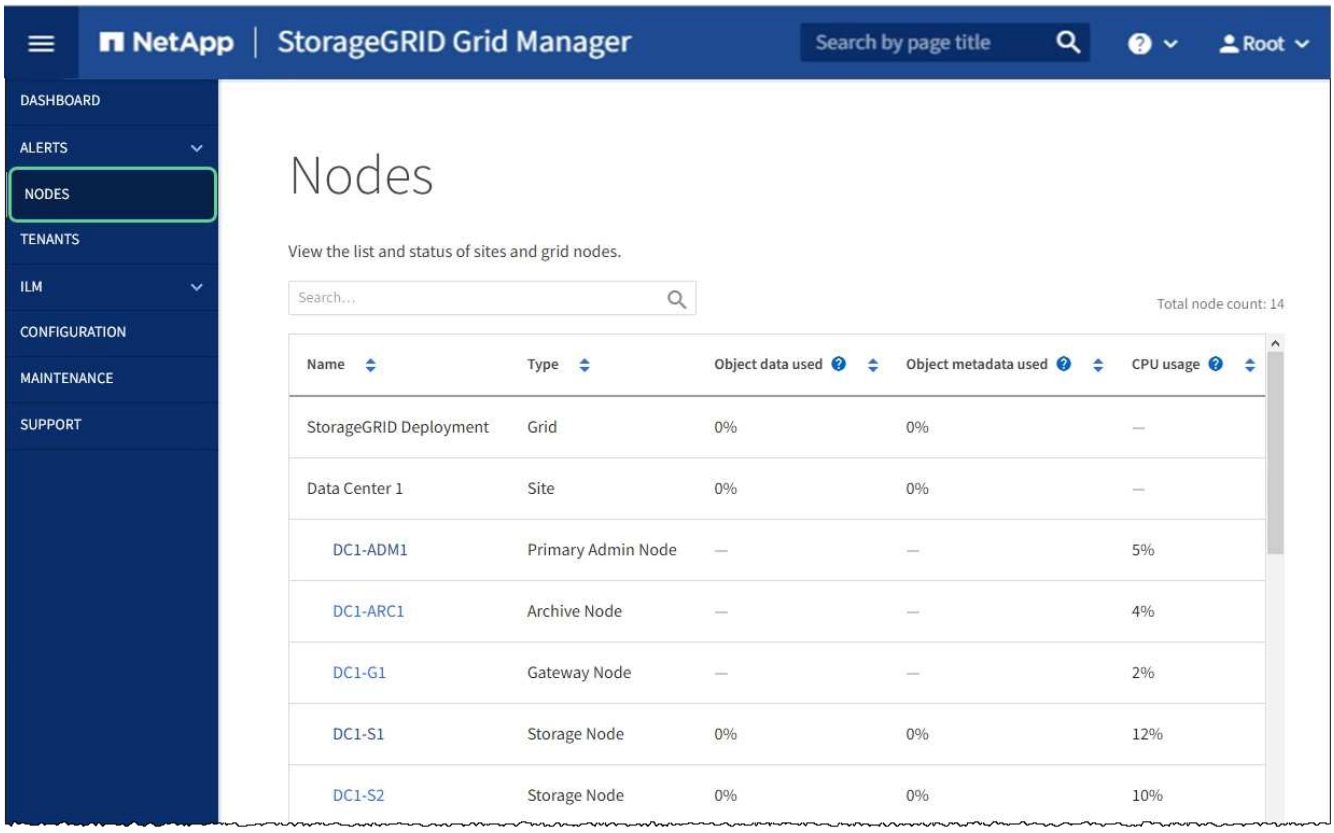
1. En el instalador del dispositivo StorageGRID, seleccione **Configurar redes** > **Configuración IP**.
2. Realice los cambios deseados en la configuración de MTU para la red de grid, la red de administración y la red de cliente.



3. Cuando esté satisfecho con los ajustes, seleccione **Guardar**.
4. Reiniciar el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:
   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Administre StorageGRID

Comprobar la configuración del servidor DNS

Puede comprobar y cambiar temporalmente los servidores del sistema de nombres de dominio (DNS) que está utilizando actualmente este nodo de dispositivo.

Lo que necesitará

El aparato se ha estado se colocó en modo de mantenimiento.

Acerca de esta tarea

Es posible que deba cambiar la configuración del servidor DNS si un dispositivo cifrado no puede conectarse con el servidor de gestión de claves (KMS) o un clúster KMS porque el nombre de host del KMS se especificó como un nombre de dominio en lugar de una dirección IP. Cualquier cambio realizado en la configuración de DNS del dispositivo es temporal y se pierde al salir del modo de mantenimiento. Para que estos cambios sean permanentes, especifique los servidores DNS en Grid Manager (**MAINTENANCE** > **Network** > **servidores DNS**).

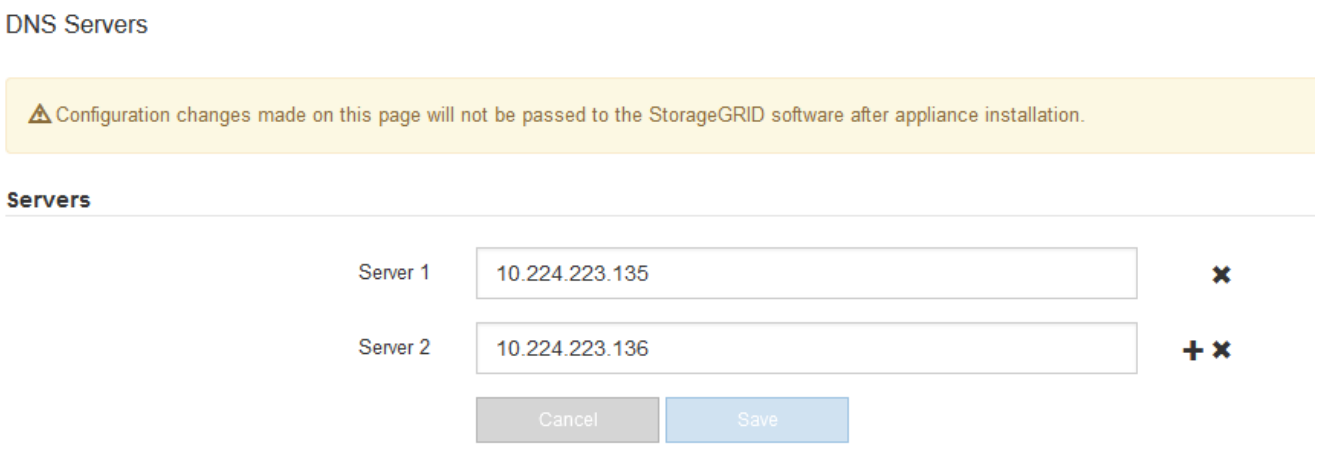
- Los cambios temporales en la configuración DNS sólo son necesarios para los dispositivos cifrados por nodo en los que el servidor KMS se define mediante un nombre de dominio completo, en lugar de una dirección IP, para el nombre de host.
- Cuando un dispositivo cifrado por nodo se conecta a un KMS mediante un nombre de dominio, debe conectarse a uno de los servidores DNS definidos para la cuadrícula. A continuación, uno de estos servidores DNS convierte el nombre de dominio en una dirección IP.
- Si el nodo no puede llegar a un servidor DNS para la cuadrícula, o si cambió la configuración de DNS para toda la cuadrícula cuando un nodo de dispositivo cifrado por nodo estaba sin conexión, el nodo no podrá conectarse al KMS. Los datos cifrados en el dispositivo no se pueden descifrar hasta que se resuelva el problema de DNS.

Para resolver un problema de DNS que impide la conexión de KMS, especifique la dirección IP de uno o más servidores DNS en el instalador de dispositivos de StorageGRID. Estas configuraciones temporales de DNS permiten que el dispositivo se conecte al KMS y descifre los datos en el nodo.

Por ejemplo, si el servidor DNS de la cuadrícula cambia mientras un nodo cifrado estaba desconectado, el nodo no podrá llegar al KMS cuando vuelva a conectarse, ya que sigue utilizando los valores DNS anteriores. La introducción de la nueva dirección IP del servidor DNS en el instalador de dispositivos de StorageGRID permite que una conexión KMS temporal descifre los datos del nodo.

Pasos

1. En el instalador de dispositivos StorageGRID, seleccione **Configurar redes** > **Configuración de DNS**.
2. Compruebe que los servidores DNS especificados sean correctos.



3. Si es necesario, cambie los servidores DNS.

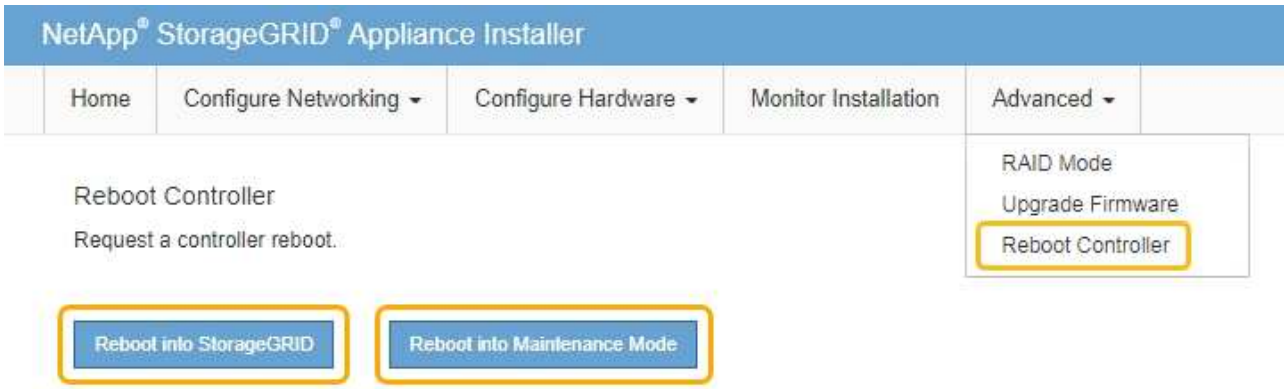
> Los cambios realizados en la configuración de DNS son temporales y se pierden al salir del modo de mantenimiento.

4. Cuando esté satisfecho con la configuración temporal de DNS, seleccione **Guardar**.

   El nodo utiliza la configuración del servidor DNS especificada en esta página para volver a conectarse al KMS, lo que permite descifrar los datos del nodo.

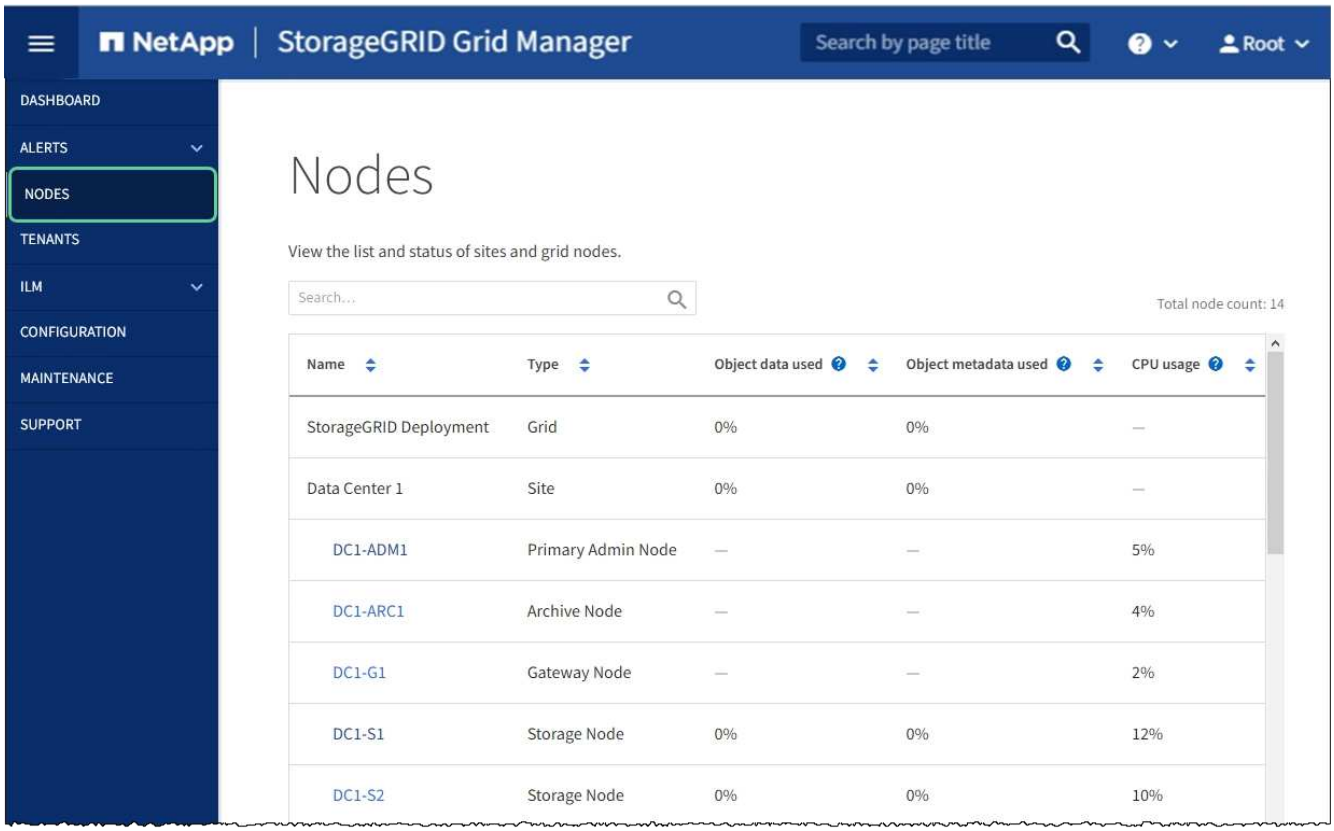
5. Tras descifrar los datos del nodo, reinicie el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:

   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



> Cuando el nodo se reinicia y se vuelve a unir a la cuadrícula, utiliza los servidores DNS de todo el sistema enumerados en Grid Manager. Después de volver a unirse a la cuadrícula, el dispositivo ya no utilizará los servidores DNS temporales especificados en el instalador de dispositivos StorageGRID mientras el dispositivo estaba en modo de mantenimiento.

El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Supervisar el cifrado de nodos en modo de mantenimiento (SG5600)

Si habilitó el cifrado de nodos para el dispositivo durante la instalación, puede supervisar el estado de cifrado del nodo de cada nodo de dispositivo, incluidos el estado del cifrado del nodo y detalles del servidor de gestión de claves (KMS).

Lo que necesitará

- El cifrado de nodos debe haber estado habilitado para el dispositivo durante la instalación. No se puede habilitar el cifrado de nodos después de que el dispositivo se haya instalado.
- El aparato se ha estado se pone en modo de mantenimiento.

Pasos

1. En el instalador del dispositivo StorageGRID, seleccione **Configurar hardware** > **cifrado de nodos**.

Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

Encryption Status

You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption ☑

Save

Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate >

Client certificate >

Clear KMS Key

Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

La página cifrado de nodos incluye estas tres secciones:

- El estado de cifrado muestra si el cifrado de nodos está habilitado o deshabilitado para el dispositivo.
- Detalles del servidor de gestión de claves muestra información sobre el KMS que se utiliza para cifrar el dispositivo. Puede expandir las secciones de certificados de servidor y cliente para ver los detalles y el estado del certificado.
  - Para solucionar problemas con los propios certificados, como renovar certificados caducados, consulte la información sobre KMS en las instrucciones para administrar StorageGRID.
  - Si hay problemas inesperados al conectarse a los hosts KMS, compruebe que los servidores del sistema de nombres de dominio (DNS) son correctos y que la red del dispositivo está configurada correctamente.

    Comprobar la configuración del servidor DNS

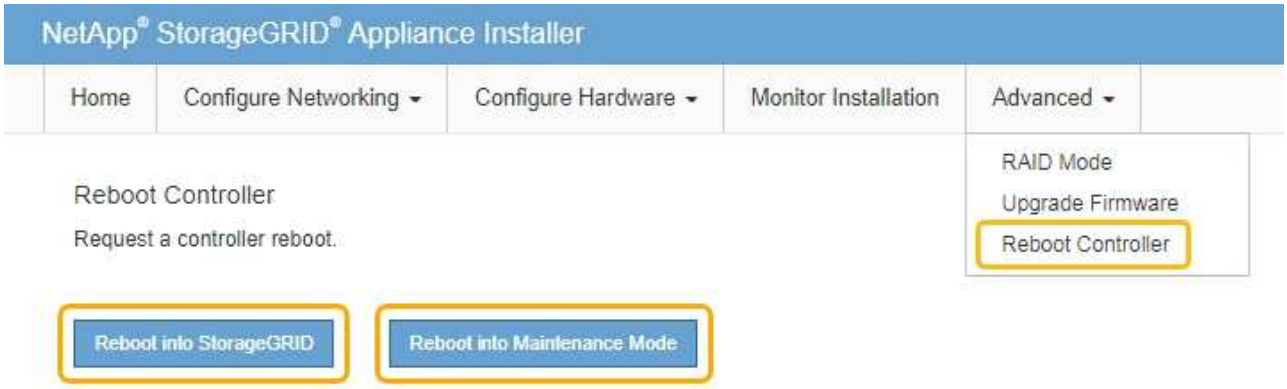
  - Si no puede resolver problemas de certificado, póngase en contacto con el soporte técnico.
- Clear KMS Key deshabilita el cifrado de nodos para el dispositivo, elimina la asociación entre el

dispositivo y el servidor de gestión de claves configurado para el sitio StorageGRID y elimina todos los datos del dispositivo. Debe borrar la clave KMS antes de poder instalar el dispositivo en otro sistema StorageGRID.

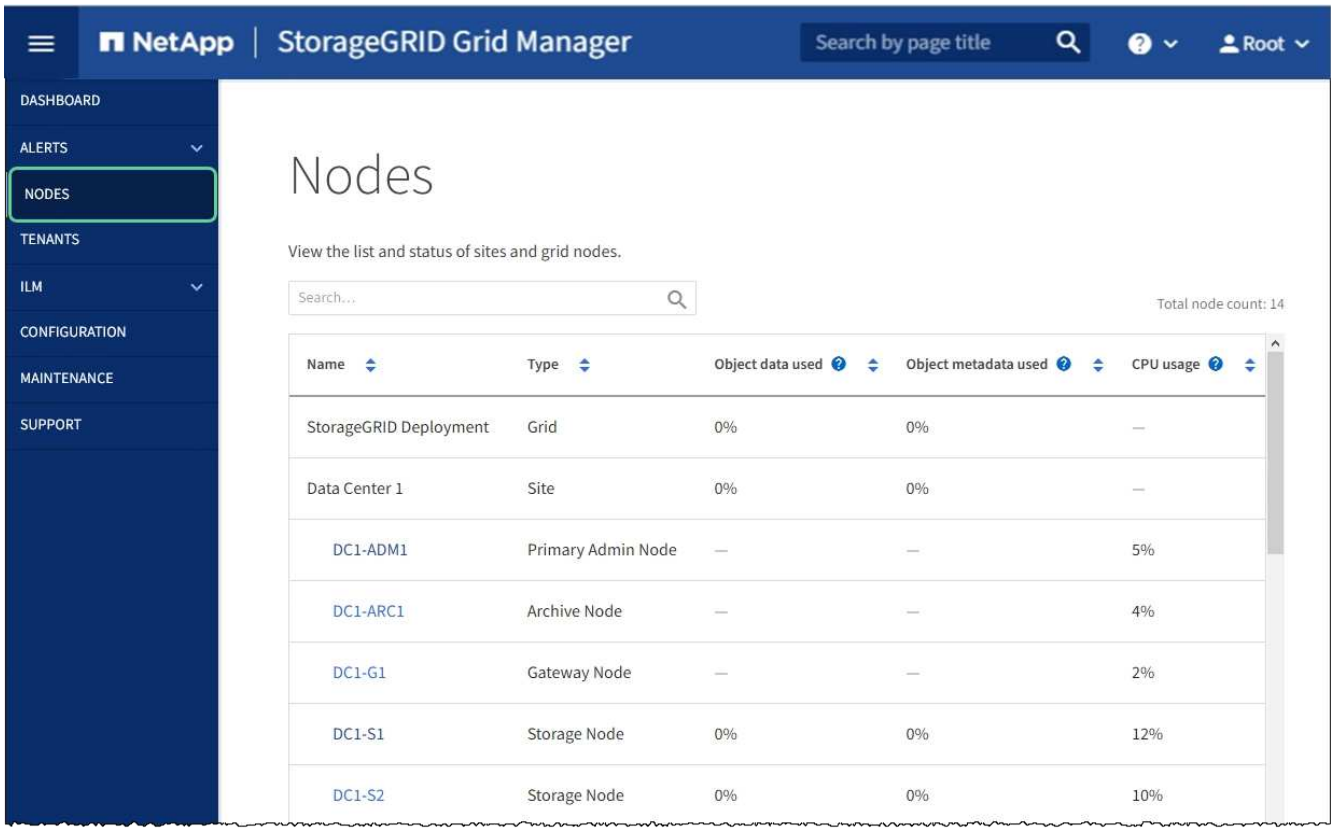
Borrar configuración de servidor de gestión de claves

> Al borrar la configuración de KMS se eliminan los datos del dispositivo, lo que hace que no se pueda acceder a ellos de forma permanente. Estos datos no se pueden recuperar.

2. Cuando haya terminado de comprobar el estado de cifrado de nodo, reinicie el nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione una de estas opciones:
   - Seleccione **Reiniciar en StorageGRID** para reiniciar el controlador con el nodo que vuelve a unir la cuadrícula. Seleccione esta opción si hizo trabajo en modo de mantenimiento y está listo para devolver el nodo a su funcionamiento normal.
   - Seleccione **Reiniciar en el modo de mantenimiento** para reiniciar el controlador con el nodo restante en modo de mantenimiento. (Esta opción solo está disponible si la controladora se encuentra en modo de mantenimiento). Seleccione esta opción si hay otras operaciones de mantenimiento que debe realizar en el nodo antes de volver a unir la cuadrícula.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **NODES** debe mostrar un estado normal (sin icono) para el nodo del dispositivo, indicando que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Información relacionada

Administre StorageGRID

Borrar configuración de servidor de gestión de claves

Al borrar la configuración del servidor de gestión de claves (KMS), se deshabilita el cifrado de nodos en el dispositivo. Tras borrar la configuración de KMS, los datos del dispositivo se eliminan de forma permanente y ya no se puede acceder a ellos. Estos datos no se pueden recuperar.

Lo que necesitará

Si necesita conservar datos en el dispositivo, debe realizar un procedimiento de retirada del nodo o clonar el nodo antes de borrar la configuración de KMS.

> Cuando se borra KMS, los datos del dispositivo se eliminan de forma permanente y ya no se puede acceder a ellos. Estos datos no se pueden recuperar.

Retire el nodo Para mover los datos que contiene a otros nodos en StorageGRID.

Acerca de esta tarea

Al borrar la configuración de KMS del dispositivo, se deshabilita el cifrado de nodos y se elimina la asociación entre el nodo del dispositivo y la configuración de KMS del sitio StorageGRID. Los datos del dispositivo se eliminan y el dispositivo se deja en estado previo a la instalación. Este proceso no se puede revertir.

Debe borrar la configuración de KMS:

- Antes de poder instalar el dispositivo en otro sistema StorageGRID, que no utiliza un KMS o que utiliza un

KMS diferente.

> No borre la configuración de KMS si piensa volver a instalar un nodo de dispositivo en un sistema StorageGRID que utilice la misma clave KMS.

- Antes de poder recuperar y volver a instalar un nodo en el que se perdió la configuración de KMS y la clave KMS no se puede recuperar.
- Antes de devolver cualquier aparato que se haya utilizado anteriormente en su centro.
- Después de retirar un dispositivo con el cifrado de nodos habilitado.

> Retire el dispositivo antes de borrar KMS para mover sus datos a otros nodos del sistema StorageGRID. La eliminación de KMS antes de retirar el dispositivo provocará la pérdida de datos y podría hacer que el dispositivo deje de funcionar.

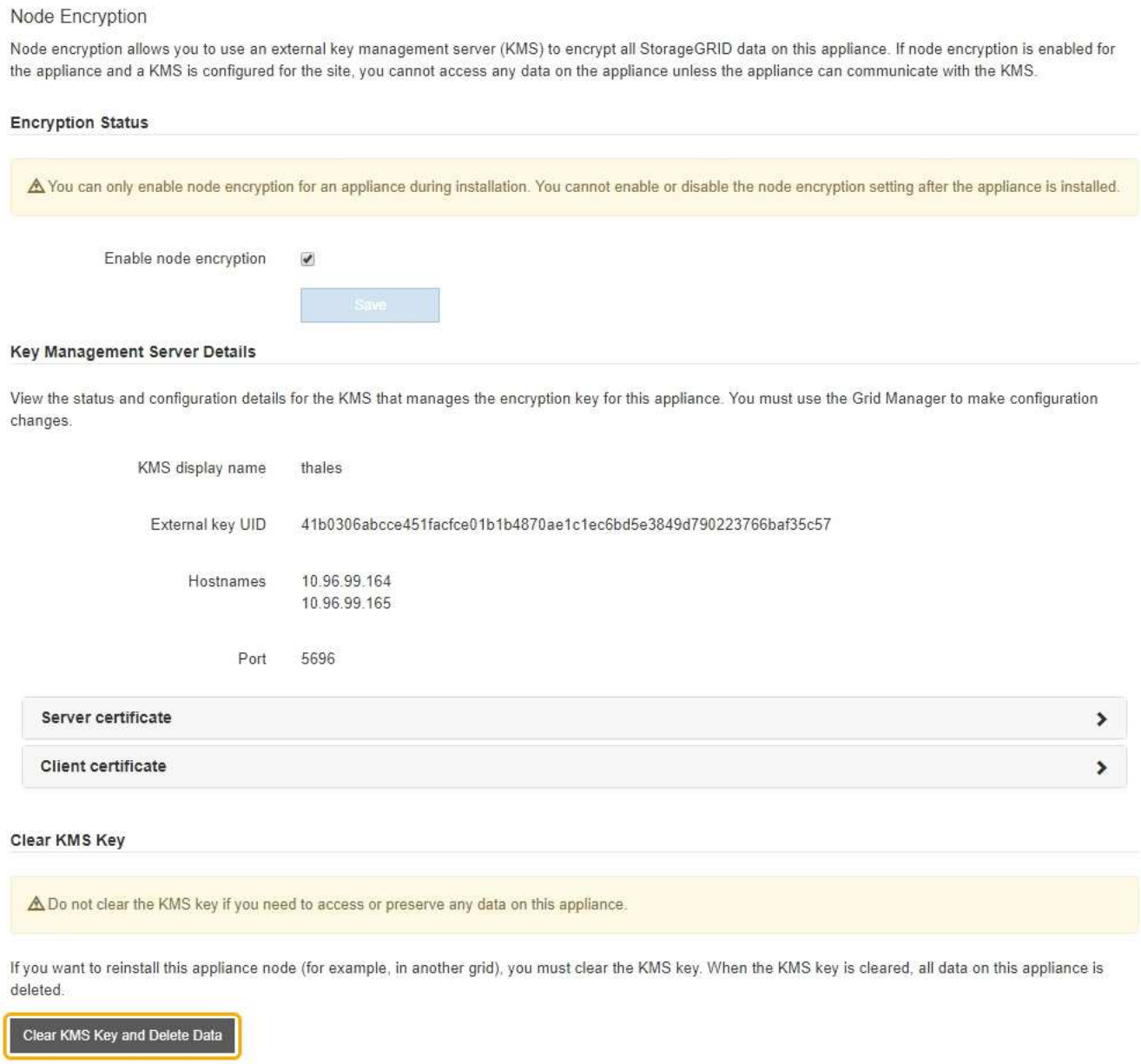
Pasos

1. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.
   `https://Controller_IP:8443`

   `Controller_IP` Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

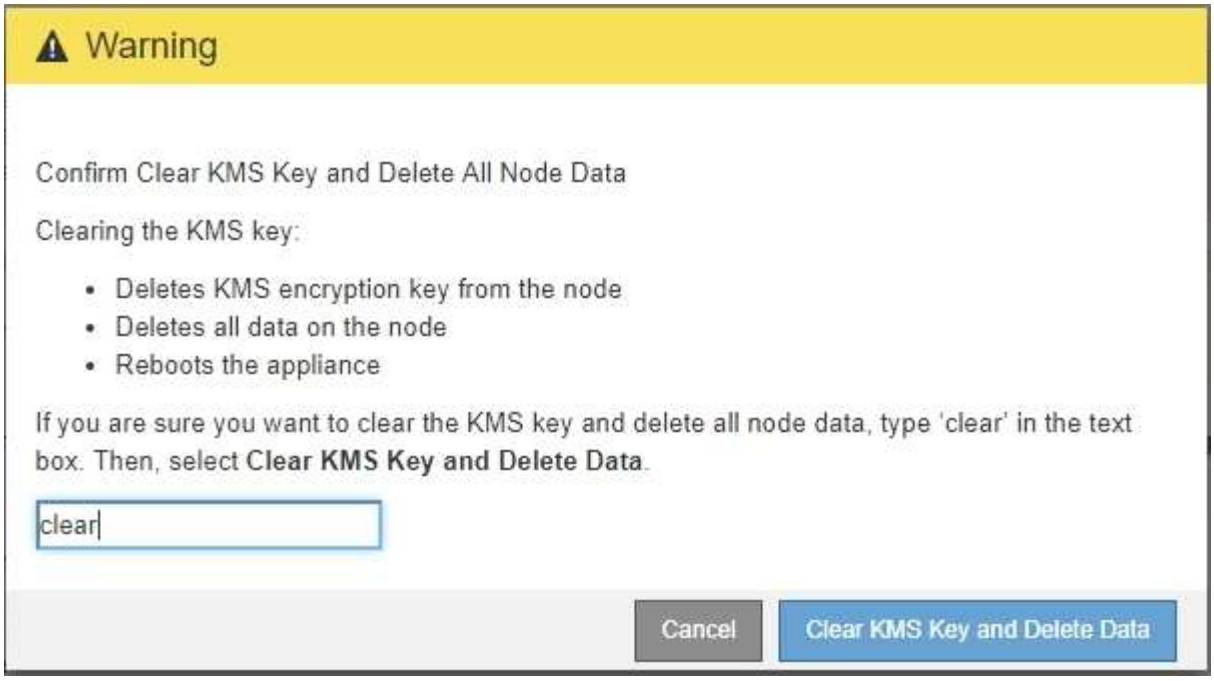
   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Configurar hardware** > **cifrado de nodos**.



> Si se borra la configuración de KMS, los datos del dispositivo se eliminarán permanentemente. Estos datos no se pueden recuperar.

3. En la parte inferior de la ventana, seleccione **Borrar clave KMS y Eliminar datos**.
4. Si está seguro de que desea borrar la configuración de KMS, escriba `clear` + y seleccione **Borrar clave KMS y Eliminar datos**.



La clave de cifrado KMS y todos los datos se eliminan del nodo y el dispositivo se reinicia. Esto puede tardar hasta 20 minutos.

5. Abra un explorador e introduzca una de las direcciones IP para la controladora de computación del dispositivo.
   `https://Controller_IP:8443`

   `Controller_IP` Es la dirección IP de la controladora de computación (no la controladora de almacenamiento) en cualquiera de las tres redes StorageGRID.

   Aparece la página de inicio del instalador de dispositivos de StorageGRID.

6. Seleccione **Configurar hardware** > **cifrado de nodos**.
7. Compruebe que el cifrado de nodos está desactivado y que la información de claves y certificados de **Detalles del servidor de administración de claves** y el control **Borrar clave KMS y Eliminar datos** se eliminan de la ventana.

   El cifrado de nodos no se puede volver a habilitar en el dispositivo hasta que se vuelva a instalar en una cuadrícula.

Después de terminar

Una vez que el dispositivo se haya reiniciado y haya verificado que se ha borrado KMS y que el dispositivo está en estado previo a la instalación, puede quitar físicamente el dispositivo del sistema de StorageGRID. Consulte las instrucciones de recuperación y mantenimiento para obtener información acerca de Prepare el aparato para su reinstalación.

Información relacionada

Administre StorageGRID

Instale y actualice el software

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

En estas instrucciones, se describen las novedades de StorageGRID 11.6 y se proporcionan instrucciones paso a paso para actualizar todos los nodos del sistema StorageGRID a la nueva versión.

Antes de empezar

Revise estos temas para obtener información sobre las nuevas funciones y mejoras de StorageGRID 11.6, determine si alguna función ha sido obsoleta o eliminada y obtenga información acerca de los cambios en las API de StorageGRID.

- Novedades de StorageGRID 11.6
- Operaciones eliminadas o obsoletas
- Cambios en la API de gestión de grid
- Cambios en la API de gestión de inquilinos

Novedades de StorageGRID 11.6

Esta versión de StorageGRID presenta las siguientes funciones.

Mejoras en la facilidad de uso

La interfaz de usuario de Grid Manager se ha rediseñado de manera considerable para mejorar la experiencia del usuario.

- Una nueva barra lateral reemplaza los menús desplegables de la interfaz de usuario antigua.
- Se reorganizaron varios menús para mantener juntos las opciones relacionadas. Por ejemplo, el menú **CONFIGURACIÓN** incluye una nueva sección **Seguridad** para las opciones certificados, servidor de administración de claves, Configuración de proxy y redes de cliente no confiables.
- Un campo **Buscar** en la barra de encabezado permite navegar rápidamente a las páginas de Grid Manager.
- La tabla de resumen de la página **Nodes** proporciona información de alto nivel para todos los sitios y nodos, como los datos de objeto utilizados y los metadatos de objetos utilizados, e incluye un nuevo campo de búsqueda. Se muestran iconos de alerta junto a cualquier nodo con alertas activas.
- Los nuevos asistentes le guían en configuraciones más complejas, como los flujos de trabajo de grupos de administración, usuarios de administración, inquilinos, extremos de equilibrador de carga y grupos de alta disponibilidad (ha).
- Todas las páginas de la interfaz de usuario se han vuelto a imprimir con fuentes actualizadas, estilos de botones y formatos de tabla.

A menos que se haya producido un cambio funcional, las capturas de pantalla del sitio de documentación de StorageGRID 11.6 no se han actualizado para reflejar el nuevo estilo de página de Grid Manager.

Consulte lo siguiente:

- Administre StorageGRID
- Supervisión y solución de problemas

Múltiples interfaces VLAN

Ahora puede crear interfaces de LAN virtual (VLAN) para los nodos de administración y de puerta de enlace. Puede utilizar interfaces VLAN en grupos de alta disponibilidad y extremos de equilibrio de carga para aislar y dividir el tráfico del cliente en particiones para seguridad, flexibilidad y rendimiento.

- El nuevo asistente **Crear una interfaz VLAN** le guiará a través del proceso de introducir una identificación VLAN y elegir una interfaz padre en uno o más nodos. Una interfaz principal puede ser Grid Network, Client Network o una interfaz troncal adicional para la máquina virtual o el host sin sistema operativo. Consulte Configure las interfaces VLAN.
- Ahora se puede añadir un tronco o interfaces de acceso adicionales a un nodo. Si agrega una interfaz troncal, debe configurar una interfaz VLAN. Si agrega una interfaz de acceso, puede agregar la interfaz directamente a un grupo de alta disponibilidad; no es necesario configurar una interfaz de VLAN. Consulte lo siguiente:
  - **Linux (antes de instalar el nodo)**: Mejoras en la instalación
  - **Linux (después de instalar el nodo)**: Linux: Añada tronco o interfaces de acceso a un nodo
  - **VMware (después de instalar el nodo)**: Recopile información sobre el entorno de implementación

Puede usar Azure AD para la federación de identidades

Ahora puede seleccionar Azure Active Directory (Azure AD) como origen de identidades al configurar la federación de identidades para el Administrador de grid o el Administrador de inquilinos. Consulte Usar la federación de identidades.

Puede utilizar Azure AD y PingFederate para SSO

Ahora puede seleccionar Azure AD o PingFederate como tipo SSO al configurar el inicio de sesión único (SSO) para su grid. A continuación, puede utilizar el modo Sandbox para configurar y probar las aplicaciones empresariales de Azure AD o las conexiones del proveedor de servicios de PingFederate (SP) a cada nodo de administración de StorageGRID. Consulte Configurar el inicio de sesión único.

Gestión de certificados centralizada

- La nueva página de certificados (**CONFIGURACIÓN** > **Seguridad** > **certificados**) consolida la información sobre todos los certificados de seguridad StorageGRID en una única ubicación. Puede gestionar los certificados globales de StorageGRID, de la CA de grid y de cliente desde la página nueva o ver información sobre otros certificados, como los que se utilizan para extremos de equilibrador de carga, inquilinos y federación de identidades. Consulte Acerca de los certificados de seguridad.
- Como parte de este cambio, se cambió el nombre de los siguientes certificados globales:
  - El **Certificado de servidor de interfaz de administración** es ahora el **Certificado de interfaz de administración**.

- El certificado de servidor * Object Storage API Service Endpoints* (también llamado Storage API Server Certificate) es ahora el certificado de la API **S3 y Swift**.
- El **Certificado CA interno**, **Certificado CA del sistema**, **Certificado CA** y **Certificado CA predeterminado** se conocen de manera consistente como el **Certificado CA de Grid**.

Otras mejoras de Grid Manager

- **Actualizaciones a grupos de alta disponibilidad**. Ahora, un asistente lo guiará en el proceso de creación de un grupo de alta disponibilidad. Consulte Configuración de grupos de alta disponibilidad.
  - Además de seleccionar interfaces en Grid Network (eth0) o Client Network (eth2), ahora puede seleccionar interfaces VLAN o cualquier interfaz de acceso que haya agregado al nodo.
  - Ahora puede especificar un orden de prioridad para las interfaces. Puede elegir la interfaz principal y clasificar cada interfaz de backup en orden.
  - Si alguno de los clientes S3, Swift, administrativos o inquilinos tendrá acceso a las direcciones VIP del grupo de alta disponibilidad desde una subred diferente, ahora puede proporcionar la dirección IP para la puerta de enlace.
- **Actualizaciones a los extremos del equilibrador de carga**. Un nuevo asistente le guiará a través del proceso de creación de un punto final de equilibrio de carga. Consulte Configurar puntos finales del equilibrador de carga.
  - Ahora puede seleccionar el tipo de cliente (S3 o Swift) cuando crea el extremo por primera vez, en lugar de añadir este detalle después de crear el extremo.
  - Ahora puede utilizar el certificado global * StorageGRID S3 y Swift* para un extremo de equilibrador de carga en lugar de cargar o generar un certificado independiente.

> Este certificado global se utilizó anteriormente para conexiones al servicio CLB obsoleto y a nodos de almacenamiento. Si desea utilizar el certificado global para un extremo de equilibrio de carga, debe cargar un certificado personalizado en la página del certificado API S3 y Swift.

Nuevas funciones del administrador de inquilinos

- **Nueva Consola Experimental S3**. Disponible como enlace de la página Buckets en el Administrador de inquilinos, la nueva consola de S3 experimental permite a los usuarios de inquilinos S3 ver y gestionar los objetos de sus bloques. Consulte Utilice la consola Experimental S3.

> La consola de S3 de experimental no se ha probado completamente y no está pensada para la gestión masiva de objetos ni para su uso en un entorno de producción. Los inquilinos solo deben usar S3 Console al realizar funciones para un número reducido de objetos, o cuando se utilizan grids de prueba de concepto o no de producción.

- **Puede eliminar varios bloques S3**. Los usuarios de inquilinos ahora pueden eliminar más de un bloque de S3 a la vez. Cada segmento que desea eliminar debe estar vacío. Consulte Eliminar bloque de S3.
- **Actualiza a permiso de cuentas de inquilino**. Los usuarios de administrador que pertenecen a un grupo con el permiso Cuentas de arrendatario ahora pueden ver las directivas de clasificación de tráfico existentes. Anteriormente, se requería a los usuarios tener permiso acceso raíz para ver estas métricas.

Nuevo proceso de actualización y revisión

- La página **actualización de StorageGRID** se ha rediseñado (**MANTENIMIENTO** > **sistema** >

actualización de software > **actualización de StorageGRID**).

- Después de que se completa la actualización a StorageGRID 11.6, puede utilizar el Administrador de grid para actualizar a una versión futura y aplicar una revisión para esa versión al mismo tiempo. La página de actualización de StorageGRID mostrará la ruta de actualización recomendada y vinculará directamente con las páginas de descarga correctas.
- Una nueva casilla de verificación **Buscar actualizaciones de software** en la página AutoSupport (**SUPPORT** > **Tools** > **AutoSupport**) permite controlar esta funcionalidad. Puede desactivar la búsqueda de actualizaciones de software disponibles si el sistema no tiene acceso WAN. Consulte Configurar las comprobaciones de de AutoSupport para actualizaciones de software.

> Para la actualización a StorageGRID 11.6, puede utilizar opcionalmente una secuencia de comandos para actualizar y aplicar una revisión al mismo tiempo. Consulte "Base de conocimientos de NetApp: Cómo ejecutar scripts combinados de actualizaciones importantes y revisiones para StorageGRID".

- Ahora puede pausar una actualización del sistema operativo de SANtricity y omitir la actualización de algunos nodos si necesita finalizar la actualización en el futuro. Consulte las instrucciones para su dispositivo de almacenamiento:
  - Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante Grid Manager (SG5600)
  - Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante Grid Manager (SG5700)
  - Actualizar el sistema operativo SANtricity en controladoras de almacenamiento mediante Grid Manager (SG6000)

Compatibilidad con servidores de syslog externos

- Ahora puede configurar un servidor de syslog externo si desea guardar y administrar mensajes de auditoría y un subconjunto de registros de StorageGRID de forma remota (**CONFIGURACIÓN** > **Supervisión** > **servidor de auditoría y syslog**). Una vez que se configura un servidor de syslog externo, puede guardar mensajes de auditoría y ciertos archivos de registro de forma local, remota o ambos. Al configurar los destinos de la información de auditoría, puede reducir el tráfico de red en los nodos admin. Consulte Configurar los mensajes de auditoría y los destinos de registro.
- En relación con esta funcionalidad, las nuevas casillas de verificación de la página registros (**SUPPORT** > **Tools** > **Logs**) le permiten especificar qué tipos de registros desea recopilar, como ciertos registros de aplicaciones, registros de auditoría, registros utilizados para la depuración de la red y registros de la base de datos Prometheus. Consulte Recopilar archivos de registro y datos del sistema.

S3 Select

Ahora puede permitir a los inquilinos S3 que emita solicitudes SelectObjectContent a 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. Consulte Gestione S3 Select para cuentas de inquilinos y.. Utilice S3 Select.

También se añadieron los gráficos Grafana para las operaciones de S3 Select. Consulte Revisar las métricas de soporte.

Período de retención de bloques predeterminado de S3 Object Lock

Cuando se usa el bloqueo de objetos S3, ahora se puede especificar un período de retención predeterminado

para el bloque. El período de retención predeterminado se aplica a cualquier objeto agregado al bloque que no tenga su propia configuración de retención. Consulte Utilice el bloqueo de objetos de S3.

Compatibilidad con Google Cloud Platform

Ahora puede usar Google Cloud Platform (GCP) como extremo de los pools de almacenamiento en cloud y el servicio de la plataforma CloudMirror. Consulte Especifique el URN para un extremo de servicios de plataforma y.. Cree un pool de almacenamiento en el cloud.

Compatibilidad con AWS C2S

Ahora puede usar extremos de los servicios de cloud comercial (C2S) de AWS para la replicación de CloudMirror. Consulte Cree un extremo de servicios de plataforma.

Otros cambios de S3

- **OBTENER soporte de objeto Y OBJETO PRINCIPAL para objetos multipartes**. Anteriormente, StorageGRID no era compatible con `partNumber` Solicitar parámetro EN GET Object o HEAD Object peticiones. Ahora puede emitir solicitudes GET Y HEAD para recuperar una parte específica de un objeto de varias partes. GET and HEAD Object también es compatible con `x-amz-mp-parts-count` elemento de respuesta para indicar cuántas partes tiene un objeto.
- **Cambios en el control de consistencia "disponible"**. El control de consistencia “disponible” ahora se comporta igual que el nivel de consistencia de “lectura tras escritura nueva”, pero proporciona una coherencia eventual para las operaciones DE CABEZAL Y GET. El control de coherencia “disponible” ofrece una mayor disponibilidad para las operaciones HEAD y GET que “Read-after-new-write” si los nodos de almacenamiento no están disponibles. Se diferencia de las garantías de coherencia de Amazon S3 para HEAD y GET.

  Use S3

Mejoras en el rendimiento

- **Los nodos de almacenamiento admiten 2000 millones de objetos**. La estructura de directorios subyacente en nodos de almacenamiento se optimizó para mejorar la escalabilidad y el rendimiento. Ahora, los nodos de almacenamiento utilizan subdirectorios adicionales para almacenar hasta 2000 millones de objetos replicados y maximizar el rendimiento. Los subdirectorios de nodos se modifican al actualizar a StorageGRID 11.6, pero los objetos existentes no se redistribuyen a los nuevos directorios.
- **Aumento del rendimiento de la eliminación basada en ILM para dispositivos de alto rendimiento**. Los recursos y el rendimiento empleados para realizar operaciones de eliminación del ciclo de vida de la información ahora se adaptan al tamaño y la funcionalidad de cada nodo de la aplicación StorageGRID. Para los dispositivos SG5600, el rendimiento es el mismo que para StorageGRID 11.5. Para los dispositivos SG5700, se realizaron pequeñas mejoras para eliminar el rendimiento de la ILM. Para los dispositivos SG6000, que tienen más RAM y más CPU, las eliminaciones de ILM se procesan ahora de forma mucho más rápida. Las mejoras se hacen especialmente notables en los dispositivos SGF6024 all-flash.
- **Marcas de agua de volumen de almacenamiento optimizadas**. En las versiones anteriores, la configuración de las tres marcas de agua de volumen de almacenamiento se aplicaba a cada volumen de almacenamiento en cada nodo de almacenamiento. StorageGRID ahora puede optimizar estas marcas de agua para cada volumen de almacenamiento, según el tamaño del nodo de almacenamiento y la capacidad relativa del volumen. Consulte ¿Qué son las marcas de agua del volumen de almacenamiento.

  Las marcas de agua optimizadas se aplican automáticamente a todos los sistemas StorageGRID 11.6 nuevos y más actualizados. Las marcas de agua optimizadas serán mayores que los ajustes

predeterminados anteriores.

Si utiliza marcas de agua personalizadas, la alerta **anulación de Marca de agua de sólo lectura baja** puede activarse después de actualizar. Esta alerta le permite saber si la configuración personalizada de la Marca de agua es demasiado pequeña. Consulte Solucionar los problemas de las alertas de anulación de la Marca de agua de sólo lectura baja.

Como parte de este cambio, se añadieron dos métricas Prometheus:

  - `storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark`
  - `storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark`

- **Aumento del espacio máximo de metadatos permitido**. El espacio máximo de metadatos permitido para los nodos de almacenamiento aumentó a 3.96 TB (de 2.64 TB) en el caso de los nodos de mayor capacidad, que son nodos con un espacio reservado real para metadatos de más de 4 TB. Este nuevo valor permite que se almacenen más metadatos de objetos en determinados nodos de almacenamiento y puede aumentar la capacidad de los metadatos de StorageGRID hasta un 50 %.

  > Si todavía no lo ha hecho, y si sus nodos de almacenamiento tienen suficiente RAM y espacio suficiente en el volumen 0, podrá Aumente manualmente la configuración del espacio reservado de metadatos hasta 8 TB después de instalar o actualizar.

  - Gestione el almacenamiento de metadatos de objetos espacio de metadatos permitido
  - Aumentar el espacio reservado de metadatos

Mejoras en los procedimientos de mantenimiento y las herramientas de soporte

- **Puede cambiar las contraseñas de la consola de nodos**. Ahora puede utilizar Grid Manager para cambiar las contraseñas de la consola del nodo (**CONFIGURACIÓN** > **Control de acceso** > **contraseñas de cuadrícula**). Estas contraseñas se utilizan para iniciar sesión en un nodo como “admin” mediante SSH, o al usuario root en una conexión de VM/consola física. Consulte Cambie las contraseñas de la consola de los nodos.
- **Asistente para comprobación de la existencia de nuevos objetos**. Ahora puede verificar la integridad del objeto con un asistente de comprobación de la existencia de objetos fácil de usar (**MANTENIMIENTO** > **tareas** > **comprobación de la existencia de objetos**), que sustituye al procedimiento de verificación en primer plano. El nuevo procedimiento tarda un tercio o menos en completarse y puede verificar varios nodos a la vez. Consulte Verifique la integridad del objeto.
- * Cuadro de "tiempo estimado hasta la finalización" para el reequilibrio de EC y trabajos de reparación de EC*. Ahora puede ver el tiempo estimado hasta la finalización y el porcentaje de finalización de un reequilibrio de EC actual o un trabajo de reparación EC.
- **Porcentaje estimado completado para reparaciones de datos replicadas**. Ahora puede agregar el `show-replicated-repair-status` de la `repair-data` comando para ver un porcentaje estimado de finalización para una reparación replicada.

  > La `show-replicated-repair-status` Esta opción está disponible para la versión preliminar técnica de StorageGRID 11.6. Esta característica está en desarrollo y el valor devuelto puede ser incorrecto o retardado. Para determinar si una reparación está completa, continúe utilizando **esperando - todos**, **reparaciones intentadas (XRPA)** y **periodo de exploración — estimado (XSCM)** como se describe en los procedimientos de recuperación.

- Los resultados de la página Diagnósticos (**SUPPORT** > **Tools** > **Diagnostics**) ahora se ordenan por gravedad y, a continuación, por orden alfabético.
- Prometheus y Grafana se actualizaron a nuevas versiones con interfaces y gráficos modificados. Como parte de este cambio, se cambiaron las etiquetas de algunas métricas.
  - Si tiene consultas personalizadas de las que ha utilizado las etiquetas de `node_network_up`, ahora debe utilizar las etiquetas de `node_network_info` en su lugar.
  - Si también se utilizó el nombre de la etiqueta `interface` desde cualquiera de las `node_network` métricas, ahora debe utilizar la `device` en su lugar, etiquete.
- Anteriormente, las métricas de Prometheus se almacenaban en nodos de administración durante 31 días. Ahora, las métricas se almacenan hasta que se llena el espacio reservado a los datos de Prometheus, lo cual puede aumentar significativamente el tiempo de disponibilidad de las métricas históricas.

  Cuando la `/var/local/mysql_ibdata/` el volumen alcanza la capacidad; las métricas más antiguas se eliminan primero.

Mejoras en la instalación

- Ahora tiene la opción de utilizar Podman como contenedor durante la instalación de Red Hat Enterprise Linux. Anteriormente, StorageGRID solo admitía un contenedor Docker.
- Los esquemas API para StorageGRID ahora se incluyen en los archivos de instalación para las plataformas Red Hat Enterprise Linux/CentOS, Ubuntu/Debian y VMware. Después de extraer el archivo, puede encontrar los esquemas en `/extras/api-schemas` carpeta.
- La `BLOCK_DEVICE_RANGEDB` introduzca el archivo de configuración del nodo para las implementaciones con configuración básica y ahora debe contener tres dígitos en lugar de dos. Es decir, en lugar de `BLOCK_DEVICE_RANGEDB_nn`, debe especificar `BLOCK_DEVICE_RANGEDB_nnn`.

  Para comprobar la compatibilidad con las puestas en marcha existentes, aún se admiten las claves de dos dígitos para los nodos actualizados.

- Opcionalmente, puede añadir una o varias instancias del nuevo `INTERFACES_TARGET_nnnn` clave del archivo de configuración del nodo para puestas en marcha con configuración básica. Cada clave proporciona el nombre y la descripción de una interfaz física en el host de configuración básica, que se mostrará en la página interfaces VLAN y la página grupos de alta disponibilidad.
  - Crear archivos de configuración de nodos para implementaciones de Red Hat Enterprise Linux o CentOS
  - Cree archivos de configuración de nodos para implementaciones de Ubuntu o Debian

Nuevas alertas

Se han añadido las siguientes alertas nuevas para StorageGRID 11.6:

- Los registros de auditoría se están agregando a la cola de la memoria
- Tablas dañadas en Cassandra
- Fallo de reequilibrio de EC
- Fallo de reparación de EC
- Reparación EC bloqueada
- Caducidad de certificado de servidor global para la API de S3 y Swift

- Vencimiento del certificado de CA de syslog externo
- Vencimiento del certificado de cliente de syslog externo
- Vencimiento del certificado de servidor de syslog externo
- Error de reenvío del servidor de syslog externo
- Error de sincronización de la federación de identidades para un inquilino
- Se ha detectado una actividad de equilibrador de carga de CLB heredada
- Los registros se están agregando a la cola del disco
- Anulación de Marca de agua de sólo lectura baja
- Bajo espacio libre en el directorio tmp
- Error en la comprobación de la existencia del objeto
- Comprobación de existencia de objeto bloqueada
- S3 PUT Object size demasiado grande

Consulte Referencia de alertas.

Cambios en los mensajes de auditoría

- Se ha agregado un nuevo campo **BUID** al mensaje de auditoría ORLM: Object Rules met. El campo **BUID** muestra el ID de cucharón, que se utiliza para operaciones internas. El nuevo campo sólo aparece si el estado del mensaje es PRGD.
- Se ha agregado un nuevo campo **SGRP** a los siguientes mensajes de auditoría. El campo **SGRP** sólo está presente si un objeto se eliminó en un sitio diferente al lugar donde se ingirió.
  - IDEL: Eliminación de ILM iniciada
  - OVWR: Sobrescritura de objetos
  - SDEL: ELIMINACIÓN DE S3
  - WDEL: ELIMINACIÓN de Swift

Consulte Revisar los registros de auditoría.

Cambios en la documentación de StorageGRID

La apariencia del sitio de documentación de StorageGRID 11.6 se ha modificado y ahora utiliza GitHub como plataforma subyacente.

NetApp agradece las valoraciones que se han proporcionado en relación con el contenido y anima a los usuarios a aprovechar la nueva función «solicitar cambios en la documentación» que se encuentra disponible en todas las páginas de la documentación del producto. La plataforma de documentación también ofrece una función de contribución de contenido incrustado para los usuarios de GitHub.

Eche un vistazo y contribuya a esta documentación. Puede editar, solicitar un cambio o simplemente enviar comentarios.

Operaciones eliminadas o obsoletas

En esta versión, se quitaron o obsoletos algunas funciones. Revise estos elementos para saber si necesita actualizar las aplicaciones del cliente o modificar la configuración antes

de realizar la actualización.

El sistema de alarmas y las API basadas en alarmas quedaron obsoletas

A partir del lanzamiento de StorageGRID 11.6, el sistema de alarma heredado queda obsoleto. La interfaz de usuario y las API del sistema de alarma heredado se eliminarán en una versión futura.

> Si todavía está utilizando alarmas heredadas, planea realizar una transición completa al sistema de alertas después de actualizar a StorageGRID 11.6. Consulte Gestionar alertas y alarmas: Descripción general para obtener más información acerca de las alertas.

La versión 11.6 deja obsoleto todas las API basadas en alarmas. Este cambio afecta a las siguientes API:

- `GET /grid/alarms`: Totalmente obsoleto
- `GET /grid/health/topology`: Totalmente obsoleto
- `GET /grid/health`: La `alarm-counts` la sección de la respuesta está obsoleta

Las versiones futuras no admiten el tamaño máximo de objeto de 5 TIB para PUT Object

En las próximas versiones de StorageGRID, el tamaño máximo para una sola operación DE PUT Object será de 5 GIB, en lugar de 5 TIB. Puede usar la carga de varias partes para objetos que sean más grandes de 5 GIB, hasta un máximo de 5 TIB (5,497,558,138,880 bytes).

Para ayudarle a realizar la transición de clientes a utilizar tamaños de objeto más pequeños en PUT Object, se activará la alerta * S3 PUT Object size demasiado grande* en StorageGRID 11.6 si un cliente S3 intenta cargar un objeto que supere los 5 GIB.

Función de puente NAS obsoleta

La función de puente NAS introdujo anteriormente acceso limitado con la versión StorageGRID 11.4. La función de puente NAS permanece con acceso limitado y está en desuso a partir de StorageGRID 11.6.

El puente NAS 11.4 sigue siendo la versión final y seguirá siendo compatible con StorageGRID 11.6. Revise la "Herramienta de matriz de interoperabilidad de NetApp" Para obtener compatibilidad continua entre las versiones NAS Bridge 11.4 y StorageGRID.

Consulte el sitio de soporte de NetApp para ver el "Calendario de soporte del puente NAS".

Cambios en la API de gestión de grid

StorageGRID 11.6 utiliza la versión 3 de la API de administración de grid. La versión 3 deja obsoleto la versión 2; sin embargo, la versión 1 y la versión 2 siguen siendo compatibles.

> Puede continuar utilizando la versión 1 y versión 2 de la API de gestión con StorageGRID 11.6; sin embargo, la compatibilidad con estas versiones de la API se eliminará en una versión futura de StorageGRID. Después de actualizar a StorageGRID 11.6, las API v1 y v2 obsoletas se pueden desactivar mediante la `PUT /grid/config/management` API.

Para obtener más información, visite Utilice la API de gestión de grid.

Puede acceder a los documentos de Swagger para operaciones de API privadas

Ahora puede acceder a los documentos de Swagger para la API privada desde Grid Manager. Para ver las operaciones disponibles, seleccione el icono de ayuda de Grid Manager y seleccione **Documentación de API**. A continuación, seleccione **Ir a documentación privada de API** en la página API de administración de StorageGRID.

Las API privadas de StorageGRID están sujetas a cambios sin previo aviso. Los extremos privados de StorageGRID también ignoran la versión de API de la solicitud.

API basadas en alarmas obsoletas

La versión 11.6 deja obsoleto todas las API basadas en alarmas. Este cambio afecta a las siguientes API:

- `GET /grid/alarms`: Totalmente obsoleto
- `GET /grid/health/topology`: Totalmente obsoleto
- `GET /grid/health`: La `alarm-counts` la sección de la respuesta está obsoleta

Puede importar claves de acceso de S3

Ahora puede usar la API de gestión de grid para importar claves de acceso S3 para usuarios inquilinos. Por ejemplo, es posible migrar claves de acceso de otro proveedor S3 a StorageGRID o usar esta función para mantener las credenciales de usuario iguales entre grids.

> Cuando esta función está habilitada, cualquier usuario de Grid Manager con permiso Cambiar contraseña raíz de inquilino tiene acceso completo a los datos de arrendatario. Deshabilite esta función inmediatamente después del uso para proteger los datos de inquilino.

Operaciones de cuenta nueva

Tres nuevos `grid/account` Se añadieron operaciones de API:

- `POST /grid/account-enable-s3-key-import`: Esta solicitud habilita la función Importar credenciales S3. Debe tener el permiso acceso raíz para habilitar esta función.
- `POST /grid/accounts/{id}/users/{user_id}/s3-access-keys`: Esta solicitud importa credenciales S3 para un usuario determinado en una cuenta de arrendatario. Debe tener el permiso acceso raíz o Cambiar contraseña raíz de inquilino y debe conocer el ID de usuario y el ID de cuenta de inquilino.
- `POST /grid/account-disable-s3-key-import`: Esta solicitud deshabilita la función Importar credenciales S3. Debe tener el permiso acceso raíz para deshabilitar esta función.

Método DE PARCHE obsoleto

El método DE REVISIÓN ha quedado obsoleto y se eliminará en una versión futura. Según sea necesario, realice una operación PUT para reemplazar un recurso en lugar de utilizar una operación DE REVISIÓN para modificar el recurso.

Adiciones a. `grid/logs/collect` extremo

Se han añadido cuatro valores booleanos al `grid/logs/collect` extremo:

- `applicationLogs`: Registros específicos de la aplicación que el soporte técnico utiliza con mayor frecuencia para la solución de problemas. Los registros recopilados son un subconjunto de los registros de aplicación disponibles. El valor predeterminado es `true`.
- `auditLogs`: Registros que contienen los mensajes de auditoría generados durante el funcionamiento normal del sistema. El valor predeterminado es `true`.
- `networkTrace`: Registros utilizados para la depuración de red. El valor predeterminado es `false`.
- `prometheusDatabase`: Métricas de series temporales de los servicios en todos los nodos. El valor predeterminado es `false`.

Nuevo `node-details /grid/service-ids` extremo

Lo nuevo `/grid/service-ids` El extremo proporciona una asignación de UUID de nodo a los nombres de nodo, identificadores de servicio y tipos de servicio asociados.

Puede recuperar las contraseñas de la consola de los nodos de grid

Ahora puede utilizar `POST /grid/node-console-passwords` para recuperar la lista de nodos de grid y sus contraseñas de la consola asociadas.

Cambios en la API de gestión de inquilinos

StorageGRID 11.6 utiliza la versión 3 de la API de gestión de inquilinos. La versión 3 deja obsoleto la versión 2; sin embargo, la versión 1 y la versión 2 siguen siendo compatibles.

> Puede continuar utilizando la versión 1 y versión 2 de la API de gestión con StorageGRID 11.6; sin embargo, la compatibilidad con estas versiones de la API se eliminará en una versión futura de StorageGRID. Después de actualizar a StorageGRID 11.6, las API v1 y v2 obsoletas se pueden desactivar mediante la `PUT /grid/config/management` API.

Para obtener más información, visite Conozca la API de gestión de inquilinos.

Método DE PARCHE obsoleto

El método DE REVISIÓN ha quedado obsoleto y se eliminará en una versión futura. Según sea necesario, realice una operación PUT para reemplazar un recurso en lugar de utilizar una operación DE REVISIÓN para modificar el recurso.

Planifique y prepare la actualización

Estime el tiempo para completar una actualización

A la hora de planificar una actualización a StorageGRID 11.6, debe tener en cuenta cuándo realizar la actualización, en función de la duración de la actualización. También debe conocer las operaciones que se pueden realizar y no se pueden realizar durante 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
Inicie el servicio de actualización	Se ejecutan comprobaciones previas de actualización, el archivo de software se distribuye y se inicia el servicio de actualización.	3 minutos por nodo de grid, a menos que se informen los errores de validación	Según sea necesario, puede ejecutar las comprobaciones previas de la actualización de forma manual antes de la ventana de mantenimiento de la actualización programada.
Actualizar nodos de grid (nodo de administrador principal)	El nodo de administrador principal se detiene, se actualiza y se reinicia.	De 30 minutos a 1 hora, con los nodos de las aplicaciones SG100 y SG1000 que requieren más tiempo.	No se puede acceder al nodo de administrador principal. Se informan errores de conexión, los cuales se pueden ignorar.
Actualizar nodos Grid (el resto de nodos)	Se actualiza el software de los demás nodos de grid, en el orden en el que se aprueban los nodos. Cada nodo de su sistema estará inactivo de uno en uno por varios minutos cada 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 servicio de asistencia técnica.

Tarea de actualización	Descripción	Tiempo aproximado necesario	Durante esta tarea
Active 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.
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 11.5 a 11.6 no requiere una actualización de la base de datos de Cassandra; sin embargo, el servicio Cassandra se detendrá y 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 finales de la actualización	Se eliminan los archivos temporales y se completa la actualización a la versión nueva.	5 minutos	Cuando finalice la tarea **pasos de actualización final**, 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 para actualizar a StorageGRID 11.6

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 11.6.0.

Cómo se ve afectado el sistema durante la actualización

Debe comprender 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. Los nodos de grid se ven inactivos de uno en uno durante la actualización, por lo que no hay una hora cuando todos los nodos de grid no están disponibles.

Para permitir la disponibilidad continua, debe asegurarse de que los objetos se almacenen de forma redundante con las políticas de ILM apropiadas. También debe asegurarse de que todos los clientes externos de S3 o Swift estén configurados para enviar solicitudes a una de las siguientes:

- Un extremo de StorageGRID configurado como 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

El firmware del dispositivo se ha actualizado

Durante la actualización de StorageGRID 11.6:

- Todos los nodos de dispositivos StorageGRID se actualizan automáticamente a la versión de firmware 3.6 de StorageGRID Appliance Installer.
- Los dispositivos SG6060 y SGF6024 se actualizan automáticamente a la versión de firmware del BIOS 3B07.EX y a la versión de firmware del BMC 3.93.07.
- Los dispositivos SG100 y SG1000 se actualizan automáticamente a la versión 3B12.EC del firmware del BIOS y a la versión 4.67.07 del firmware del BMC.

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 aparezca la alerta **no se puede comunicar con el nodo** cuando se detienen los servicios, o que aparezca la alerta **error de comunicación** de Cassandra cuando algunos nodos se han actualizado a StorageGRID 11.6 pero otros nodos todavía ejecutan StorageGRID 11.5. En general, estas alertas se borran cuando se completa la actualización.

La alerta de **colocación de ILM inalcanzable** puede activarse cuando se detienen los nodos de almacenamiento durante la actualización a StorageGRID 11.6. Esta alerta podría persistir durante un día después de que se completa la actualización.

Si utiliza valores personalizados para las marcas de agua del volumen de almacenamiento, la alerta **anulación de Marca de agua de sólo lectura baja** puede activarse después de finalizar la actualización. Consulte Solucionar los problemas de las alertas de anulación de la Marca de agua de sólo lectura baja para obtener más detalles.

Una vez completada la actualización, puede revisar cualquier alerta relacionada con la actualización seleccionando **Alertas resueltas recientemente** o **Alertas actuales** en el Panel 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 notificaciones excesivas, anule la selección de la casilla de verificación **Activar notificaciones de agente SNMP** (**CONFIGURACIÓN** > **Supervisión** > **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

> La lista de cambios de configuración restringidos puede cambiar de una versión a otra. Cuando actualice a otra versión de StorageGRID, consulte la lista de las instrucciones de actualización correspondientes.

Hasta que finalice la tarea **Activar nueva función**:

- No realice ningún cambio en la configuración de la cuadrícula.
- No se debe cambiar la configuración de nivel de auditoría ni configurar un servidor de syslog externo.
- No active ni desactive ninguna nueva función.
- 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 cuadrícula.
- No puede gestionar grupos de alta disponibilidad, interfaces VLAN ni extremos de equilibrador de carga mientras se actualiza a StorageGRID 11.6.

Hasta que finalice la tarea **pasos de actualización final**:

- No realice un procedimiento de expansión.

- No realice un procedimiento de retirada de servicio.

No se pueden ver los detalles de los bloques ni gestionar los bloques desde el administrador de inquilinos

Durante la actualización a StorageGRID 11.6 (es decir, mientras el sistema está funcionando como un entorno de versión mixta), no se pueden ver detalles del bloque ni gestionar bloques con el administrador de inquilinos. Aparece uno de los siguientes errores en la página Cuches del Administrador de inquilinos:

- «'no puede utilizar esta API mientras actualiza a 11.6».
- "'no se pueden ver los detalles de control de versiones de bloques en el Gestor de inquilinos mientras se actualiza a 11.6.'"

Este error se resolverá una vez que se complete la actualización a la versión 11.6.

Solución alternativa

Mientras la actualización 11.6 está en curso, utilice las siguientes herramientas para ver detalles de bloques o gestionar bloques, en lugar de utilizar el Gestor de inquilinos:

- Para realizar operaciones estándar de S3 en un bloque, utilice la 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 el nivel de coherencia de bloques, habilitar o deshabilitar actualizaciones del tiempo de último acceso, o configurar la integración de búsqueda), use la API de gestión de inquilinos.

Consulte Comprender la API de gestión de inquilinos y.. Use S3 si desea obtener instrucciones.

Impacto de una actualización en grupos y cuentas de usuario

Debe comprender el impacto de la actualización de StorageGRID de modo que pueda actualizar los grupos y las cuentas de usuario según corresponda una vez completada la actualización.

Cambios en los permisos y opciones de grupo

Después de actualizar a StorageGRID 11.6, seleccione opcionalmente los siguientes permisos y opciones nuevos o actualizados (**CONFIGURACIÓN** > **control de acceso** > **grupos de administración**).

Permiso u opción	Descripción
Cuentas de inquilino	Además de permitir a los usuarios crear, editar y eliminar cuentas de arrendatario, este permiso ahora permite a los usuarios de administración ver las directivas de clasificación de tráfico existentes (**CONFIGURATION** > **Network** > **Traffic Classification**).

Consulte Gestione los grupos de administradores.

Comprobar la versión instalada de StorageGRID

Antes de iniciar la actualización, debe comprobar que la versión anterior de StorageGRID está actualmente instalada con la revisión más reciente disponible aplicada.

Acerca de esta tarea

Antes de actualizar a StorageGRID 11.6, el grid debe tener instalado StorageGRID 11.5. 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 la red sea StorageGRID 11.5.*x.y*.

En la 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.

Tenga en cuenta que puede ejecutar una secuencia de comandos para actualizar de 11.3.0.13+ a 11.4.0.*y* en un solo paso y de 11.4.0.7+ a 11.5.0.*y* en un solo paso. Consulte "Base de conocimientos de NetApp: Cómo ejecutar scripts combinados de actualizaciones importantes y revisiones para StorageGRID".

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. Compruebe que **Versión** es 11.5.*x.y*.

   En StorageGRID 11.5.*x.y* número de versión:

   - La **versión principal** tiene un valor *x* de 0 (11.5.0).
   - Una **revisión**, si se ha aplicado una, tiene un valor *y* (por ejemplo, 11.5.0.1).
4. Si **Versión** no es 11.5.*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 11.5 desde la versión 11.3.0.8

En el ejemplo siguiente se muestran los pasos para actualizar de StorageGRID versión 11.3.0.8 a la versión 11.5 como preparación para una actualización de StorageGRID 11.6.

> Opcionalmente, puede ejecutar una secuencia de comandos para combinar los pasos 2 y 3 (actualización de 11.3.0.13+ a 11.4.0.*y*) y combinar los pasos 4 y 5 (actualización de 11.4.0.7+ a 11.5.0.*y*). Consulte "Base de conocimientos de NetApp: Cómo ejecutar scripts combinados de actualizaciones importantes y revisiones para StorageGRID".

Descargue e instale software en la siguiente secuencia para preparar el sistema para la actualización:

1. Aplique la última revisión StorageGRID 11.3.0.*y*.
2. Actualice a la versión principal de StorageGRID 11.4.0.
3. Aplique la última revisión StorageGRID 11.4.0.*y*.

4. Actualice a la versión principal de StorageGRID 11.5.0.
5. Aplique la última revisión StorageGRID 11.5.0.*y*.

Obtenga los materiales necesarios para una actualización de software

Antes de iniciar la actualización de software, debe obtener todos los materiales necesarios para poder completar la actualización correctamente.

Elemento	Notas
Archivos de actualización de StorageGRID	Descargue los archivos de actualización de StorageGRID al ordenador portátil de servicio.
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.
Paquete de recuperación (`.zip`)	Descargue el paquete de recuperación antes de realizar la actualización y guardar el archivo en una ubicación segura. El archivo de paquete de recuperación permite restaurar el sistema si se produce un fallo.
`Passwords.txt` archivo	Este archivo se incluye en DICHO paquete, que forma parte del paquete de recuperación `.zip` archivo. Debe obtener la última versión del 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 aparece en la `Passwords.txt` archivo.
Documentación relacionada	• Notas de la versión Para StorageGRID 11.6. Asegúrese de leerlos detenidamente antes de iniciar la actualización. • Instrucciones para Administración de StorageGRID. • Si va a actualizar una implementación de Linux, las instrucciones de instalación de StorageGRID para su plataforma Linux: ◦ Instale Red Hat Enterprise Linux o CentOS ◦ Instalar Ubuntu o Debian • Según sea necesario, se ofrece otra documentación de StorageGRID.

Descargue los archivos de actualización de StorageGRID

Debe descargar uno o más archivos, según dónde estén instalados los nodos.

- **Todas las plataformas**: `.upgrade` archivo

Si alguno de los nodos se implementa en hosts Linux, también debe descargar un archivo RPM o DEB, que instalará antes de iniciar la actualización:

- **Red Hat Enterprise Linux o CentOS**: Un archivo RPM adicional (`.zip` o. `.tgz`)
- **Ubuntu o Debian**: Un archivo ADICIONAL DE DEB (`.zip` o. `.tgz`)

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 una instrucción Caution/MustRead, léala y active la casilla de verificación.

   Esta instrucción aparece si hay una revisión obligatoria para la versión.

5. Lea el contrato de licencia para 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:

   - Instale StorageGRID
   - Actualice StorageGRID
   - Admita archivos de dispositivos StorageGRID

6. En la columna **StorageGRID** de actualización, seleccione y descargue `.upgrade` archivado.

   Cada plataforma requiere el `.upgrade` archivado.

7. Si hay algún nodo implementado en hosts Linux, también descargue el archivo RPM o DEB en ninguno de los dos `.tgz` o. `.zip` formato. Seleccione la `.zip` Archivo si está ejecutando Windows en el portátil de servicio.

   - Red Hat Enterprise Linux o CentOS
     `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`

     No se requieren archivos adicionales para SG100 ni SG1000.

Descargue el paquete de recuperación

El archivo de paquete de recuperación permite restaurar el sistema StorageGRID en caso de producirse un fallo. 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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener la clave de acceso de aprovisionamiento.
- Debe tener permisos de acceso específicos.

Pasos

1. Seleccione **Mantenimiento** > **sistema** > **paquete de recuperación**.
2. Introduzca la frase de acceso de aprovisionamiento y seleccione **Iniciar descarga**.

   La descarga comienza inmediatamente.

3. Cuando finalice la descarga:
   a. Abra el `.zip` archivo.
   b. Confirme que incluye un `gpt-backup` directorio y un interior `.zip` archivo.
   c. Extraer el interior `.zip` archivo.
   d. Confirme que puede abrir 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.

Compruebe el estado del sistema

Antes de actualizar un sistema StorageGRID, es necesario comprobar que el sistema está listo para admitir la actualización. Debe asegurarse de que el sistema se ejecute con normalidad y que todos los nodos de grid estén operativos.

Pasos

1. Inicie sesión en Grid Manager mediante una navegador web compatible.
2. Compruebe y resuelva cualquier alerta activa.

   Para obtener información sobre alertas específicas, consulte Referencia de alertas.

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.

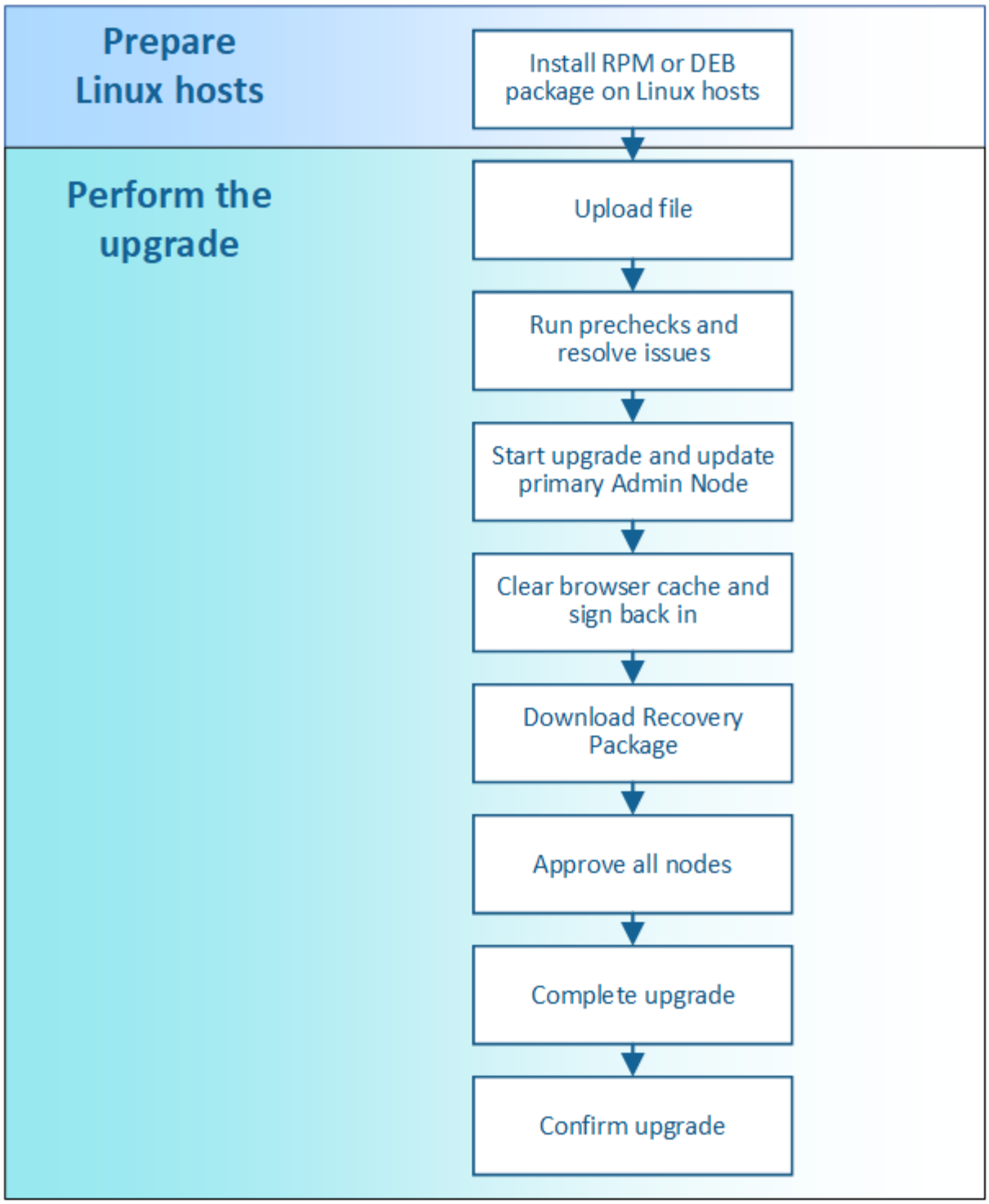
4. Consulte Comunicaciones internas de los nodos de grid y.. Comunicaciones externas Para garantizar que todos los puertos necesarios para StorageGRID 11.6 estén abiertos antes de actualizar.

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.

Actualice el software StorageGRID

Actualizar el flujo de trabajo

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. 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. Desde el nodo de administrador principal, acceda a la página StorageGRID Upgrade y cargue el archivo de actualización.
3. De forma opcional, ejecute comprobaciones previas de actualizaciones para detectar y resolver cualquier problema antes de iniciar la actualización real.
4. Inicie la actualización, que ejecuta comprobaciones previas y actualiza automáticamente el nodo de administrador principal. No se puede acceder a Grid Manager mientras se actualiza el nodo de administración principal. Además, los registros de auditoría no estarán disponibles. Esta actualización

puede llevar hasta 30 minutos.

5. Una vez que se haya actualizado el nodo de administración principal, borre la memoria caché del explorador web, vuelva a iniciar sesión y vuelva a la página de actualización de StorageGRID.
6. Descargue un nuevo paquete de recuperación.
7. Apruebe los nodos de la cuadrícula. 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 reiniciar.

8. Reanude 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 ampliación hasta que se hayan completado las tareas de base de datos **actualización** y los pasos de **actualización final**.
9. Una vez finalizada la actualización, confirme la versión del software y aplique cualquier revisión.

Información relacionada

Estime el tiempo para completar una actualización

Linux: Instale el paquete RPM o DEB en todos los hosts

Si hay nodos StorageGRID implementados en hosts Linux, debe instalar un paquete DE RPM o DEB adicional en cada uno de estos hosts antes de iniciar la actualización.

Lo que necesitará

Debe haber descargado una de las siguientes opciones `.tgz` o. `.zip` Archivos desde la página de descargas de NetApp para StorageGRID.

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

Plataforma Linux	Archivo adicional (elija uno)
Red Hat Enterprise Linux o CentOS	• `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`

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 host de StorageGRID en las instrucciones de instalación de la plataforma Linux.

   - Instale Red Hat Enterprise Linux o CentOS

- Instalar Ubuntu o Debian

Los nuevos paquetes se instalan como paquetes adicionales. No elimine los paquetes existentes.

Realice la actualización

Cuando esté listo para realizar la actualización, seleccione el `.upgrade` archive e introduzca la clave de acceso de aprovisionamiento. Como opción, puede ejecutar las comprobaciones previas de la actualización antes de realizar la actualización real.

Lo que necesitará

Ha revisado todas las consideraciones y completado todos los pasos de planificación y preparación.

Cargue el archivo de actualización

1. Inicie sesión en Grid Manager mediante una navegador web compatible.
2. Seleccione **Mantenimiento** > **sistema** > **actualización de software**.

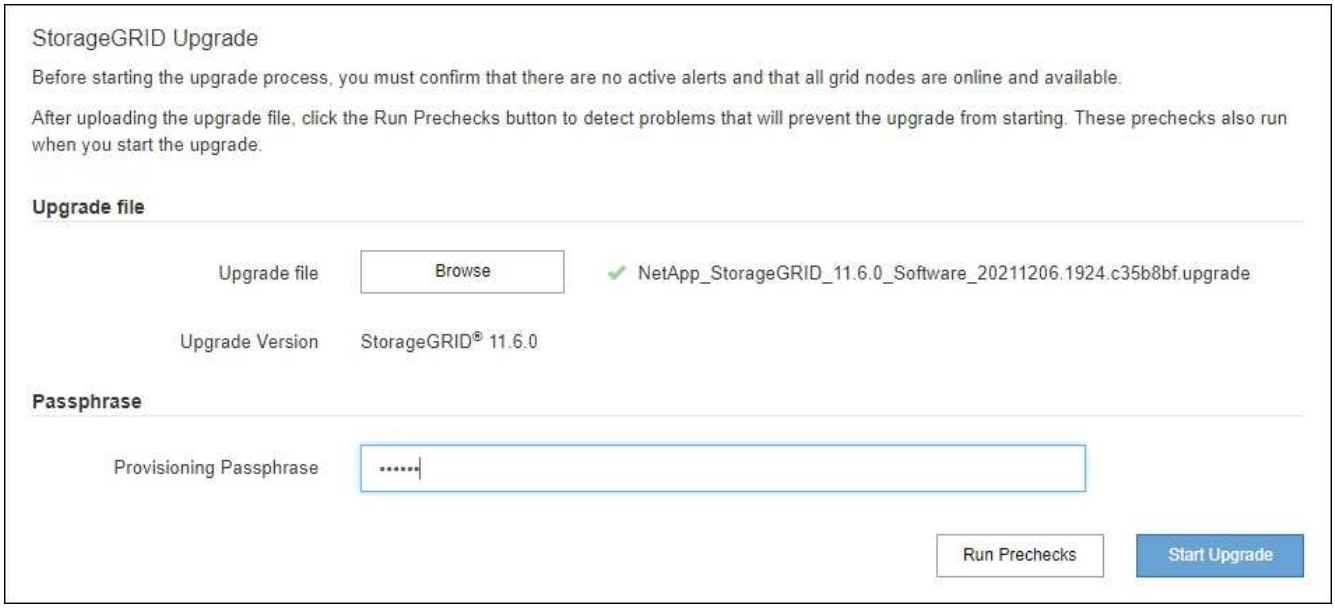
   Aparece la página actualización de software.

3. Seleccione **StorageGRID Upgrade**.
4. En la página StorageGRID Upgrade, seleccione el `.upgrade` archivado.
   a. Seleccione **examinar**.
   b. Localice y seleccione el archivo: `NetApp_StorageGRID_11.6.0_Software_uniqueID.upgrade`
   c. Seleccione **Abrir**.

      El archivo se carga y se valida. Cuando se realiza el proceso de validación, aparece una Marca de verificación verde junto al nombre del archivo de actualización.

5. Introduzca la clave de acceso de aprovisionamiento en el cuadro de texto.

   Los botones **Ejecutar comprobaciones previas** y **Iniciar actualización** se activan.



Realice comprobaciones previas

Opcionalmente, puede validar la condición del sistema antes de iniciar la actualización real. Seleccionar **Ejecutar comprobaciones previas** le permite detectar y resolver problemas antes de iniciar la actualización. Las mismas comprobaciones previas se realizan al iniciar la actualización. Los fallos de comprobación previa detendrán el proceso de actualización y podrían requerir la implicación del soporte técnico para solucionarlos.

1. Seleccione **Ejecutar comprobaciones previas**.
2. Espere a que se completen las comprobaciones previas.
3. Siga las instrucciones para resolver los errores de las comprobaciones previas notificados.

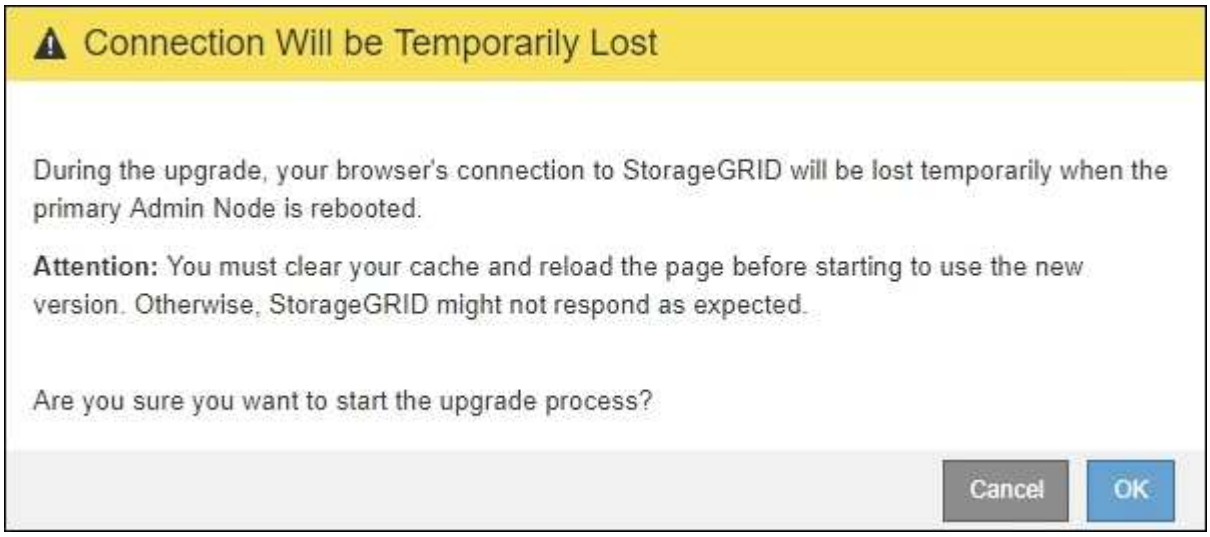
> Si ha abierto algún puerto de firewall personalizado, se le notificará durante la validación de las comprobaciones previas. Debe comunicarse con el soporte técnico antes de continuar con la actualización.

Inicie la actualización y actualice el nodo de administrador principal

Cuando se inicia la actualización, se realizan comprobaciones previas de actualización y se actualiza el nodo de administración principal, lo cual incluye detener servicios, actualizar el software y reiniciar servicios. No se puede acceder a Grid Manager mientras se actualiza el nodo de administración principal. Además, los registros de auditoría no estarán disponibles. Esta actualización puede llevar hasta 30 minutos.

1. Cuando esté listo para realizar la actualización, seleccione **Iniciar actualización**.

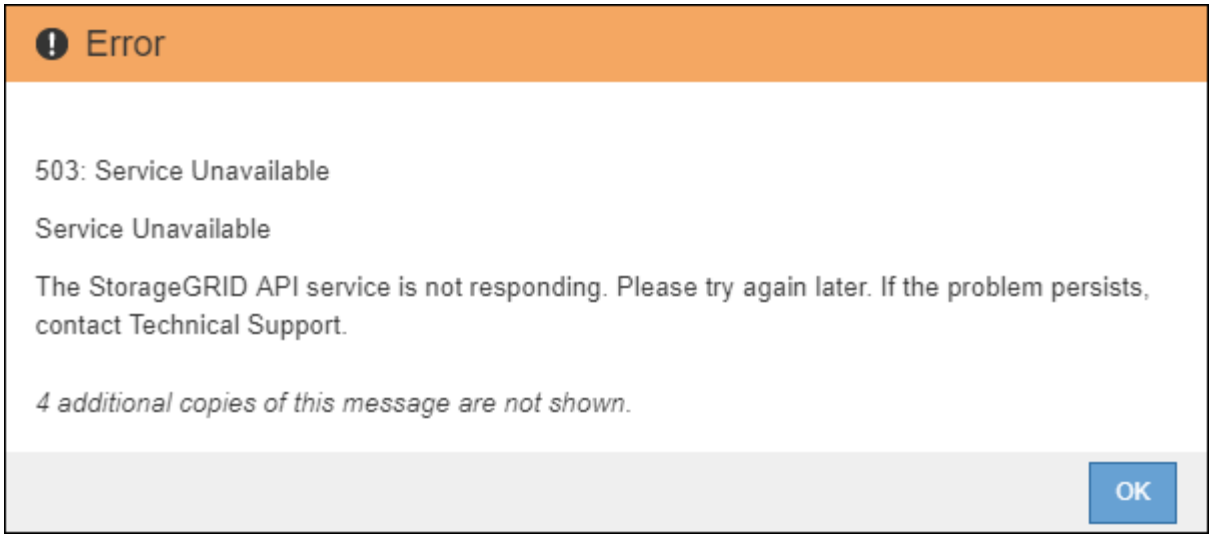
   Aparece una advertencia para recordarle que la conexión del explorador se perderá cuando se reinicie el nodo de administración principal.



2. Seleccione **Aceptar** para confirmar la advertencia e iniciar el proceso de 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 las comprobaciones previas, solucione y seleccione **Iniciar actualización** de nuevo.

   Mientras se está actualizando el nodo de administración principal, aparecen varios mensajes **503: Servicio no disponible** y **problema al conectar con el servidor**, que puede ignorar.



4. Cuando vea el mensaje **400: Bad Request**, vaya al paso siguiente. Se completó la actualización del nodo de administrador.

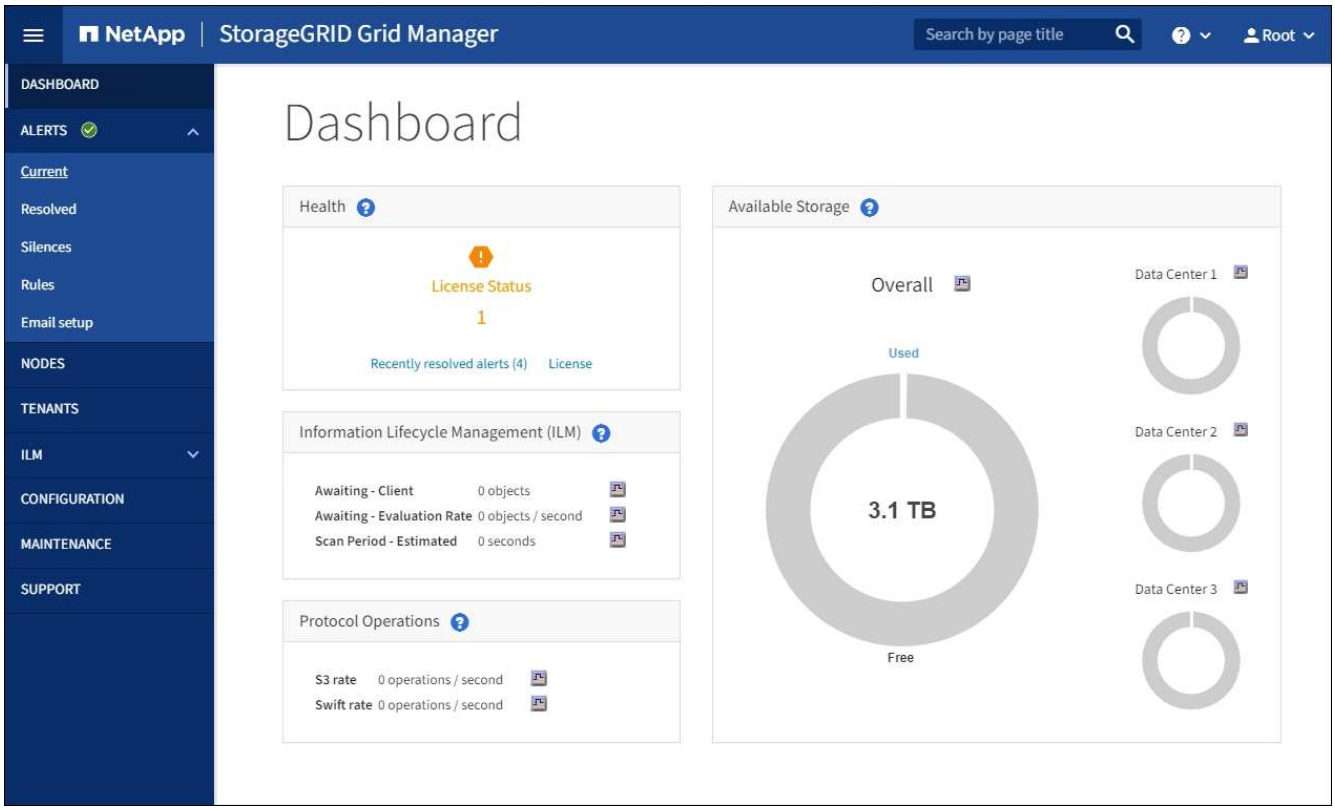
Borre la caché del navegador y vuelva a iniciar sesión

1. Una vez que se haya actualizado el nodo de administración principal, borre la memoria caché del explorador web y vuelva a iniciar sesión.

   Para obtener instrucciones, consulte la documentación de su navegador web.

Debe borrar el caché del explorador Web para eliminar los recursos obsoletos utilizados por la versión anterior del software.

Aparece la interfaz rediseñada de Grid Manager, que indica que se ha actualizado el nodo de administración principal.



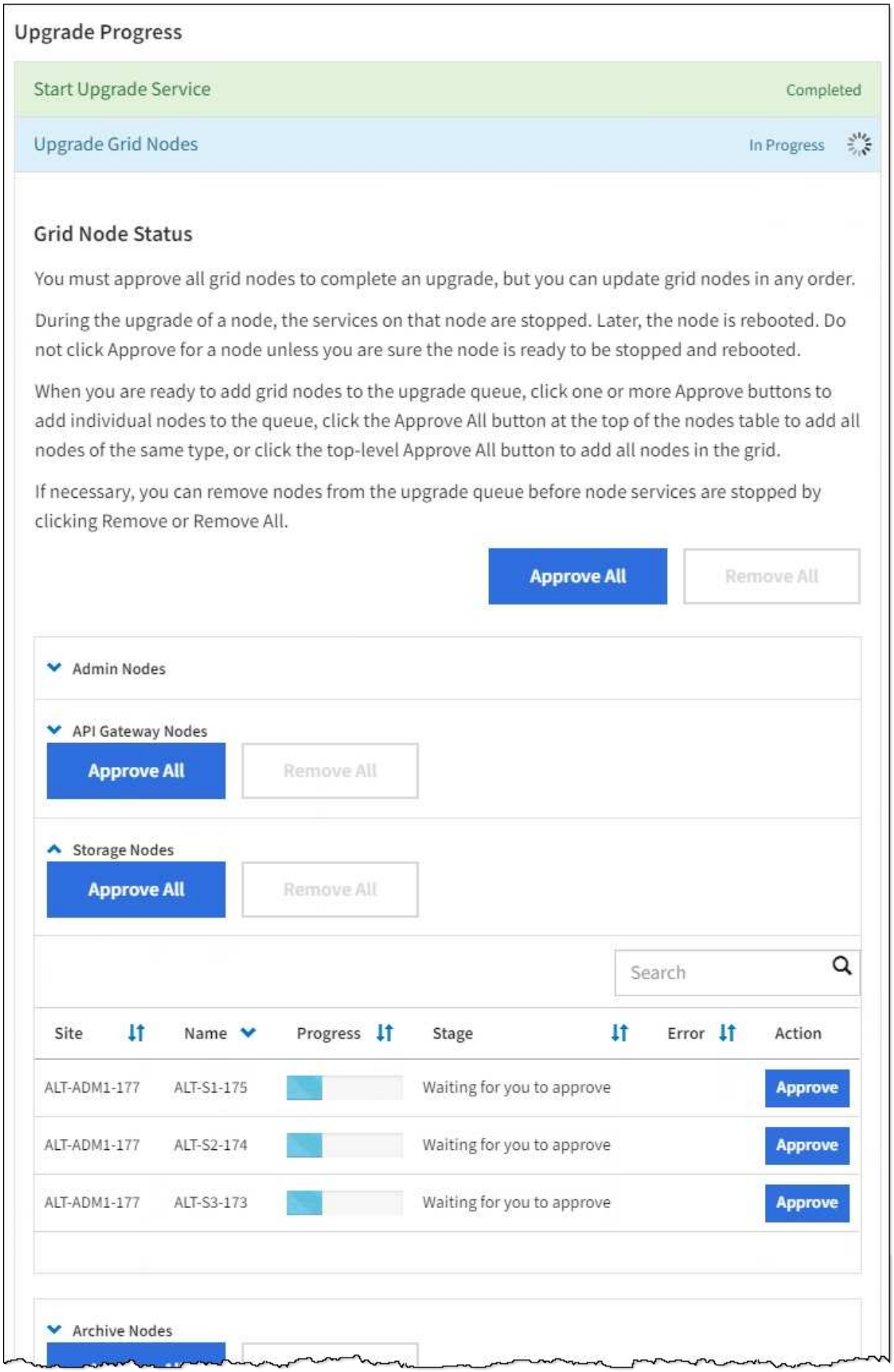
2. En la barra lateral, seleccione **MANTENIMIENTO** para abrir el menú Mantenimiento.
3. En la sección **sistema**, seleccione **actualización de software**.
4. En la sección **actualización de StorageGRID**, seleccione **actualización**.
5. Revise la sección progreso de la actualización en la página actualización de StorageGRID, que proporciona información acerca de cada tarea de actualización importante.
   a. **Iniciar servicio de actualización** es la primera tarea de actualización. Durante esta tarea, el archivo de software se distribuye a los nodos de grid y se inicia el servicio de actualización.
   b. Una vez completada la tarea **Iniciar servicio de actualización**, se inicia la tarea **Actualizar nodos de cuadrícula**.
   c. Mientras la tarea **Actualizar nodos de cuadrícula** está en curso, aparece la tabla Estado del nodo de cuadrícula y muestra la fase de actualización de cada nodo de cuadrícula del sistema.

Descargue el paquete de recuperación y actualice todos los nodos de grid

1. Una vez que los nodos de cuadrícula aparecen en la tabla Estado del nodo de cuadrícula, pero antes de aprobar los nodos de cuadrícula, Descargue una nueva copia del paquete de recuperación.

Debe descargar una nueva copia del archivo Recovery Package después de actualizar la versión de software en el nodo de administración principal. El archivo de paquete de recuperación permite restaurar el sistema si se produce un fallo.

2. Revise la información de la tabla Estado del nodo de cuadrícula. Los nodos de grid se organizan en secciones por tipo: Nodos de administrador, nodos de puerta de enlace de API, nodos de almacenamiento y nodos de archivado.


Upgrade Progress
Start Upgrade Service
Completed
Upgrade Grid Nodes
In Progress
Grid Node Status
You must approve all grid nodes to complete an upgrade, but you can update grid nodes in any order.
During the upgrade of a node, the services on that node are stopped. Later, the node is rebooted. Do not click Approve for a node unless you are sure the node is ready to be stopped and rebooted.
When you are ready to add grid nodes to the upgrade queue, click one or more Approve buttons to add individual nodes to the queue, click the Approve All button at the top of the nodes table to add all nodes of the same type, or click the top-level Approve All button to add all nodes in the grid.
If necessary, you can remove nodes from the upgrade queue before node services are stopped by clicking Remove or Remove All.
Approve All
Remove All
Admin Nodes
API Gateway Nodes
Approve All
Remove All
Storage Nodes
Approve All
Remove All
Search
Site
Name
Progress
Stage
Error
Action
ALT-ADM1-177
ALT-S1-175
Waiting for you to approve
Approve
ALT-ADM1-177
ALT-S2-174
Waiting for you to approve
Approve
ALT-ADM1-177
ALT-S3-173
Waiting for you to approve
Approve
Archive Nodes

Un nodo de cuadrícula puede estar en una de estas fases cuando aparece por primera vez esta página:

- Done (solo nodo de administración principal)
- Preparando actualización
- Descarga de software en cola
- Descarga
- Esperando a que usted apruebe

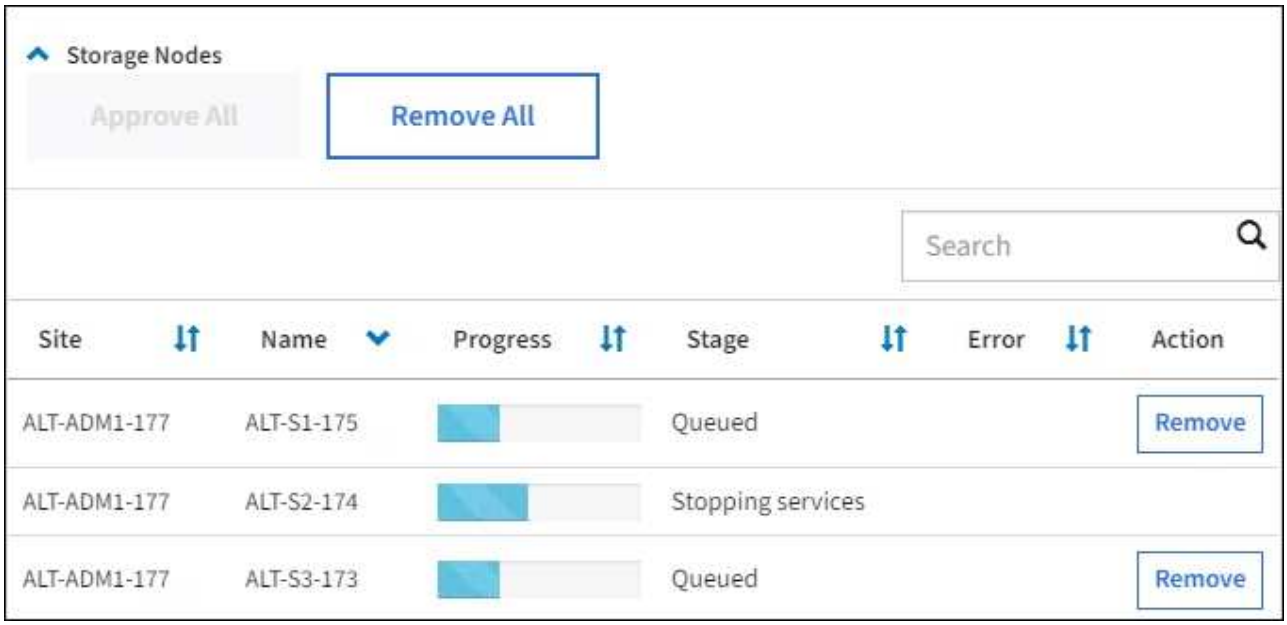
3. Apruebe los nodos de cuadrícula que está listo para agregar a la cola de actualización.

> 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 de servicio en 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.

Debe actualizar todos los nodos de grid en el sistema StorageGRID, pero se puede personalizar la secuencia de actualización. Puede aprobar nodos de cuadrícula individuales, grupos de nodos de cuadrícula o todos los nodos de cuadrícula.

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.

- Seleccione uno o más botones **aprobar** para agregar uno o más nodos individuales a la cola de actualización. Si aprueba más de un nodo del mismo tipo, los nodos se actualizarán de uno en uno.
- Seleccione el botón **aprobar todo** de cada sección para agregar todos los nodos del mismo tipo a la cola de actualización.
- Seleccione el botón * aprobar todo* de nivel superior para agregar todos los nodos de la cuadrícula a la cola de actualización.
- Seleccione **Quitar** o **Quitar todo** para eliminar un nodo o todos los nodos de la cola de actualización. No se puede quitar un nodo cuando su etapa alcanza **Servicios de parada**. El botón **Quitar** está oculto.



4. Espere a que cada nodo avance por las etapas de actualización, que incluyen Queued, servicios de detención, contenedor, limpieza de imágenes de Docker, actualización de paquetes de sistema operativo base, reinicio, ejecución de pasos después del reinicio, inicio de los servicios y realización de tareas.

> Cuando un nodo de dispositivo alcanza la fase actualizando paquetes de sistema operativo base, el software StorageGRID Appliance Installer del dispositivo se actualiza. Este proceso automatizado garantiza que la versión del instalador de dispositivos StorageGRID permanezca sincronizada con la versión del software StorageGRID.

Se completó la actualización

Una vez que todos los nodos de grid han completado las fases de actualización, la tarea **Actualizar nodos de grid** se muestra como completada. Las tareas de actualización restantes se realizan automáticamente y en segundo plano.

1. Tan pronto como la tarea **Activar características** esté completa (lo que se produce rápidamente), de forma opcional empezar a utilizar las nuevas características en la versión actualizada de StorageGRID.
2. Durante la tarea **base de datos de actualización**, el proceso de actualización comprueba cada nodo para verificar que la base de datos de Cassandra no necesita actualizarse.

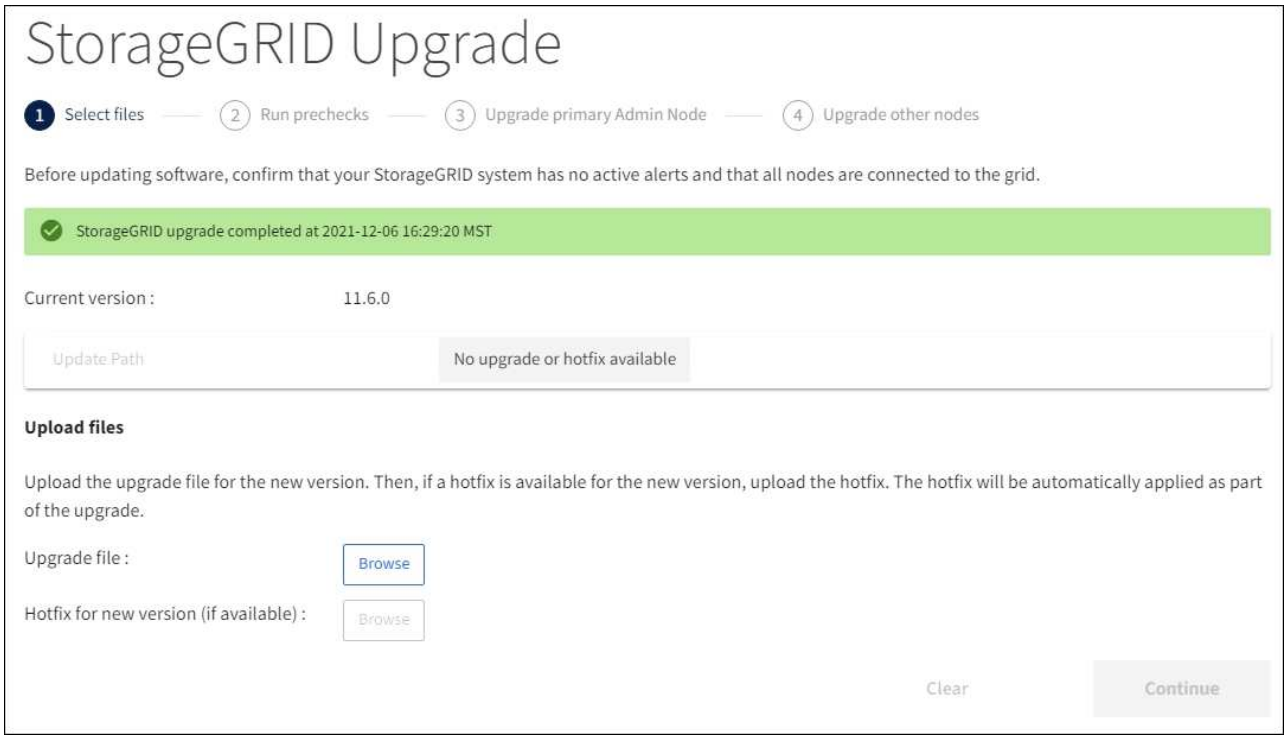
> La actualización de StorageGRID 11.5 a 11.6 no requiere una actualización de la base de datos de Cassandra; sin embargo, el servicio Cassandra se detendrá y reiniciará en cada nodo de almacenamiento. En las próximas versiones de la función StorageGRID, el paso de actualización de la base de datos de Cassandra podría tardar varios días en completarse.

3. Una vez completada la tarea **Actualizar base de datos**, espere unos minutos hasta que finalice la tarea **pasos de actualización final**.

   Una vez completada la tarea de pasos de actualización final, la actualización se realiza.

Confirme la actualización

1. Confirme que la actualización se completó correctamente.
   a. En la parte superior de Grid Manager, seleccione el icono de ayuda y seleccione **Acerca de**.
   b. Confirme que la versión que se muestra es lo que esperaría.
   c. Seleccione **MANTENIMIENTO** > **sistema** > **actualización de software**.
   d. En la sección **actualización de StorageGRID**, seleccione **actualización**.
   e. Confirme que el banner verde muestra que la actualización del software se ha completado en la fecha y la hora esperados.



2. En la página actualización de StorageGRID, determine si hay alguna revisión disponible para la versión actual de StorageGRID.

> Si no se muestra ninguna ruta de actualización, es posible que su navegador no pueda comunicarse con el sitio de soporte de NetApp. O bien, la casilla de verificación **Buscar actualizaciones de software** de la página AutoSupport (**SUPPORT** > **Tools** > **AutoSupport**) puede estar desactivada.

3. Si hay una revisión disponible, descargue el archivo. A continuación, utilice la Procedimiento de revisión de StorageGRID para aplicar la revisión.
4. 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

No se completó la actualización

Si la actualización no se realiza correctamente, es posible que pueda resolver el problema por su cuenta. Si no puede resolver un problema, debe recopilar la información necesaria antes de ponerse en contacto con el soporte técnico.

Las secciones siguientes describen cómo recuperar de situaciones en las que la actualización ha fallado parcialmente. Si no puede resolver un problema de actualización, póngase en contacto con el soporte técnico.

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. Si necesita ayuda, póngase en contacto con el soporte técnico.

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 recuperación de datos se interrumpe de forma inesperada cuando 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

Solucionar problemas de la interfaz de usuario

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

La interfaz Web no responde de la manera esperada

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

Si tiene problemas con la interfaz web:

- Asegúrese de utilizar un navegador 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 “Docker Image Availability check” (comprobación de disponibilidad de imagen Docker)

Al intentar iniciar el proceso de actualización, puede recibir un mensaje de error que indique ""los siguientes problemas fueron identificados por el paquete de validación de

comprobación de disponibilidad de imagen Docker"." Todos los problemas deben resolverse para poder 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.
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.

Aumentar el espacio reservado de metadatos

Después de actualizar a StorageGRID 11.6, es posible que pueda aumentar la configuración del sistema espacio reservado de metadatos si los nodos de almacenamiento cumplen con los requisitos específicos de la RAM y el espacio disponible.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener el permiso acceso raíz o los permisos Configuración de página de topología de cuadrícula y otros permisos Configuración de cuadrícula.
- Ha completado la actualización de StorageGRID 11.6.

Acerca de esta tarea

Es posible aumentar manualmente la configuración del espacio reservado de metadatos para todo el sistema hasta 8 TB después de actualizar a StorageGRID 11.6. Reservar espacio de metadatos adicional después de la actualización 11.6 simplificará las futuras actualizaciones de hardware y software.

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 la configuración de espacio reservado de metadatos afecta al espacio permitido para el almacenamiento de metadatos de objetos en un nodo de almacenamiento determinado, vaya a. Gestione el almacenamiento de metadatos de objetos.

Pasos

1. Inicie sesión en Grid Manager mediante una navegador web compatible.
2. 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**.
3. Asegúrese de tener suficiente espacio disponible en el volumen de almacenamiento 0 de cada nodo de almacenamiento para aumentar este valor.
   a. Seleccione **NODES**.

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.

4. Asegúrese de tener al menos 128 GB de RAM en cada nodo de almacenamiento.

   a. Seleccione **NODES**.

   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.

5. Actualice la configuración espacio reservado de metadatos.

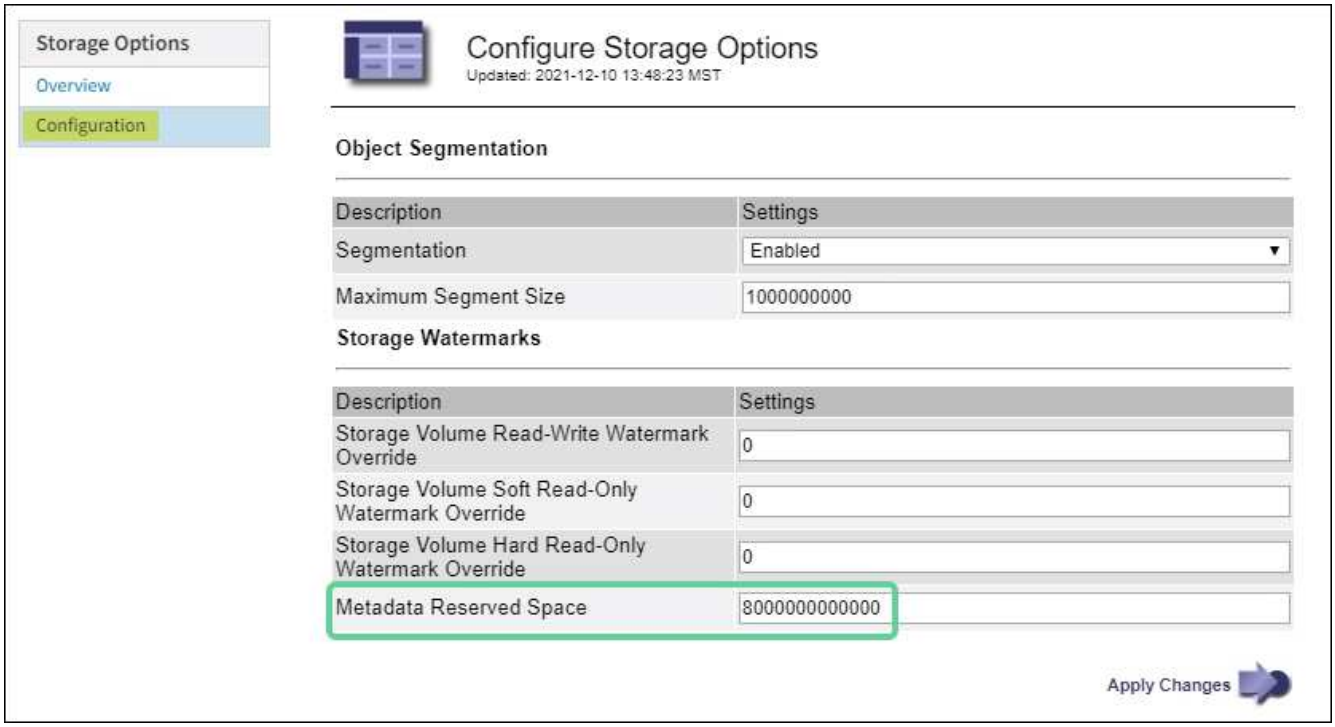
   a. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de almacenamiento**.

   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**.

Instale Red Hat Enterprise Linux o CentOS

Instale Red Hat Enterprise Linux o CentOS: Descripción general

La instalación de un sistema StorageGRID en un entorno Red Hat Enterprise Linux (RHEL) o CentOS Linux incluye tres pasos principales.

1. **Preparación**: Durante la planificación y preparación, realiza las siguientes tareas:
   - Conozca los requisitos de hardware y almacenamiento para StorageGRID.
   - Conozca los aspectos específicos de Redes StorageGRID de este modo, puede configurar la red de forma adecuada.
   - Identificar y preparar los servidores físicos o virtuales que planea usar para alojar los nodos de grid de StorageGRID.
   - En los servidores que ha preparado:
     - Instale Linux
     - Configure la red del host
     - Configurar el almacenamiento del host
     - Instalar el motor del contenedor
     - Instale los servicios host StorageGRID
2. **Implementación**: Implementar nodos de red utilizando la interfaz de usuario adecuada. Cuando se implementan nodos de grid, se crean como parte del sistema StorageGRID y se conectan a una o varias redes.
   a. Utilice los archivos de configuración de nodos y línea de comandos de Linux para implementar nodos de grid basados en software en los hosts que preparó en el paso 1.

b. Use el instalador de dispositivos StorageGRID para poner en marcha los nodos del dispositivo StorageGRID.

> El procedimiento de instalación de StorageGRID no incluye las instrucciones de instalación e integración específicas de hardware. Para aprender a instalar dispositivos StorageGRID, consulte las instrucciones de instalación y mantenimiento del dispositivo.

3. **Configuración**: Cuando se han implementado todos los nodos, utilice el administrador de grid para configurar la cuadrícula y completar la instalación.

Estas instrucciones recomiendan un método estándar para implementar y configurar un sistema StorageGRID. Consulte también la información acerca de los siguientes enfoques alternativos:

- Utilice un marco de orquestación estándar como Ansible, Puppet o Chef para instalar RHEL o CentOS, configurar redes y almacenamiento, instalar el motor de contenedores y el servicio de host de StorageGRID y poner en marcha nodos de grid virtual.
- Automatice la puesta en marcha y configuración del sistema StorageGRID mediante un script de configuración Python (incluido en el archivo de instalación).
- Automatice la puesta en marcha y configuración de los nodos del grid de los dispositivos con un script de configuración Python (disponible desde el archivo de instalación o desde el instalador de dispositivos de StorageGRID).
- Si es un desarrollador avanzado de implementaciones de StorageGRID, use las API DE REST de instalación para automatizar la instalación de los nodos de grid de StorageGRID.

Planificar y preparar la instalación de Red Hat o CentOS

Antes de instalar (Red Hat o CentOS)

Antes de implementar nodos de grid y configurar la cuadrícula de StorageGRID, debe estar familiarizado con los pasos y los requisitos para completar el procedimiento.

Los procedimientos de puesta en marcha y configuración de StorageGRID dan por sentado que está familiarizado con la arquitectura y el funcionamiento del sistema StorageGRID.

Puede implementar un solo sitio o varios sitios a la vez; sin embargo, todos los sitios deben cumplir con el requisito mínimo de tener al menos tres nodos de almacenamiento.

Antes de iniciar una instalación de StorageGRID, debe:

- Comprenda los requisitos de computación de StorageGRID, incluidos los requisitos mínimos de CPU y RAM para cada nodo.
- Comprenda cómo StorageGRID admite varias redes para la separación del tráfico, la seguridad y la comodidad administrativa. Además, tenga un plan para qué redes piensa conectar a cada nodo StorageGRID.

  Consulte las directrices para redes de StorageGRID.

- Comprenda los requisitos de almacenamiento y rendimiento de cada tipo de nodo 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.
- Comprenda los requisitos para la migración de nodos si desea realizar tareas de mantenimiento

programadas en hosts físicos sin ninguna interrupción del servicio.

- Recopile toda la información de la red con antelación. A menos que utilice DHCP, recopile las direcciones IP para asignar a cada nodo de grid y las direcciones IP de los servidores del sistema de nombres de dominio (DNS) y del protocolo de hora de red (NTP) que se utilizarán.
- Instale, conecte y configure todo el hardware necesario, incluidos los dispositivos StorageGRID, según las especificaciones.

> El procedimiento de instalación de StorageGRID no incluye las instrucciones de instalación e integración específicas de hardware. Para aprender a instalar dispositivos StorageGRID, consulte las instrucciones de instalación y mantenimiento del dispositivo.

- Decida qué herramientas de implementación y configuración disponibles desea utilizar.

Información relacionada

Directrices sobre redes

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG5600

Materiales requeridos

Antes de instalar StorageGRID, debe recopilar y preparar los materiales necesarios.

Elemento	Notas
Licencia de StorageGRID de NetApp	Debe tener una licencia de NetApp válida y con firma digital. **Nota**: En el archivo de instalación de StorageGRID se incluye una licencia de no producción, que puede utilizarse para probar y probar cuadrículas de concepto.
Archivo de instalación de StorageGRID	Debe 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

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

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 instrucción Caution/MustRead, léala y active 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 para 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 Red Hat Enterprise Linux o CentOS.

   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 RPM para instalar las imágenes de nodo StorageGRID en sus hosts RHEL o CentOS.

Ruta y nombre de archivo	Descripción
	PAQUETE RPM para instalar el servicio host StorageGRID en sus hosts RHEL o CentOS.
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.
	Un archivo de configuración en blanco para usar con el `configure-storagegrid.py` guión.
	Ejemplo de rol de Ansible y libro de estrategia para configurar hosts de RHEL o CentOS para puesta en marcha del contenedor StorageGRID. Puede personalizar el rol o el libro de estrategia según sea necesario.
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede utilizar estos esquemas para confirmar que cualquier código que haya escrito para utilizar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no dispone de un entorno StorageGRID que no sea de producción para la comprobación de compatibilidad de actualizaciones.

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.

Para obtener información sobre los servidores admitidos, consulte la matriz de interoperabilidad.

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 cómo gestionar el almacenamiento de metadatos de objetos, aumentar la configuración de espacio reservado de metadatos y supervisar el uso de la CPU y la memoria, consulte las instrucciones para administrar, supervisar 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 la información sobre los requisitos de almacenamiento.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Los requisitos de almacenamiento y rendimiento

Administre StorageGRID

Supervisión y solución de problemas

Actualizar el software de

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 no redundantes, SSD o JBOD. 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 de StorageGRID, debe almacenar tanto datos de sistema como datos de objetos en almacenamiento compartido.

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 los hosts que usan almacenamiento ONTAP de NetApp

Si el nodo StorageGRID utiliza almacenamiento asignado desde un sistema ONTAP de NetApp, confirme que el volumen no tiene habilitada la 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.

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 único 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.
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

> Según el nivel de auditoría configurado, el tamaño de las entradas de usuario, como el nombre de la clave de objeto S3 y la cantidad de datos del registro de auditoría que se deben conservar, es posible que deba aumentar el tamaño de la LUN del registro de auditoría de cada nodo de administración. Como regla general, un grid genera aproximadamente 1 KB de datos de auditoría por operación de S3, lo que significa que una LUN de 200 GB admitirá 70 millones de operaciones diarias 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 snapshots de disco no se pueden utilizar para restaurar nodos de grid. En su lugar, consulte los procedimientos de recuperación y mantenimiento de 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

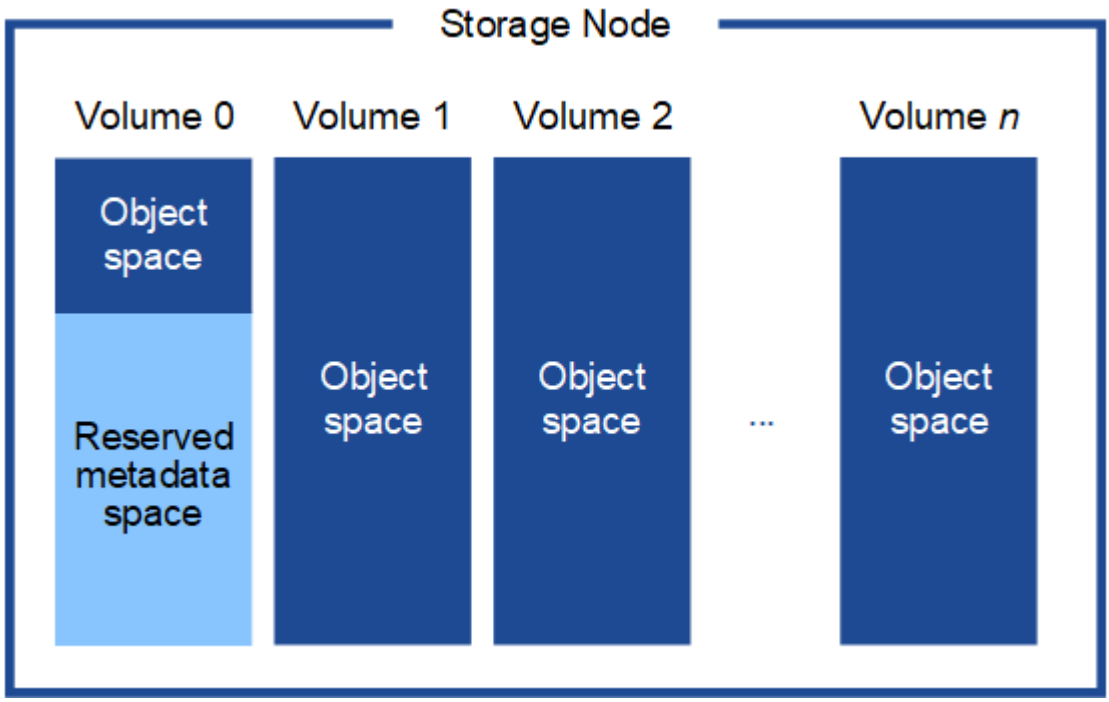
Tipo de nodo	Propósito de LUN	Número de LUN	Tamaño de LUN
Total		**9**	• Piscina de contenedores:* 300 GB **Datos del sistema:** 670 GB **Datos del objeto:** 12,000 GB

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 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 está instalando un nuevo sistema StorageGRID 11.6 y cada nodo de almacenamiento tiene 128 GB o más de RAM, debe asignar 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.

Información relacionada

Requisitos de migración de contenedores de nodos

Recuperación y mantenimiento

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. Solo tiene que mover todos los nodos 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 funcionalidad 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

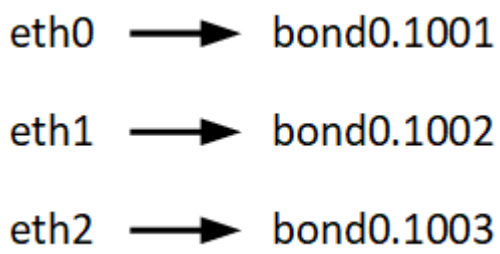
OpenStack Live Migration y VMware Live vMotion hacen que salte el tiempo del reloj de la máquina virtual y no son compatibles con los nodos de grid de ningún tipo. Aunque es poco frecuente, las horas de reloj incorrectas pueden provocar la pérdida de datos o actualizaciones de configuración.

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 de StorageGRID debe tener cierto grado de 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 poder realizar migraciones de nodos rápidas y con baja sobrecarga, la función de migración de nodos de StorageGRID no mueve físicamente los datos de nodos. 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 nodos'», se extrae una pequeña cantidad de datos de estado persistente del contenedor de nodos que se ejecuta en 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 "'node import'", se crea una instancia del contenedor de nodos en HostB que utiliza la misma interfaz de red y las asignaciones de almacenamiento de bloque que estaban en vigor en Hosta. 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.

/var/local → /dev/mapper/sgws-sn1-var-local

rangedb0 → /dev/mapper/sgws-sn1-rangedb0

rangedb1 → /dev/mapper/sgws-sn1-rangedb1

rangedb2 → /dev/mapper/sgws-sn1-rangedb2

rangedb3 → /dev/mapper/sgws-sn1-rangedb3

Herramientas de puesta en marcha

Podría beneficiarse de la automatización de toda la instalación de StorageGRID o de parte de ella.

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 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.

Si está interesado en automatizar toda la implementación de StorageGRID o una parte de ella, consulte Automatizar la instalación antes de iniciar el proceso de instalación.

Preparar los hosts (Red Hat o CentOS)

Instale Linux

Debe instalar Linux en todos los hosts Grid. Utilice la "Herramienta de matriz de interoperabilidad de NetApp" para obtener una lista de las versiones compatibles.

Pasos

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

> En el caso de que utilice el instalador Linux estándar, NetApp recomienda seleccionar la configuración del software «nodo informático», si está disponible, o el entorno base «instalación decimal». 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 o CentOS)

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.

Lo que necesitará

- 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 los nodos ni entre el host y ningún 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 sus hosts son máquinas virtuales y va a implementar uno o dos nodos de StorageGRID para cada host, puede simplemente crear el número correcto de interfaces de red en el hipervisor y utilizar 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 método que satisfaga sus necesidades.

> No utilice dispositivos de enlace o puente directamente como interfaz de red de contenedores. 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, más bien, permite que todas las interfaces reciban y transmitan datos para direcciones MAC distintas a las asignadas por el hipervisor, Asegúrese de que las propiedades de seguridad de los niveles de conmutador virtual y grupo de puertos están configuradas en **Aceptar** para modo promiscuous, cambios de dirección MAC y señales falsificadas. Los valores establecidos en el conmutador virtual pueden ser anulados por los valores en el nivel de grupo de puertos, por lo que asegúrese de que la configuración sea la misma en ambos lugares.

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

Ejemplo de clonación EN MAC

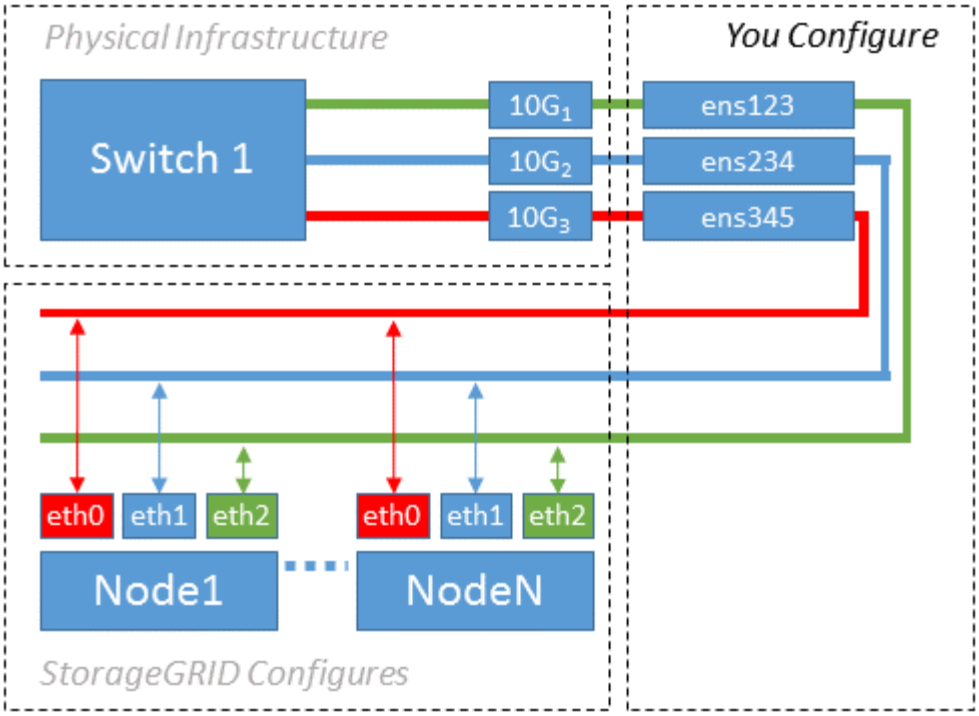
Ejemplo de clonación MAC habilitada con un host que tiene la dirección MAC 11:22:33:44:55:66 para la interfaz ens256 y las siguientes claves en el archivo de configuración del nodo:

- `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

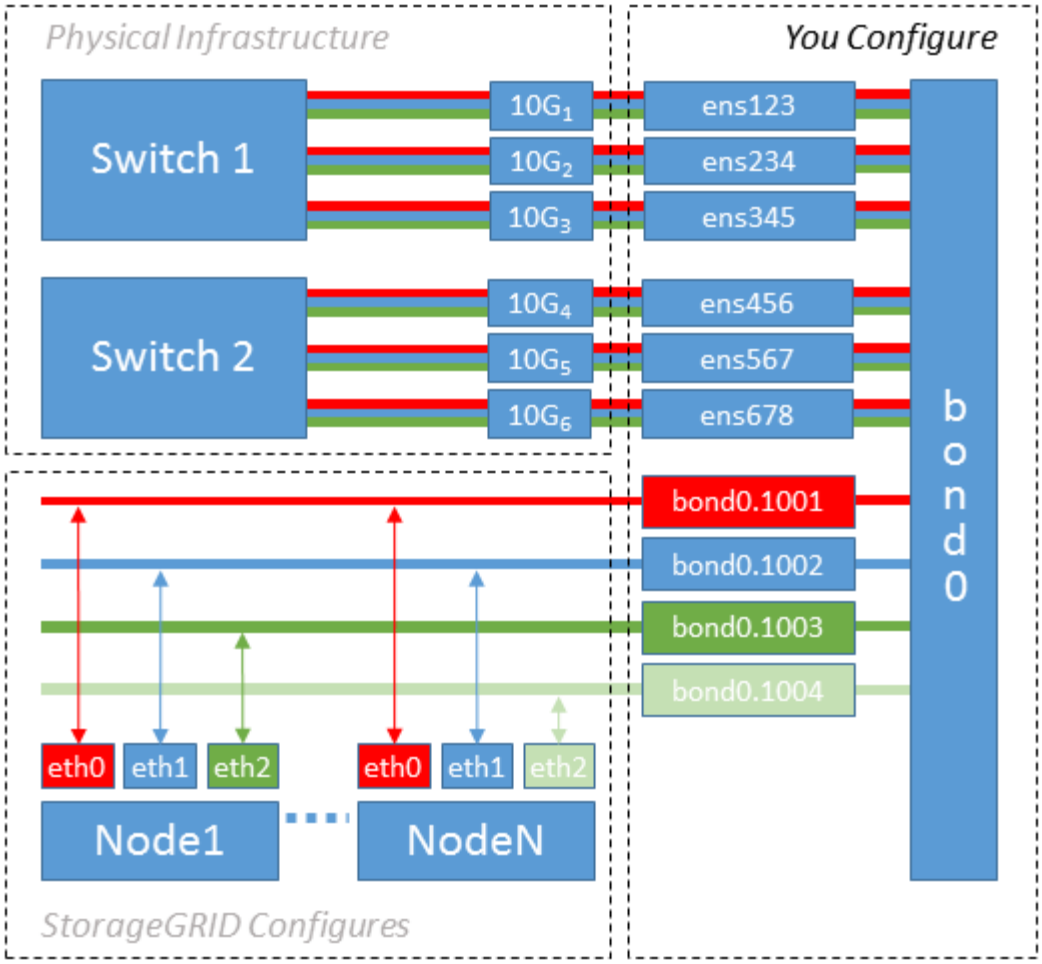
Acerca de esta tarea

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," `using the standard VLAN interface naming convention` `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.

Lo que necesitará

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

Al asignar volúmenes de almacenamiento en bloque (LUN) a los hosts, utilice las tablas de «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 realizar particiones, formatear ni montar ninguno de estos volúmenes; solo tiene que asegurarse de que son visibles para los hosts.

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 de iSCSI y accesos múltiples de asignación de dispositivos, considere la posibilidad de utilizar alias multivía en el `/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 configura un almacenamiento compartido para que sea compatible con la migración de nodos StorageGRID y con la función multivía 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 o CentOS como 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 cliente y servidor deben ser 3.2.3 o posterior.

```
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 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.

Ponga en marcha nodos de grid virtual (Red Hat o CentOS)

Crear archivos de configuración de nodos para implementaciones de Red Hat Enterprise Linux o CentOS

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 los nodos se usan para los nodos virtuales y no se usan para los nodos del dispositivo.

¿Dónde se colocan los archivos de configuración del nodo?

Debe colocar el archivo de configuración para 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.

¿Qué nombre tienen los archivos de configuración del nodo?

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 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.

¿Qué hay en un archivo de configuración de nodo?

Los archivos de configuración contienen pares clave/valor, con una clave y un valor por línea. Para cada par clave/valor, debe seguir 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.

Algunas claves son necesarias para cada nodo, mientras que otras son opcionales o solo necesarias para ciertos tipos de nodo.

La tabla define los valores aceptables para todas las claves admitidas. En la columna central:

R: Requerido + BP: Mejor práctica + o: Opcional

Clave	¿R, BP O O?	Valor
IP_ADMINISTRADOR	BP	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.
ADMIN_NETWORK_CONFIG	O	DHCP, ESTÁTICO O DESHABILITADO
ADMIN_NETWORK_ESL	O	Lista de subredes separadas por comas en la notación CIDR a la que este nodo se debe comunicar a través de la puerta de enlace de red de administración. Ejemplo: `172.16.0.0/21,172.17.0.0/21`

ADMIN_NETWORK_GATEWAY	O (**R**)	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.
		
		Nota: Este parámetro es necesario si SE especifica ADMIN_NETWORK_ESL.
		
		Ejemplos:
		
		`1.1.1.1`
		
		`10.224.4.81`

Clave	¿R, BP O O?	Valor

IP_RED_ADMIN	O	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`

ADMIN_NETWORK_MAC	O	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`

ADMIN_NETWORK_MASK	O	La máscara de red IPv4 para este nodo, en la red de administrador. Esta clave solo es necesaria cuando ADMIN_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
		
		Ejemplos:
		
		`255.255.255.0`
		
		`255.255.248.0`

Clave	¿R, BP O O?	Valor

MTU_RED_ADMIN	O	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 usa 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`

ADMIN_NETWORK_TARGET	BP	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 destino 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`

ADMIN_NETWORK_TARGET_TYPE	O	Interfaz (Este es el único valor admitido).

Clave	¿R, BP O O?	Valor
ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	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 o CentOS) Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)
ADMIN_ROLE	**R**	Primario o no primario Esta clave solo es necesaria cuando NODE_TYPE = VM_Admin_Node; no la especifique para otros tipos de nodos.

BLOCK_DEVICE_AUDIT_LOGS	**R**	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. Esta clave solo es necesaria para nodos con NODE_TYPE = VM_Admin_Node; no la especifique para otros tipos de nodo.
		
		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`

Clave	¿R, BP O O?	Valor

BLOCK_DEVICE_RANGEDB_000
 	
BLOCK_DEVICE_RANGEDB_001
 	
BLOCK_DEVICE_RANGEDB_002
 	
BLOCK_DEVICE_RANGEDB_003
 	
BLOCK_DEVICE_RANGEDB_004
 	
BLOCK_DEVICE_RANGEDB_005
 	
BLOCK_DEVICE_RANGEDB_006
 	
BLOCK_DEVICE_RANGEDB_007
 	
BLOCK_DEVICE_RANGEDB_008
 	
BLOCK_DEVICE_RANGEDB_009
 	
BLOCK_DEVICE_RANGEDB_010
 	
BLOCK_DEVICE_RANGEDB_011
 	
BLOCK_DEVICE_RANGEDB_012
 	
BLOCK_DEVICE_RANGEDB_013
 	
BLOCK_DEVICE_RANGEDB_014
 	
BLOCK_DEVICE_RANGEDB_015
	R	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 nodos con NODE_TYPE = VM_Storage_Node; no la especifique para otros tipos de nodo.
		
		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. 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`

Clave	¿R, BP O O?	Valor

BLOCK_DEVICE_TABLES	**R**	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 nodos con NODE_TYPE = VM_Admin_Node; no la especifique para otros tipos de nodo.
		
		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`

BLOCK_DEVICE_VAR_LOCAL	**R**	Ruta y nombre del archivo especial del dispositivo de bloque que este nodo utilizará para su almacenamiento persistente /var/local.
		
		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`

CLIENT_NETWORK_CONFIG	O	DHCP, ESTÁTICO O DESHABILITADO

PUERTA_DE_ENLACE_RED_CLIENTE	O	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`

Clave	¿R, BP O O?	Valor

IP_RED_CLIENTE	O	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`

MAC_RED_CLIENTE	O	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`

MÁSCARA_RED_CLIENTE	O	La máscara de red IPv4 para este nodo en la red de cliente. Esta clave solo es necesaria cuando CLIENT_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
		
		Ejemplos:
		
		`255.255.255.0`
		
		`255.255.248.0`

Clave	¿R, BP O O?	Valor

MTU_RED_CLIENTE	O	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 usa 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`

DESTINO_RED_CLIENTE	BP	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 destino 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`

CLIENT_NETWORK_TARGET_TYPE	O	Interfaz (Solo se admite este valor).

Clave	¿R, BP O O?	Valor
CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	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 o CentOS) Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)
GRID_NETWORK_CONFIG	BP	ESTÁTICO o DHCP (De forma predeterminada, ES ESTÁTICO si no se especifica.)
PUERTA_DE_ENLACE_RED_GRID	**R**	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.

IP_RED_GRID	**R**	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`

Clave	¿R, BP O O?	Valor
MAC_RED_GRID	O	La dirección MAC de la interfaz de red de red del 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:c2:27:30`

GRID_NETWORK_MASK	O	Máscara de red IPv4 para este nodo en la red de cuadrícula. Esta clave solo es necesaria cuando GRID_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
		
		Ejemplos:
		
		`255.255.255.0`
		
		`255.255.248.0`

MTU_RED_GRID	O	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 usa 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. Los valores de MTU no tienen que ser iguales para todos los tipos de red. Ejemplos: 1500 8192

Clave	¿R, BP O O?	Valor

GRID_NETWORK_TARGET	**R**	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 destino 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`

GRID_NETWORK_TARGET_TYPE	O	Interfaz (Este es el único valor admitido).
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	**BP**	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 o CentOS) Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)

Clave	¿R, BP O O?	Valor
INTERFACES_TARGET_nnnn	O	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_DESTINO_INTERFACES que esté agregando. 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. Por ejemplo: `INTERFACES_TARGET_01=ens256, Trunk` Si añade una interfaz troncal, debe configurar una interfaz VLAN en StorageGRID. Si agrega una interfaz de acceso, puede agregar la interfaz directamente a un grupo de alta disponibilidad; no es necesario configurar una interfaz de VLAN.

RAM_MÁXIMA	O	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 Instrucciones para administrar StorageGRID Para obtener una descripción de lo que es el espacio reservado de metadatos.
		
		El formato de este campo es `<number><unit>`, 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.

TIPO_NODO	**R**	Tipo de nodo: VM_Admin_Node VM_Storage_Node VM_Archive_Node VM_API_Gateway

Clave	¿R, BP O O?	Valor
REASIGNAR_PUERTO	O	Reasigna cualquier puerto que usa un nodo para las comunicaciones internas del nodo de grid o las comunicaciones externas. Es necesario volver a asignar puertos si las políticas de red de la empresa restringen uno o más puertos utilizados por StorageGRID, como se describe en «'Comunicaciones internas de nodos de grid» o «'Comunicaciones externas». **IMPORTANTE**: No reasigne los puertos que va a utilizar para configurar puntos finales de 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 el protocolo es tcp o udp. Por ejemplo: `PORT_REMAP = client/tcp/18082/443`
PORT_REMAPP_INBOUND	O	Reasigna las comunicaciones entrantes al puerto especificado. Si especifica PORT_REMAPP_INBOUND pero no especifica un valor para PORT_REMAPP, las comunicaciones salientes para el puerto no se modifican. **IMPORTANTE**: No reasigne los puertos que va a utilizar para configurar puntos finales de 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 el protocolo es tcp o udp. Por ejemplo: `PORT_REMAP_INBOUND = grid/tcp/3022/22`

Información relacionada

Directrices sobre redes

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 normalmente a través de 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.

```
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
```

Para cualquier nodo que devuelva un estado de "'no en ejecución'" o "encabezado", ejecute el siguiente comando:

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

3. 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 red y completar la instalación (Red Hat o CentOS)

Desplácese hasta Grid Manager

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

Lo que necesitará

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
```

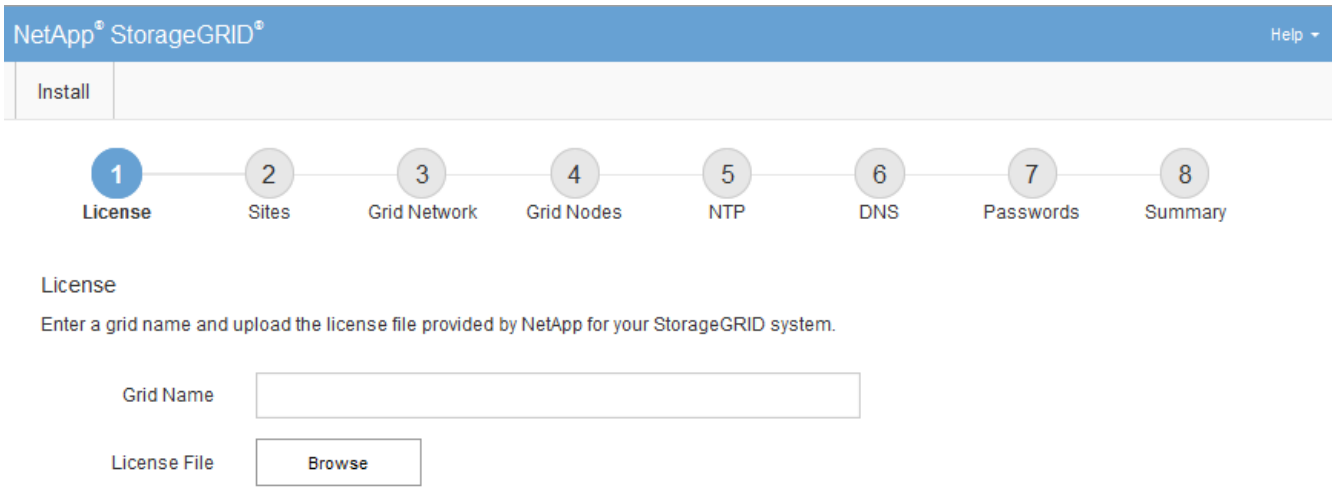
También puede acceder a Grid Manager en el puerto 8443:

```
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.

1. Haga clic en **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

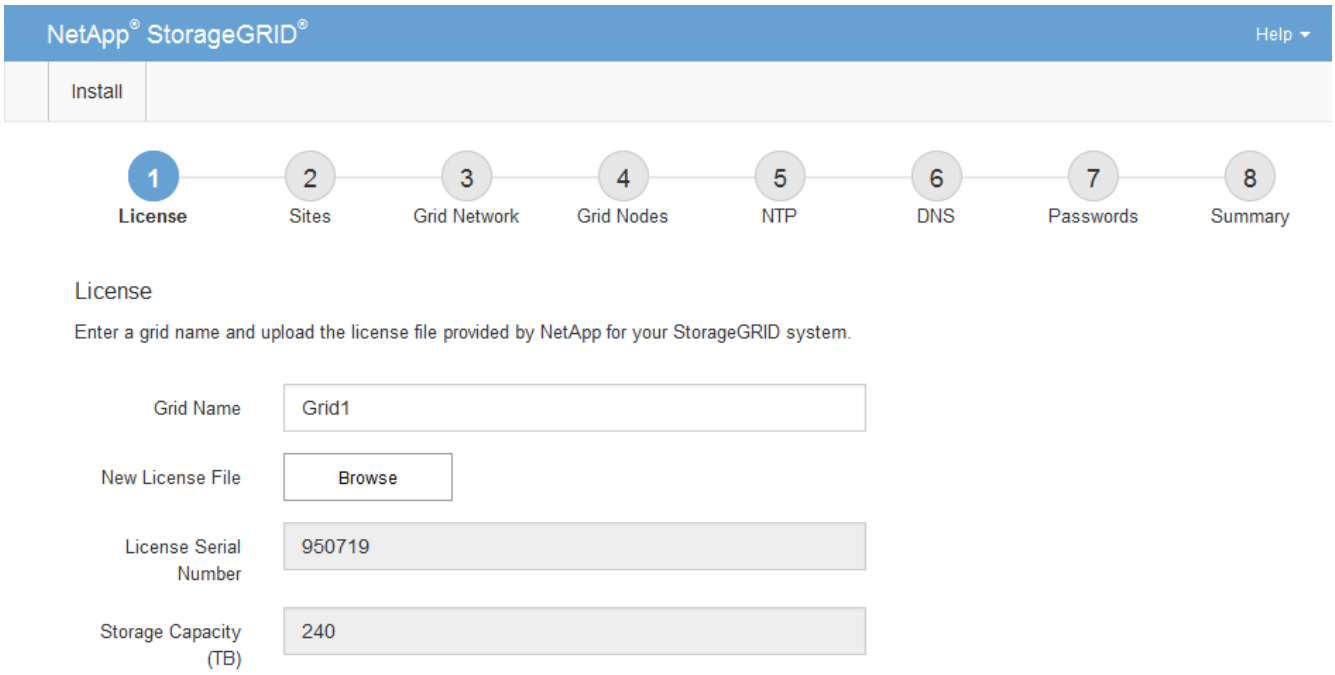
1. En la página Licencia, introduzca un nombre significativo para su sistema StorageGRID en **Nombre de cuadrícula**.

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

2. Haga clic en **Browse**, busque el archivo de licencia de NetApp (`NLFunique_id.txt`) Y haga clic en **Abrir**.

   El archivo de licencia se valida y se muestran el número de serie y la capacidad de almacenamiento con licencia.

   > 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. Haga clic en **Siguiente**.

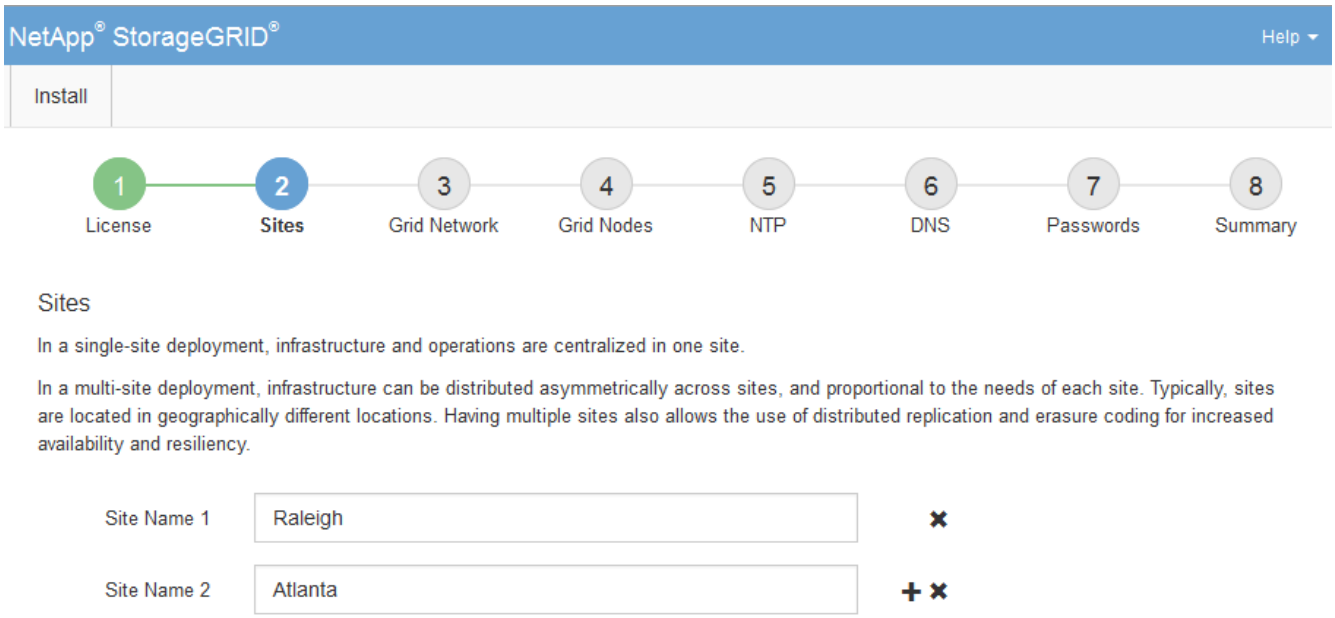
Agregar sitios

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

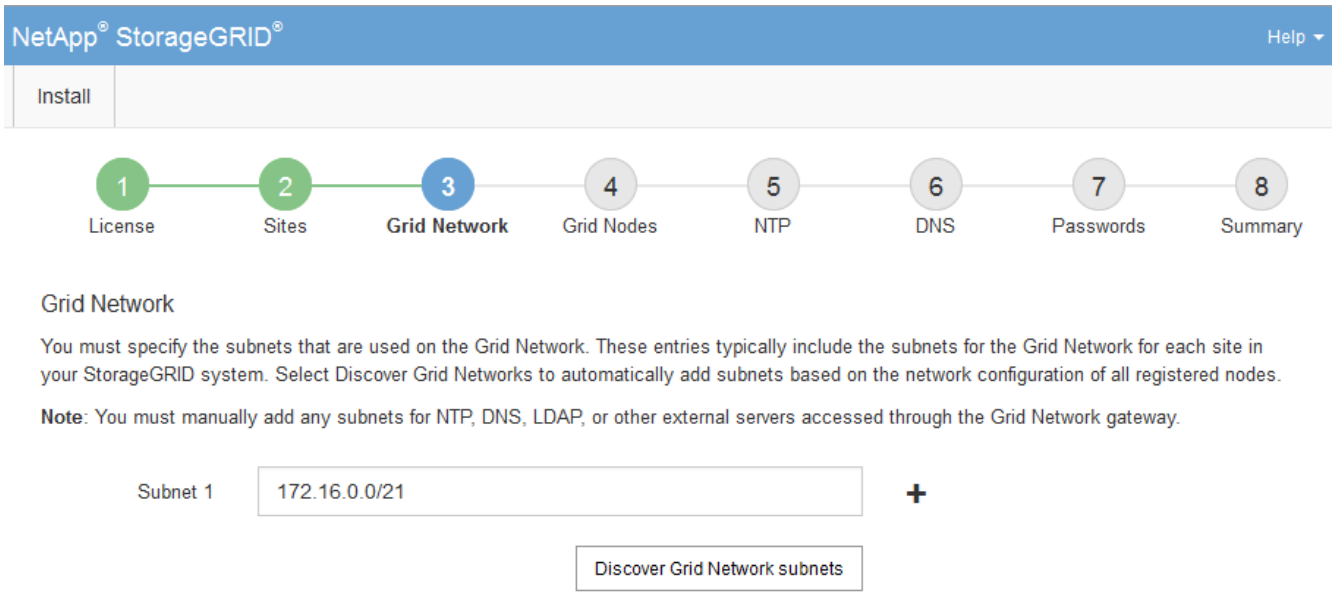
Las entradas de subred incluyen las subredes para la red de cuadrícula de cada sitio del sistema StorageGRID, junto con las subredes a las que se debe acceder a través de la red de cuadrícula.

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.

Lo que necesitará

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

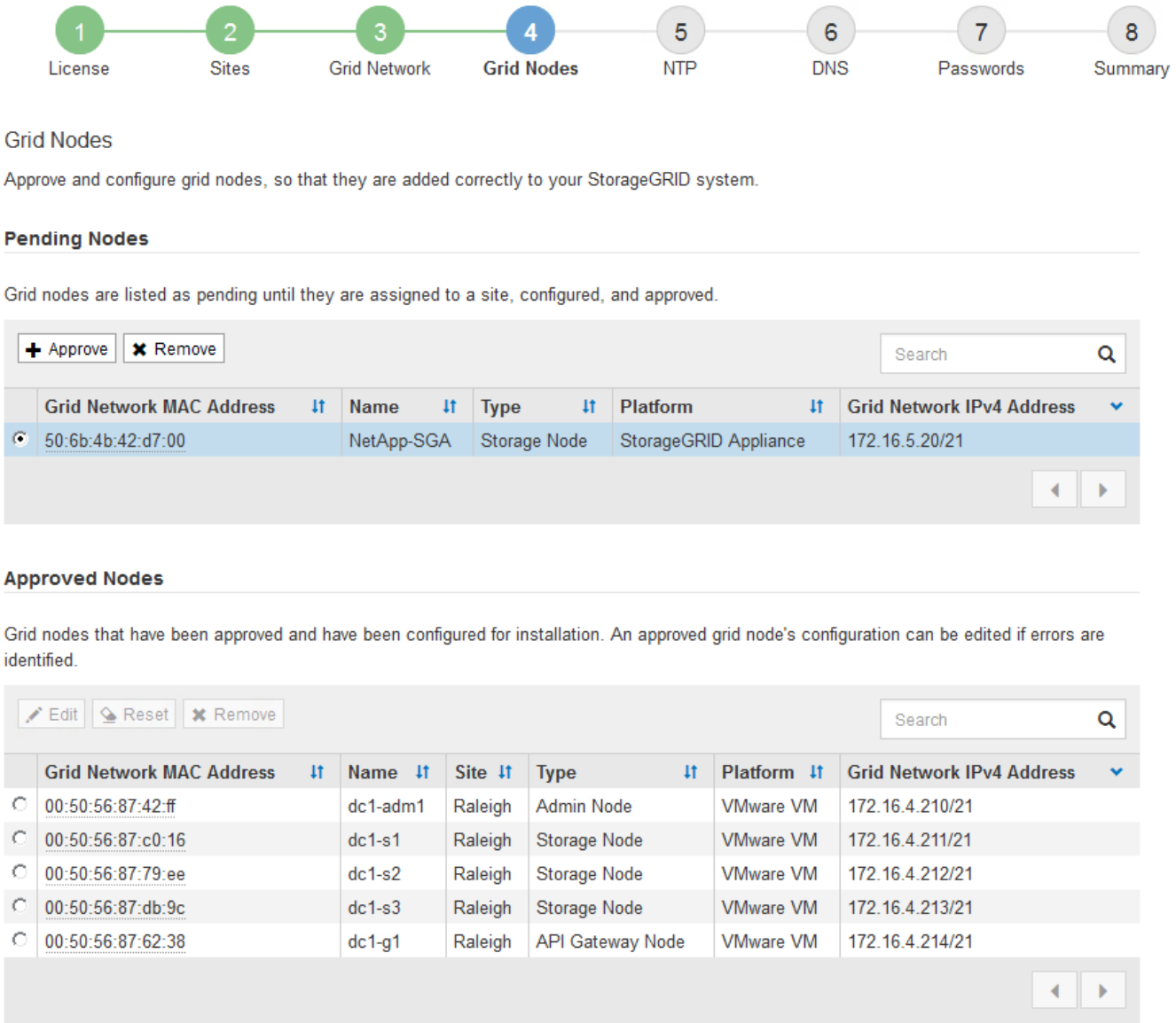
> Es más eficiente realizar una instalación única de todos los nodos, en lugar de instalar algunos ahora y algunos nodos más adelante.

Pasos

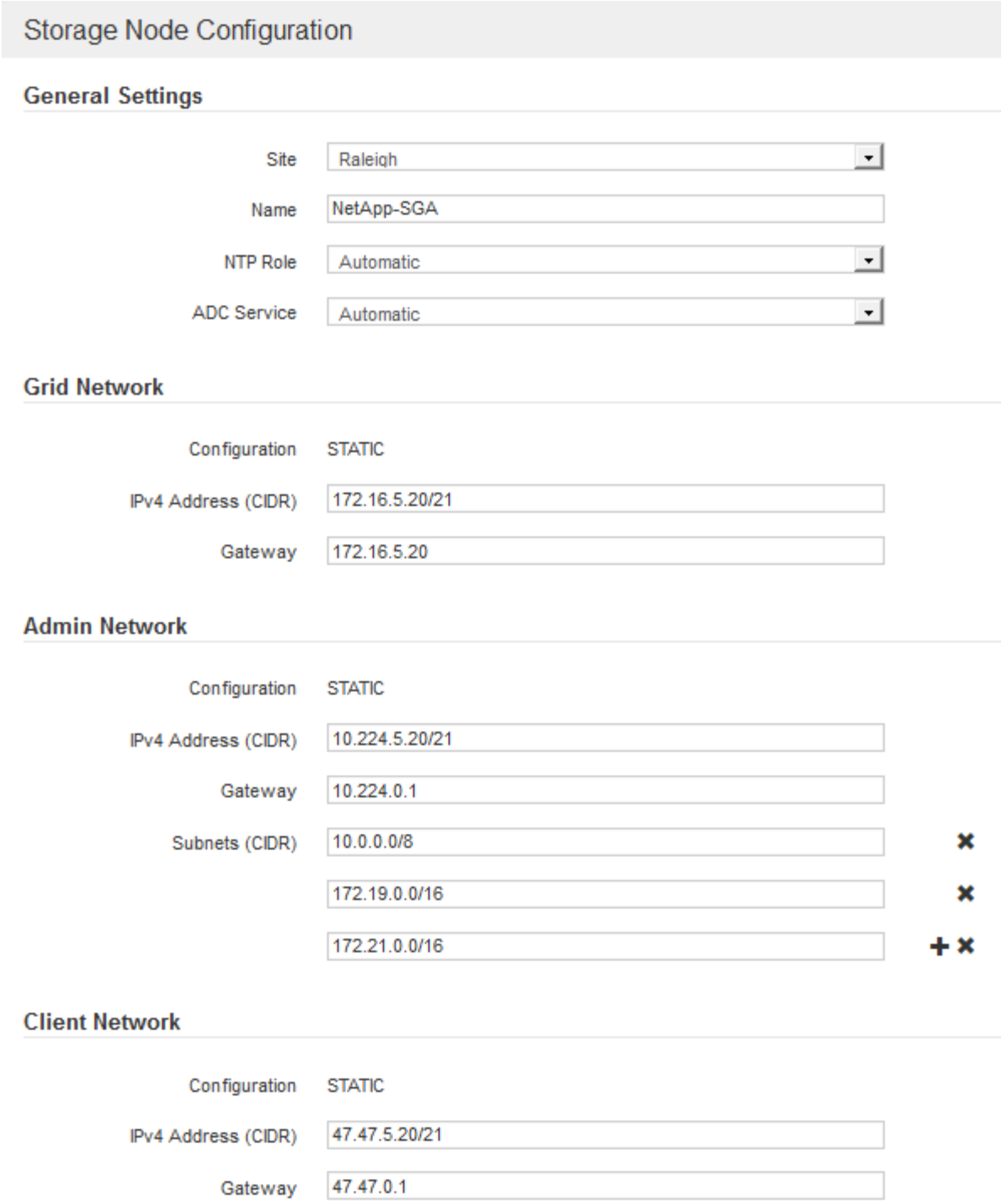
1. Revise la lista Pending Nodes y confirme que se muestran todos los nodos de grid que ha implementado.

   > 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 sitio con el que se asociará este nodo de red.
- **Nombre**: El nombre que se asignará al nodo y el nombre que se mostrará en el Gestor de cuadrícula. El nombre predeterminado es el nombre que especifique cuando configure el nodo. Durante este paso del proceso de instalación, puede cambiar el nombre según sea necesario.

> Una vez finalizada la instalación, no puede cambiar el nombre del nodo.

> 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.

- **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 haberlo implementado.

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 del 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 el Gestor de cuadrícula: Si el nodo aparece en la tabla nodos aprobados, restablezca 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 IP Configuration.

   Para obtener información adicional, consulte las instrucciones de instalación y mantenimiento del 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.

   Dispositivos: 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 del 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 el Gestor de cuadrícula: Si el nodo aparece en la tabla nodos aprobados, restablezca el nodo.

   f. Quite el nodo de la tabla Pending Nodes.

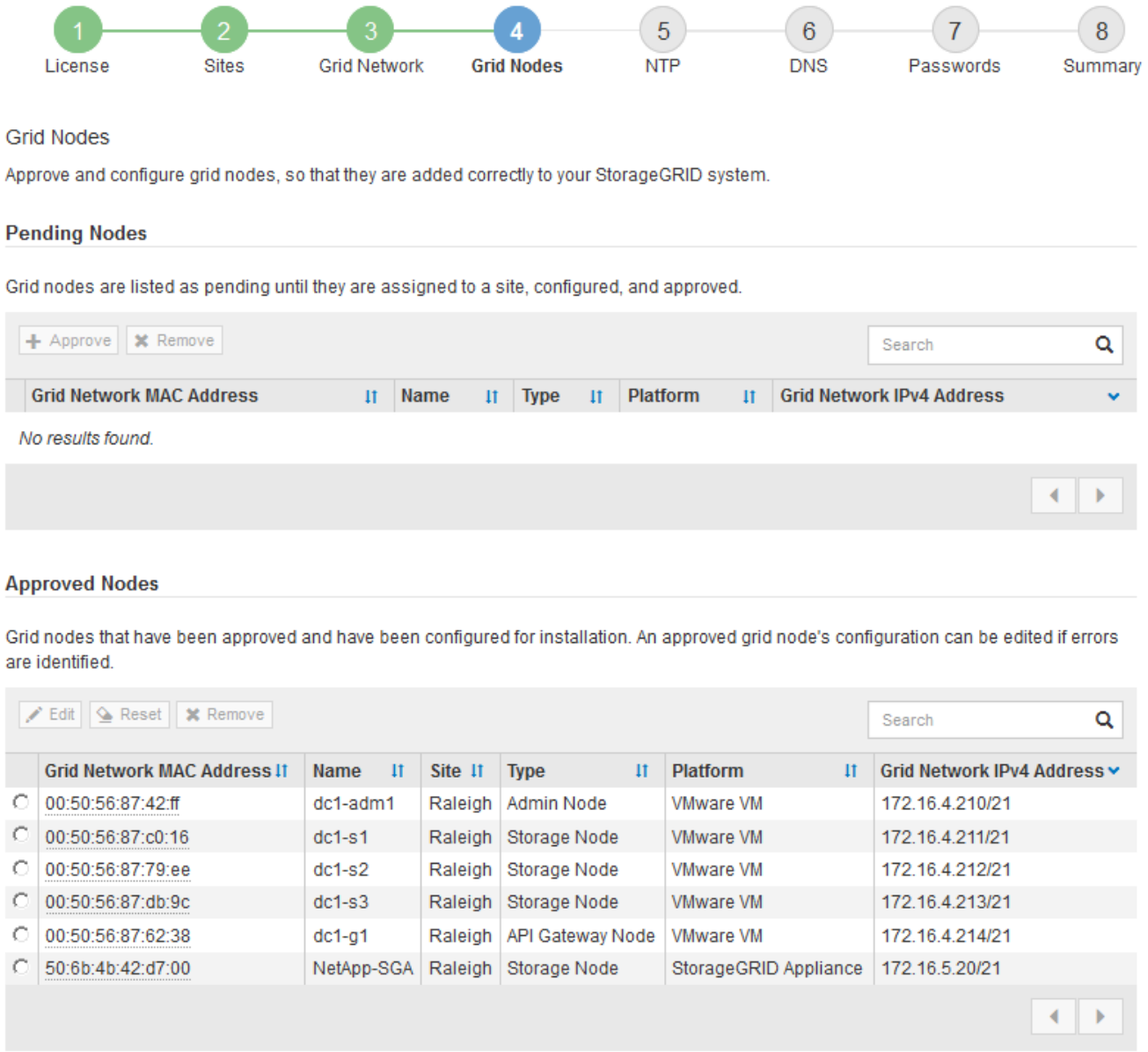
   g. Espere a que el nodo vuelva a aparecer en la lista Pending Nodes.

   h. Confirme que puede configurar las redes adecuadas. Ya deben rellenarse con la información proporcionada en la página IP Configuration.

      Para obtener más información, consulte las instrucciones de instalación y mantenimiento del dispositivo.

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.

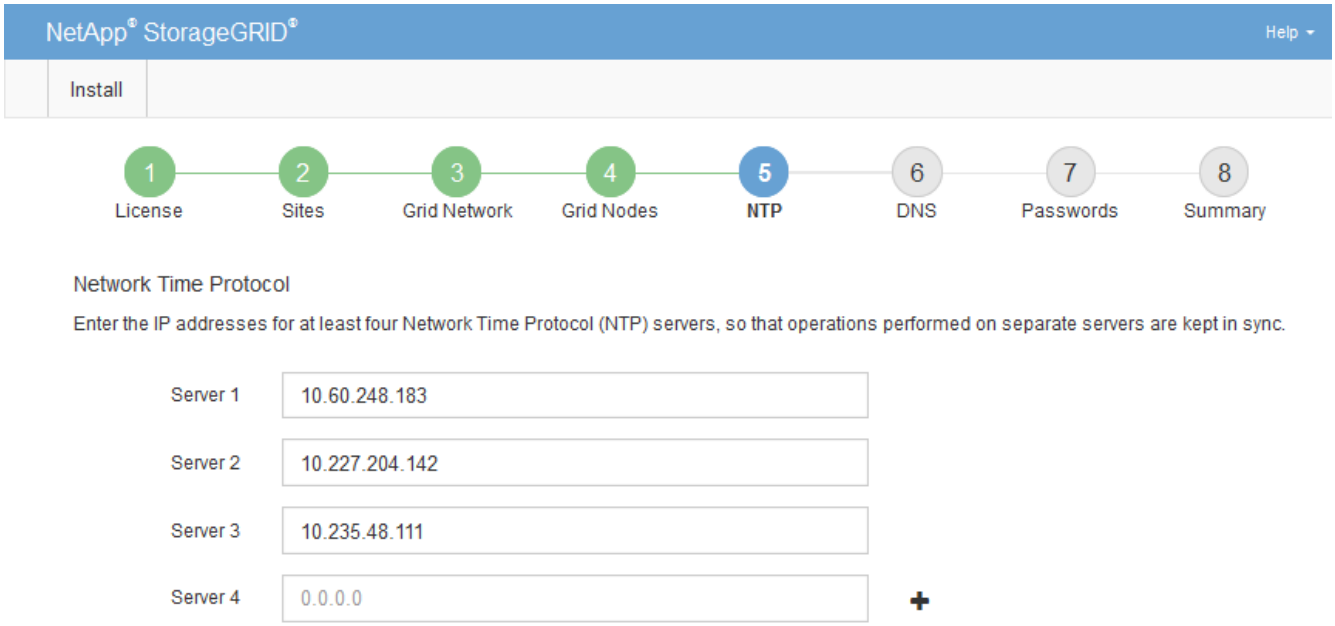
> Al especificar el origen NTP externo para una instalación StorageGRID de nivel de producción, no utilice el servicio de hora de Windows (W32Time) en una versión de Windows anterior a Windows Server 2016. El servicio de tiempo en versiones anteriores de Windows no es lo suficientemente preciso y no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

Debe especificar la información del sistema de nombres de dominio (DNS) para el

sistema StorageGRID, de modo que pueda acceder a servidores externos con nombres de host en lugar de direcciones IP.

Acerca de esta tarea

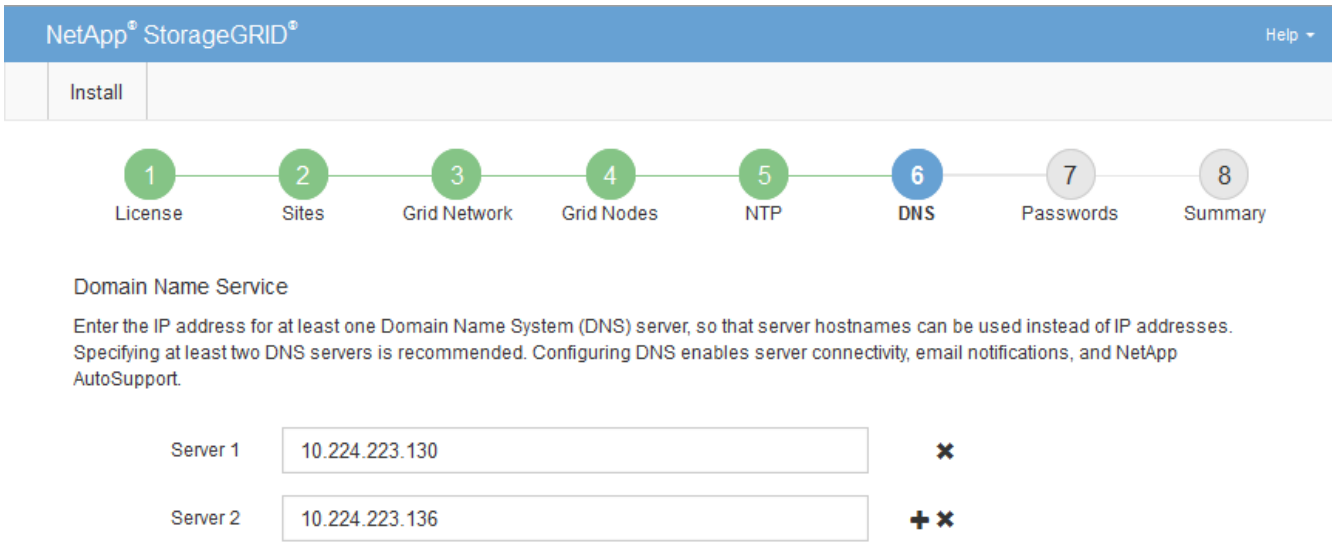
Al especificar la información del servidor DNS, se pueden utilizar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP para las notificaciones de correo electrónico y AutoSupport. Se recomienda especificar al menos dos servidores DNS.

> Proporcione de dos a seis direcciones IPv4 para los servidores DNS. Debe seleccionar los servidores DNS a los que puede acceder cada sitio localmente en el caso de que la red sea de destino. Esto es para asegurar que un sitio de llanded siga teniendo acceso al servicio DNS. Después de configurar la lista de servidores DNS para toda la cuadrícula, puede personalizar aún más la lista de servidores DNS para cada nodo. Para obtener detalles, consulte la información sobre cómo modificar la configuración de DNS en las instrucciones de recuperación y mantenimiento.

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 administración de grid se puede cambiar mediante Grid Manager.
- La consola de línea de comandos y las contraseñas SSH generadas aleatoriamente se almacenan en el archivo 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.

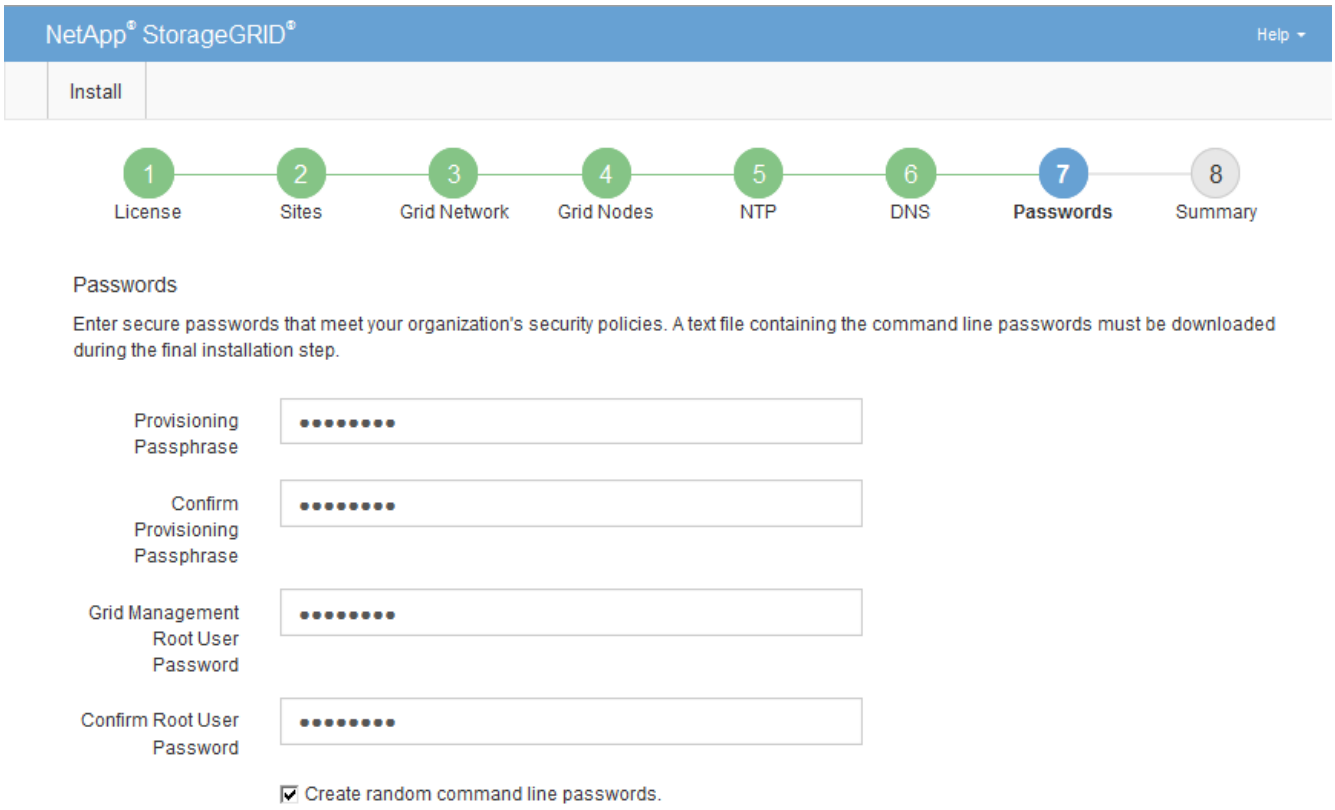
   Almacenar la clave de acceso de aprovisionamiento en un lugar seguro.

   > 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 **Contraseña de usuario raíz de Grid Management**, introduzca la contraseña que desea utilizar 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, anule la selección de 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. Anule la selección de **Crear contraseñas de línea de comandos aleatorias** sólo para cuadrículas de demostración si desea utilizar contraseñas predeterminadas para acceder a nodos de cuadrícula desde la línea de comandos mediante 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.

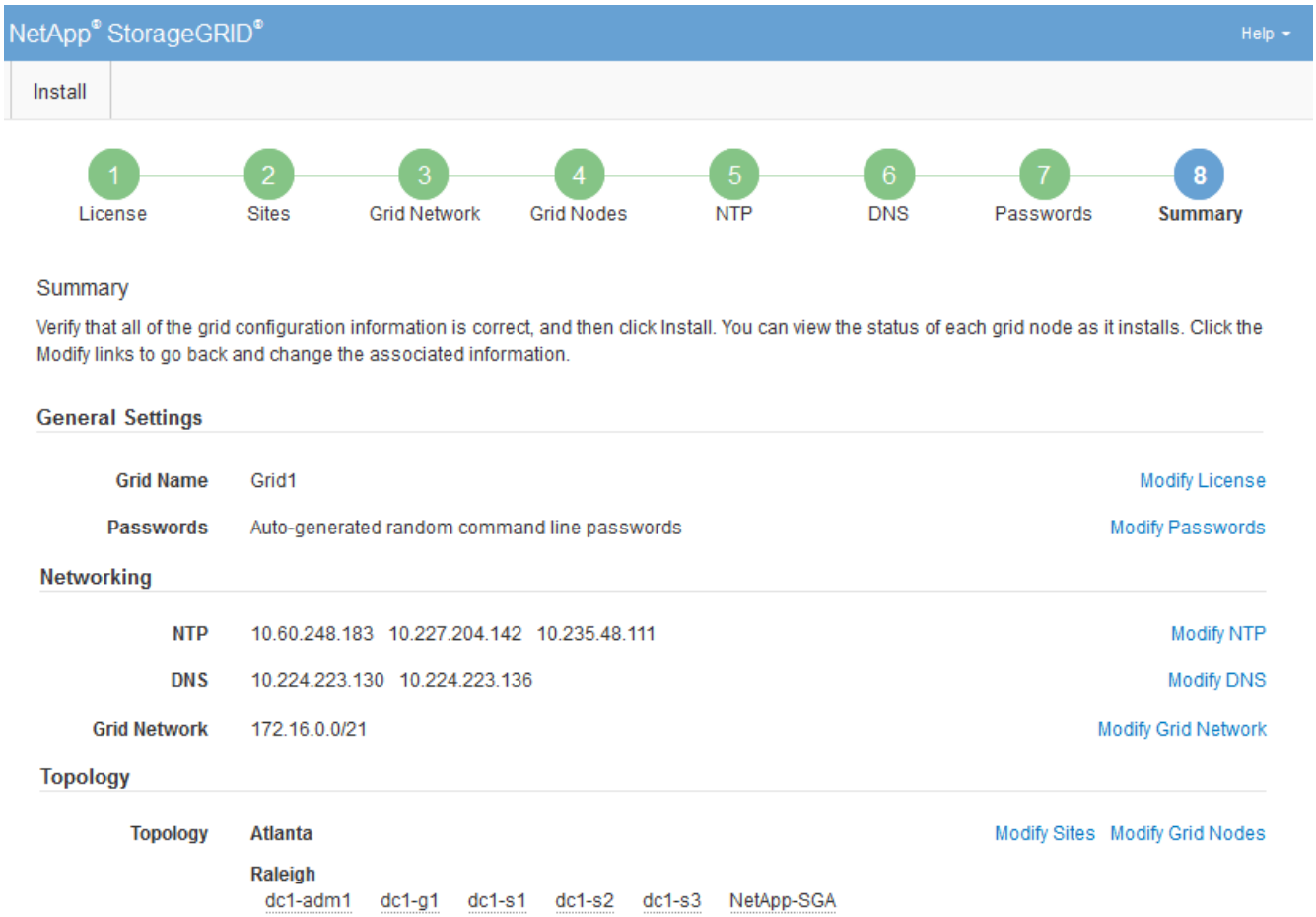
6. Haga clic en **Siguiente**.

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.

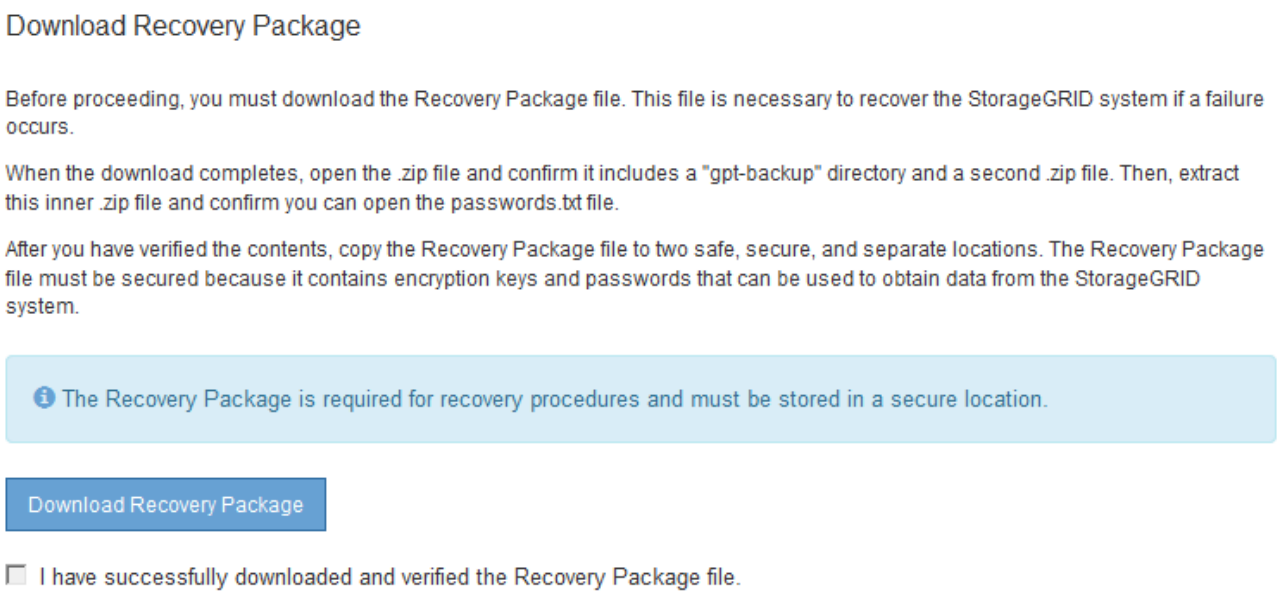
4. Haga clic en **Descargar paquete de recuperación**.

   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 puede completar la instalación y acceder al sistema StorageGRID hasta que descargue y verifique este archivo.

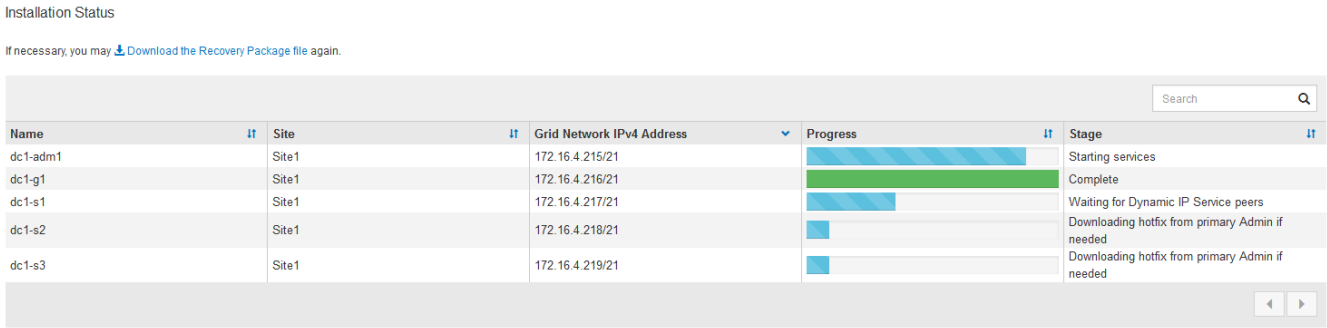
5. Compruebe que puede extraer el contenido del `.zip` archivar y, a continuación, guardarlo en dos ubicaciones seguras, seguras e independientes.

> 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. Active la casilla de verificación **he descargado y verificado correctamente el archivo de 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 es posible 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 volver a establecer estas conexiones.

Automatización de la instalación (Red Hat Enterprise Linux o CentOS)

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 de 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 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 o CentOS, agregar StorageGRID a sus libros de estrategia o recetas debe ser algo 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.

Automatice la configuración de StorageGRID

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

Lo que necesitará

- 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 ha especificado que se deben generar contraseñas aleatorias, debe extraer 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

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 (notación de objetos JavaScript).

> 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 configura inicialmente el sistema StorageGRID y en el caso de que deba realizar una recuperación de nodo de administrador principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de API, vaya a la página web de instalación del nodo de administración principal y seleccione **Ayuda** > **Documentación de 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

Tras completar una instalación, debe realizar una serie de pasos de integración y configuración. Se requieren algunos pasos; otros son opcionales.

Tareas requeridas

- Cree una cuenta de inquilino para cada protocolo de cliente (Swift o S3) que se usará para almacenar objetos en su sistema de StorageGRID.
- Controlar el acceso al sistema configurando grupos y cuentas de usuario. Opcionalmente, puede configurar un origen de identidad federado (como Active Directory u OpenLDAP) para que pueda importar grupos de administración y usuarios. También puede crear usuarios y grupos locales.
- Integre y pruebe las aplicaciones cliente API S3 o Swift que usará para cargar objetos en el sistema StorageGRID.
- Cuando esté listo, configure las reglas de gestión del ciclo de vida de la información (ILM) y la política de ILM que desee usar para proteger los datos de los objetos.

> Al instalar StorageGRID, se activa la política predeterminada de ILM, la política de copias base 2. Esta política incluye la regla de gestión del ciclo de vida de la información en stock (hacer 2 copias) y se aplica si no se ha activado ninguna otra política.

- Si la instalación incluye nodos de almacenamiento del dispositivo, use el software SANtricity para completar las siguientes tareas:
  - Conéctese a cada dispositivo StorageGRID.
  - Comprobar recepción de datos AutoSupport.
- Si el sistema StorageGRID incluye cualquier nodo de archivado, configure la conexión del nodo de archivado con el sistema de almacenamiento de archivado externo de destino.

> Si algún nodo de archivado utilizará Tivoli Storage Manager como sistema de almacenamiento de archivado externo, también deberá configurar Tivoli Storage Manager.

- Revise y siga las directrices de optimización del sistema StorageGRID para eliminar los riesgos de seguridad.
- Configurar las notificaciones por correo electrónico para las alertas del sistema.

Tareas opcionales

- Si desea recibir notificaciones del sistema de alarmas (heredadas), configure listas de correo y notificaciones por correo electrónico para alarmas.
- Actualice las direcciones IP del nodo de grid si han cambiado desde que planeó la implementación y generó el paquete de recuperación. Consulte información sobre el cambio de direcciones IP en las instrucciones de recuperación y mantenimiento.
- Configurar el cifrado del almacenamiento, si es necesario.
- Configure la compresión del almacenamiento para reducir el tamaño de los objetos almacenados, si es necesario.
- Configure el acceso de los clientes de auditoría. Puede configurar el acceso al sistema para fines de auditoría a través de un recurso compartido de archivos NFS o CIFS. Consulte las instrucciones para administrar StorageGRID.

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

Información relacionada

Administre StorageGRID

Use S3

Use Swift

Gestión de objetos con ILM

Supervisión y solución de problemas

Recuperación y mantenimiento

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG5600

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG6000

Notas de la versión

Endurecimiento del sistema

Revisar los registros de auditoría

Actualizar el software de

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 más información sobre cómo acceder a los archivos de registro, consulte las instrucciones para supervisar y solucionar problemas de StorageGRID. Para obtener ayuda sobre la solución de problemas de instalación del dispositivo, consulte las instrucciones de instalación y mantenimiento de los dispositivos. Si necesita ayuda adicional, póngase en contacto con el soporte técnico.

Información relacionada

Supervisión y solución de problemas

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG5600

"Soporte de NetApp"

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 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 Ubuntu o Debian

Instalar Ubuntu o Debian: Descripción general

La instalación de un sistema StorageGRID en un entorno Ubuntu o Debian incluye tres pasos principales.

1. **Preparación**: Durante la planificación y preparación, realiza las siguientes tareas:
   - Conozca los requisitos de hardware y almacenamiento para StorageGRID.
   - Conozca los aspectos específicos de Redes StorageGRID de este modo, puede configurar la red de forma adecuada.
   - Identificar y preparar los servidores físicos o virtuales que planea usar para alojar los nodos de grid de StorageGRID.
   - En los servidores que ha preparado:
     - Instale Linux
     - Configure la red del host
     - Configurar el almacenamiento del host
     - Instale Docker
     - Instale los servicios host StorageGRID

2. **Implementación**: Implementar nodos de red utilizando la interfaz de usuario adecuada. Cuando se implementan nodos de grid, se crean como parte del sistema StorageGRID y se conectan a una o varias redes.
   a. Utilice los archivos de configuración de nodos y línea de comandos de Linux para implementar nodos de grid virtual en los hosts que preparó en el paso 1.
   b. Use el instalador de dispositivos StorageGRID para poner en marcha los nodos del dispositivo StorageGRID.

> El procedimiento de instalación de StorageGRID no incluye las instrucciones de instalación e integración específicas de hardware. Para aprender a instalar dispositivos StorageGRID, consulte las instrucciones de instalación y mantenimiento del dispositivo.

3. **Configuración**: Cuando se han implementado todos los nodos, utilice el administrador de grid para configurar la cuadrícula y completar la instalación.

Estas instrucciones recomiendan un enfoque estándar para implementar y configurar un sistema StorageGRID en un entorno Ubuntu o Debian. Consulte también la información acerca de los siguientes enfoques alternativos:

- Use un marco de orquestación estándar como Ansible, Puppet o Chef para instalar Ubuntu o Debian, configurar redes y almacenamiento, instalar Docker y el servicio host StorageGRID, y poner en marcha nodos de grid virtual.
- Automatice la puesta en marcha y configuración del sistema StorageGRID mediante un script de configuración Python (incluido en el archivo de instalación).
- Automatice la puesta en marcha y configuración de los nodos del grid de los dispositivos con un script de configuración Python (disponible desde el archivo de instalación o desde el instalador de dispositivos de StorageGRID).
- Si es un desarrollador avanzado de implementaciones de StorageGRID, use las API DE REST de instalación para automatizar la instalación de los nodos de grid de StorageGRID.

Planear y preparar la instalación de Ubuntu o Debian

Antes de instalar (Ubuntu o Debian)

Antes de implementar nodos de grid y configurar la cuadrícula de StorageGRID, debe estar familiarizado con los pasos y los requisitos para completar el procedimiento.

Los procedimientos de puesta en marcha y configuración de StorageGRID dan por sentado que está familiarizado con la arquitectura y el funcionamiento del sistema StorageGRID.

Puede implementar un solo sitio o varios sitios a la vez; sin embargo, todos los sitios deben cumplir con el requisito mínimo de tener al menos tres nodos de almacenamiento.

Antes de iniciar una instalación de StorageGRID, debe:

- Comprenda los requisitos de computación de StorageGRID, incluidos los requisitos mínimos de CPU y RAM para cada nodo.
- Comprenda cómo StorageGRID admite varias redes para la separación del tráfico, la seguridad y la comodidad administrativa. Además, tenga un plan para qué redes piensa conectar a cada nodo StorageGRID.

Consulte las directrices para redes de StorageGRID.

- Comprenda los requisitos de almacenamiento y rendimiento de cada tipo de nodo 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.
- Comprenda los requisitos para la migración de nodos si desea realizar tareas de mantenimiento programadas en hosts físicos sin ninguna interrupción del servicio.
- Recopile toda la información de la red con antelación. A menos que utilice DHCP, recopile las direcciones IP para asignar a cada nodo de grid y las direcciones IP de los servidores del sistema de nombres de dominio (DNS) y del protocolo de hora de red (NTP) que se utilizarán.
- Instale, conecte y configure todo el hardware necesario, incluidos los dispositivos StorageGRID, según las especificaciones.

> El procedimiento de instalación de StorageGRID no incluye las instrucciones de instalación e integración específicas de hardware. Para aprender a instalar dispositivos StorageGRID, consulte las instrucciones de instalación y mantenimiento del dispositivo.

- Decida qué herramientas de implementación y configuración disponibles desea utilizar.

Información relacionada

Directrices sobre redes

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG5600

Requisitos de migración de contenedores de nodos

Materiales requeridos

Antes de instalar StorageGRID, debe recopilar y preparar los materiales necesarios.

Elemento	Notas
Licencia de StorageGRID de NetApp	Debe tener una licencia de NetApp válida y con firma digital. **Nota**: En el archivo de instalación de StorageGRID se incluye una licencia de no producción, que puede utilizarse para probar y probar cuadrículas de concepto.
Archivo de instalación de StorageGRID	Debe Descargue el archivo de instalación de StorageGRID y extraiga los archivos.

Elemento	Notas
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

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

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 instrucción Caution/MustRead, léala y active 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 para 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
	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.
	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.

Ruta y nombre de archivo	Descripción
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede utilizar estos esquemas para confirmar que cualquier código que haya escrito para utilizar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no dispone de un entorno StorageGRID que no sea de producción para la comprobación de compatibilidad de actualizaciones.

Información relacionada

Recuperación y mantenimiento

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.

Para obtener información sobre los servidores admitidos, consulte la matriz de interoperabilidad.

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 cómo gestionar el almacenamiento de metadatos de objetos, aumentar la configuración de espacio reservado de metadatos y supervisar el uso de la CPU y la memoria, consulte las instrucciones para administrar, supervisar 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 la información sobre los requisitos de almacenamiento.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Los requisitos de almacenamiento y rendimiento

Administre StorageGRID

Supervisión y solución de problemas

Actualizar el software de

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 no redundantes, SSD o JBOD. 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 de StorageGRID, debe almacenar tanto datos de sistema como datos de objetos en almacenamiento compartido.

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 los hosts que usan almacenamiento ONTAP de NetApp

Si el nodo StorageGRID utiliza almacenamiento asignado desde un sistema ONTAP de NetApp, confirme que el volumen no tiene habilitada la 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.

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 único 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

Propósito de LUN	Categoría de almacenamiento	Número de LUN	Tamaño mínimo/LUN
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 los requisitos de almacenamiento de los nodos de almacenamiento si desea obtener más información.
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

Según el nivel de auditoría configurado, el tamaño de las entradas de usuario, como el nombre de la clave de objeto S3 y la cantidad de datos del registro de auditoría que se deben conservar, es posible que deba aumentar el tamaño de la LUN del registro de auditoría de cada nodo de administración. Como regla general, un grid genera aproximadamente 1 KB de datos de auditoría por operación de S3, lo que significa que una LUN de 200 GB admitirá 70 millones de operaciones diarias 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 snapshots de disco no se pueden utilizar para restaurar nodos de grid. En su lugar, consulte los procedimientos de recuperación y mantenimiento de 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.

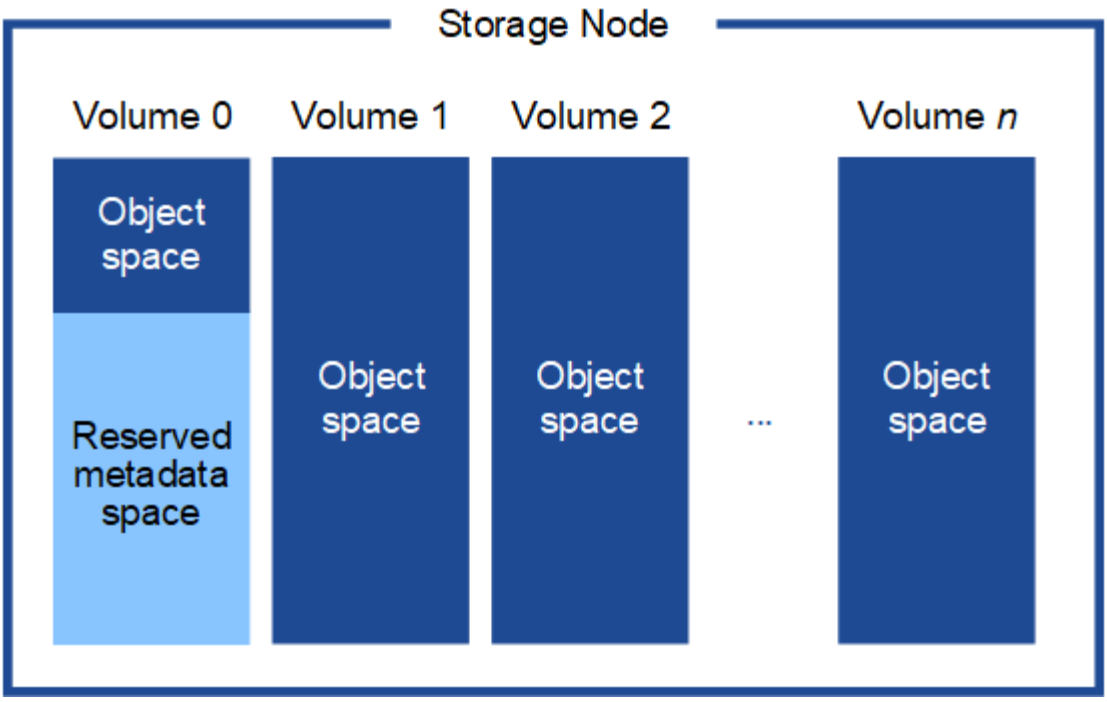
Tipo de nodo	Propósito de LUN	Número de LUN	Tamaño de LUN
Nodo de almacenamiento	Pool de almacenamiento de Docker	1	300 GB (100 GB/nodo)
Nodo de almacenamiento	`/var/local` volumen	1	90 GB
Nodo de almacenamiento	Datos de objetos	3	12 TB (4 TB/LUN)
Nodo de administración	`/var/local` volumen	1	90 GB
Nodo 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 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 está instalando un nuevo sistema StorageGRID 11.6 y cada nodo de almacenamiento tiene 128 GB o más de RAM, debe asignar 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.

Información relacionada

Requisitos de migración de contenedores de nodos

Recuperación y mantenimiento

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. Solo tiene que mover todos los nodos 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 funcionalidad 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

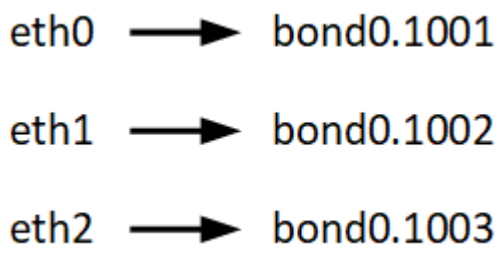
OpenStack Live Migration y VMware Live vMotion hacen que salte el tiempo del reloj de la máquina virtual y no son compatibles con los nodos de grid de ningún tipo. Aunque es poco frecuente, las horas de reloj incorrectas pueden provocar la pérdida de datos o actualizaciones de configuración.

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 de StorageGRID debe tener cierto grado de 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

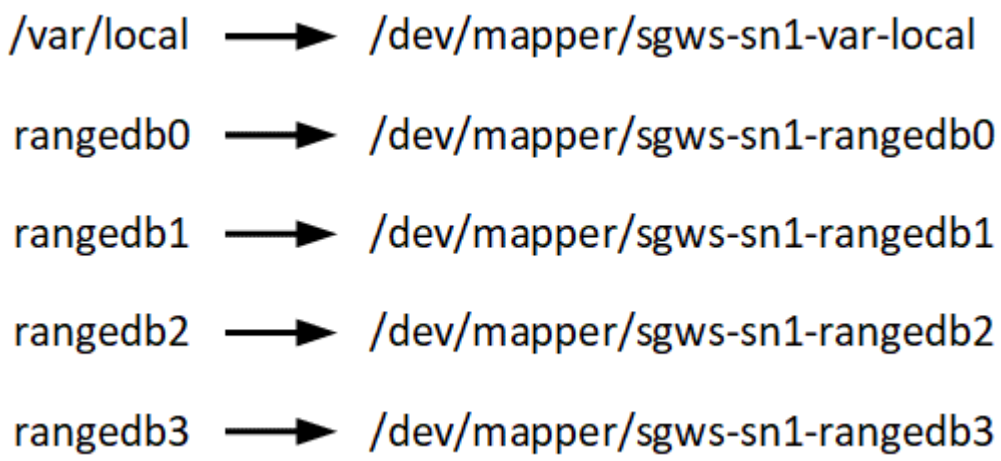
Para poder realizar migraciones de nodos rápidas y con baja sobrecarga, la función de migración de nodos de StorageGRID no mueve físicamente los datos de nodos. En su lugar, la migración de nodos se realiza como par de operaciones de exportación e importación, de la siguiente manera:

Pasos

1. Durante la operación de «'exportación de nodos'», se extrae una pequeña cantidad de datos de estado persistente del contenedor de nodos que se ejecuta en 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 "'node import'", se crea una instancia del contenedor de nodos en HostB que utiliza la misma interfaz de red y las asignaciones de almacenamiento de bloque que estaban en vigor en Hosta. 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.



Herramientas de puesta en marcha

Podría beneficiarse de la automatización de toda la instalación de StorageGRID o de parte de ella.

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.

Si está interesado en automatizar toda la implementación de StorageGRID o una parte de ella, consulte Automatizar la instalación antes de iniciar el proceso de instalación.

Preparar los hosts (Ubuntu o Debian)

Instale Linux

Debe instalar Linux en todos los hosts Grid. Utilice la "Herramienta de matriz de interoperabilidad de NetApp" para obtener una lista de las versiones compatibles.

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. El resto de opciones pueden permanecer sin seleccionar.

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".

  Una vez que haya desactivado AppArmor, no aparecerán entradas que indiquen que AppArmor esté activado 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.

Lo que necesitará

- 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 los nodos ni entre el host y ningún 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 sus hosts son máquinas virtuales y va a implementar uno o dos nodos de StorageGRID para cada host, puede simplemente crear el número correcto de interfaces de red en el hipervisor y utilizar 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 método que satisfaga sus necesidades.

> No utilice dispositivos de enlace o puente directamente como interfaz de red de contenedores. 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, más bien, permite que todas las interfaces reciban y transmitan datos para direcciones MAC distintas a las asignadas por el hipervisor, Asegúrese de que las propiedades de seguridad de los niveles de conmutador virtual y grupo de puertos están configuradas en **Aceptar** para modo promiscuous, cambios de dirección MAC y señales falsificadas. Los valores establecidos en el conmutador virtual pueden ser anulados por los valores en el nivel de grupo de puertos, por lo que asegúrese de que la configuración sea la misma en ambos lugares.

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:

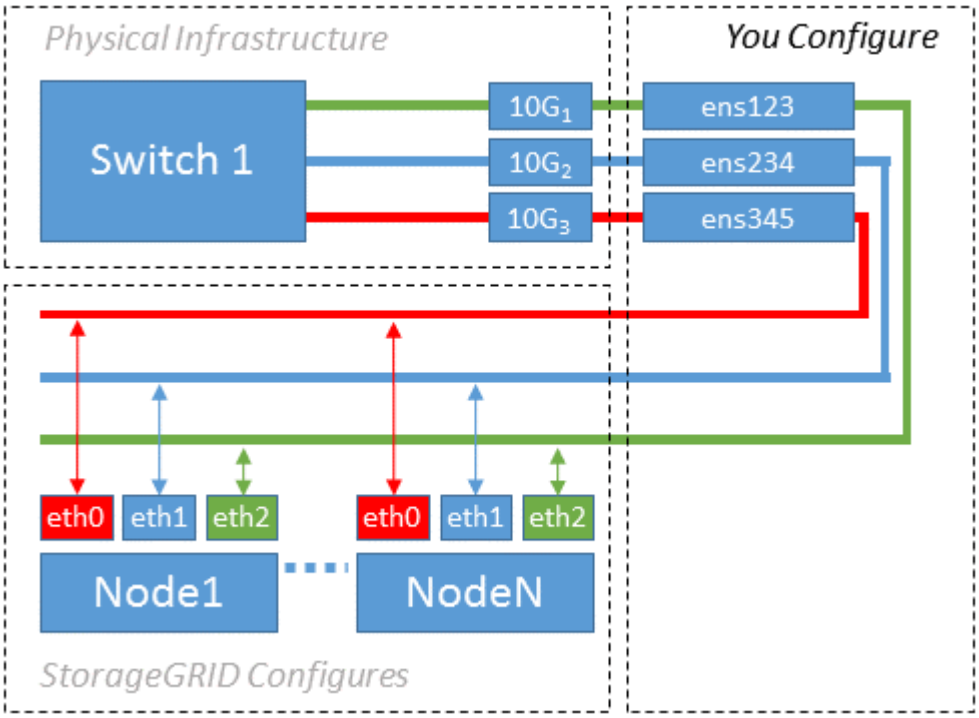
- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

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

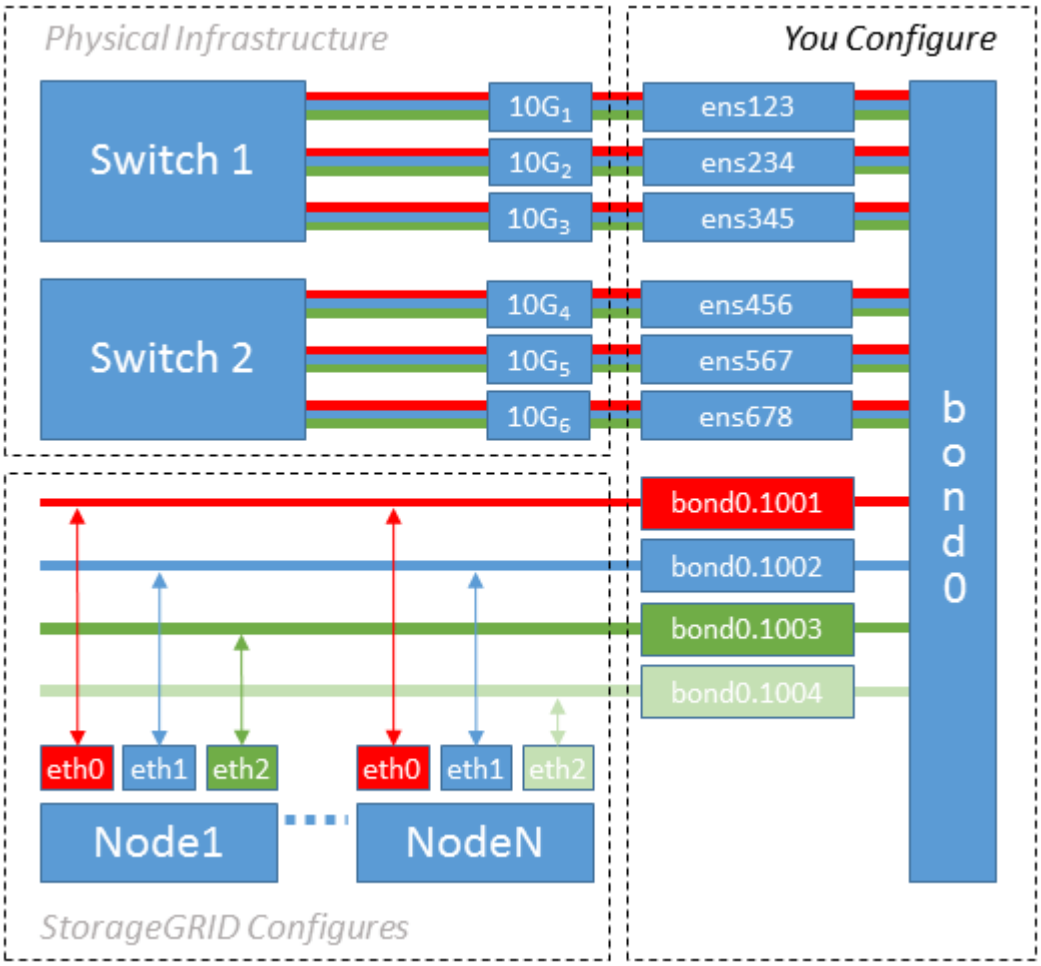
En el ejemplo 2 se supone que está familiarizado con las interfaces de red de enlace y con la creación de interfaces VLAN en la distribución Linux que está utilizando.

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," `using the standard VLAN interface naming convention `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 /etc/network/interfaces

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

Lo que necesitará

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

Al asignar volúmenes de almacenamiento en bloque (LUN) a los hosts, utilice las tablas de «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 realizar particiones, formatear ni montar ninguno de estos volúmenes; solo tiene que asegurarse de que son visibles para los hosts.

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 de iSCSI y accesos múltiples de asignación de dispositivos, considere la posibilidad de utilizar alias multivía en el `/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 configura un almacenamiento compartido para que sea compatible con la migración de nodos StorageGRID y con la función multivía 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.

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 los nodos se usan para los nodos virtuales y no se usan para los nodos del dispositivo.

¿Dónde se colocan los archivos de configuración del nodo?

Debe colocar el archivo de configuración para 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.

¿Qué nombre tienen los archivos de configuración del nodo?

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 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.

¿Qué hay en un archivo de configuración de nodo?

Los archivos de configuración contienen pares clave/valor, con una clave y un valor por línea. Para cada par clave/valor, debe seguir 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.

Algunas claves son necesarias para cada nodo, mientras que otras son opcionales o solo necesarias para ciertos tipos de nodo.

La tabla define los valores aceptables para todas las claves admitidas. En la columna central:

R: Requerido + BP: Mejor práctica + o: Opcional

Clave	¿R, BP O O?	Valor
IP_ADMINISTRADOR	BP	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.
ADMIN_NETWORK_CONFIG	O	DHCP, ESTÁTICO O DESHABILITADO
ADMIN_NETWORK_ESL	O	Lista de subredes separadas por comas en la notación CIDR a la que este nodo se debe comunicar a través de la puerta de enlace de red de administración. Ejemplo: `172.16.0.0/21,172.17.0.0/21`

ADMIN_NETWORK_GATEWAY	O (**R**)	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.
		
		Nota: Este parámetro es necesario si SE especifica ADMIN_NETWORK_ESL.
		
		Ejemplos:
		
		`1.1.1.1`
		
		`10.224.4.81`

Clave	¿R, BP O O?	Valor

IP_RED_ADMIN	O	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`

ADMIN_NETWORK_MAC	O	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`

ADMIN_NETWORK_MASK	O	La máscara de red IPv4 para este nodo, en la red de administrador. Esta clave solo es necesaria cuando ADMIN_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
		
		Ejemplos:
		
		`255.255.255.0`
		
		`255.255.248.0`

Clave	¿R, BP O O?	Valor

MTU_RED_ADMIN	O	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 usa 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`

ADMIN_NETWORK_TARGET	BP	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 destino 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`

ADMIN_NETWORK_TARGET_TYPE	O	Interfaz (Este es el único valor admitido).

Clave	¿R, BP O O?	Valor
ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	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 o CentOS) Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)
ADMIN_ROLE	**R**	Primario o no primario Esta clave solo es necesaria cuando NODE_TYPE = VM_Admin_Node; no la especifique para otros tipos de nodos.

BLOCK_DEVICE_AUDIT_LOGS	**R**	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. Esta clave solo es necesaria para nodos con NODE_TYPE = VM_Admin_Node; no la especifique para otros tipos de nodo.
		
		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`

Clave	¿R, BP O O?	Valor

BLOCK_DEVICE_RANGEDB_000
 	
BLOCK_DEVICE_RANGEDB_001
 	
BLOCK_DEVICE_RANGEDB_002
 	
BLOCK_DEVICE_RANGEDB_003
 	
BLOCK_DEVICE_RANGEDB_004
 	
BLOCK_DEVICE_RANGEDB_005
 	
BLOCK_DEVICE_RANGEDB_006
 	
BLOCK_DEVICE_RANGEDB_007
 	
BLOCK_DEVICE_RANGEDB_008
 	
BLOCK_DEVICE_RANGEDB_009
 	
BLOCK_DEVICE_RANGEDB_010
 	
BLOCK_DEVICE_RANGEDB_011
 	
BLOCK_DEVICE_RANGEDB_012
 	
BLOCK_DEVICE_RANGEDB_013
 	
BLOCK_DEVICE_RANGEDB_014
 	
BLOCK_DEVICE_RANGEDB_015
	R	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 nodos con NODE_TYPE = VM_Storage_Node; no la especifique para otros tipos de nodo.
		
		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. 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`

Clave	¿R, BP O O?	Valor

BLOCK_DEVICE_TABLES	**R**	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 nodos con NODE_TYPE = VM_Admin_Node; no la especifique para otros tipos de nodo.
		
		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`

BLOCK_DEVICE_VAR_LOCAL	**R**	Ruta y nombre del archivo especial del dispositivo de bloque que este nodo utilizará para su almacenamiento persistente /var/local.
		
		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`

CLIENT_NETWORK_CONFIG	O	DHCP, ESTÁTICO O DESHABILITADO

PUERTA_DE_ENLACE_RED_CLIENTE	O	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`

Clave	¿R, BP O O?	Valor

IP_RED_CLIENTE	O	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`

MAC_RED_CLIENTE	O	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`

MÁSCARA_RED_CLIENTE	O	La máscara de red IPv4 para este nodo en la red de cliente. Esta clave solo es necesaria cuando CLIENT_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
		
		Ejemplos:
		
		`255.255.255.0`
		
		`255.255.248.0`

Clave	¿R, BP O O?	Valor

MTU_RED_CLIENTE	O	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 usa 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`

DESTINO_RED_CLIENTE	BP	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 destino 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`

CLIENT_NETWORK_TARGET_TYPE	O	Interfaz (Solo se admite este valor).

Clave	¿R, BP O O?	Valor
CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	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 o CentOS) Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)
GRID_NETWORK_CONFIG	BP	ESTÁTICO o DHCP (De forma predeterminada, ES ESTÁTICO si no se especifica.)
PUERTA_DE_ENLACE_RED_GRID	**R**	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.

IP_RED_GRID	**R**	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`

Clave	¿R, BP O O?	Valor
MAC_RED_GRID	O	La dirección MAC de la interfaz de red de red del 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:c2:27:30`

GRID_NETWORK_MASK	O	Máscara de red IPv4 para este nodo en la red de cuadrícula. Esta clave solo es necesaria cuando GRID_NETWORK_CONFIG = STATIC; no la especifique para otros valores.
		
		Ejemplos:
		
		`255.255.255.0`
		
		`255.255.248.0`

MTU_RED_GRID	O	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 usa 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. Los valores de MTU no tienen que ser iguales para todos los tipos de red. Ejemplos: 1500 8192

Clave	¿R, BP O O?	Valor

GRID_NETWORK_TARGET	**R**	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 destino 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`

GRID_NETWORK_TARGET_TYPE	O	Interfaz (Este es el único valor admitido).
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	**BP**	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 o CentOS) Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)

Clave	¿R, BP O O?	Valor
INTERFACES_TARGET_nnnn	O	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_DESTINO_INTERFACES que esté agregando. 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. Por ejemplo: `INTERFACES_TARGET_01=ens256, Trunk` Si añade una interfaz troncal, debe configurar una interfaz VLAN en StorageGRID. Si agrega una interfaz de acceso, puede agregar la interfaz directamente a un grupo de alta disponibilidad; no es necesario configurar una interfaz de VLAN.

RAM_MÁXIMA	O	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 Instrucciones para administrar StorageGRID Para obtener una descripción de lo que es el espacio reservado de metadatos.
		
		El formato de este campo es `<number><unit>`, 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.

TIPO_NODO	**R**	Tipo de nodo: VM_Admin_Node VM_Storage_Node VM_Archive_Node VM_API_Gateway

Clave	¿R, BP O O?	Valor
REASIGNAR_PUERTO	O	Reasigna cualquier puerto que usa un nodo para las comunicaciones internas del nodo de grid o las comunicaciones externas. Es necesario volver a asignar puertos si las políticas de red de la empresa restringen uno o más puertos utilizados por StorageGRID, como se describe en «'Comunicaciones internas de nodos de grid» o «'Comunicaciones externas». **IMPORTANTE**: No reasigne los puertos que va a utilizar para configurar puntos finales de 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 el protocolo es tcp o udp. Por ejemplo: `PORT_REMAP = client/tcp/18082/443`
PORT_REMAPP_INBOUND	O	Reasigna las comunicaciones entrantes al puerto especificado. Si especifica PORT_REMAPP_INBOUND pero no especifica un valor para PORT_REMAPP, las comunicaciones salientes para el puerto no se modifican. **IMPORTANTE**: No reasigne los puertos que va a utilizar para configurar puntos finales de 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 el protocolo es tcp o udp. Por ejemplo: `PORT_REMAP_INBOUND = grid/tcp/3022/22`

Información relacionada

Directrices sobre redes

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 normalmente a través de 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.

```
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
```

Para cualquier nodo que devuelva un estado de "'no en ejecución'" o "encabezado", ejecute el siguiente comando:

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

3. 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.

Lo que necesitará

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
```

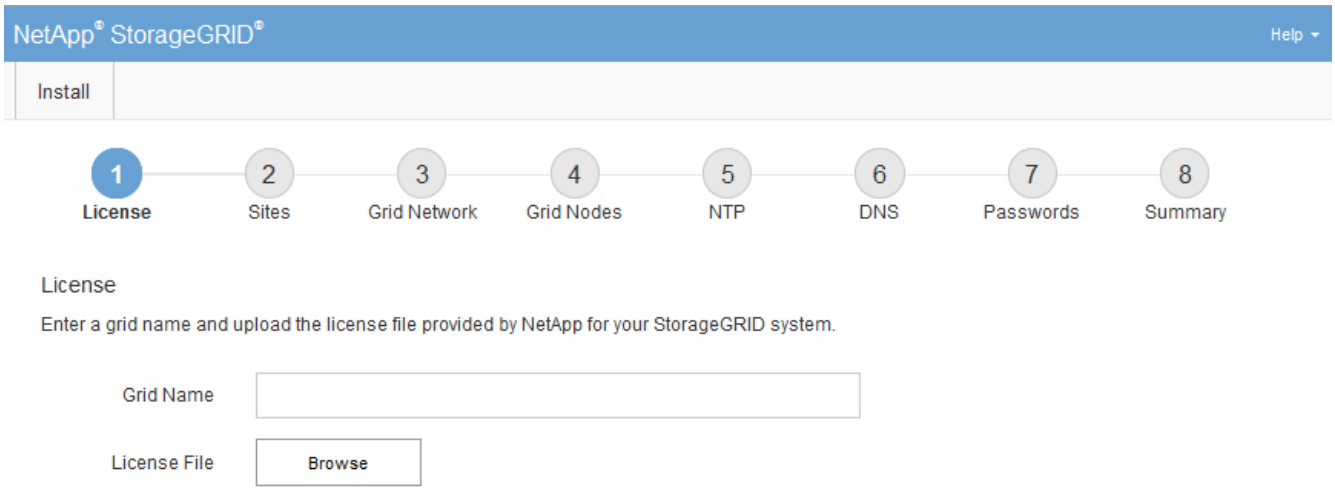
También puede acceder a Grid Manager en el puerto 8443:

```
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.

1. Haga clic en **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

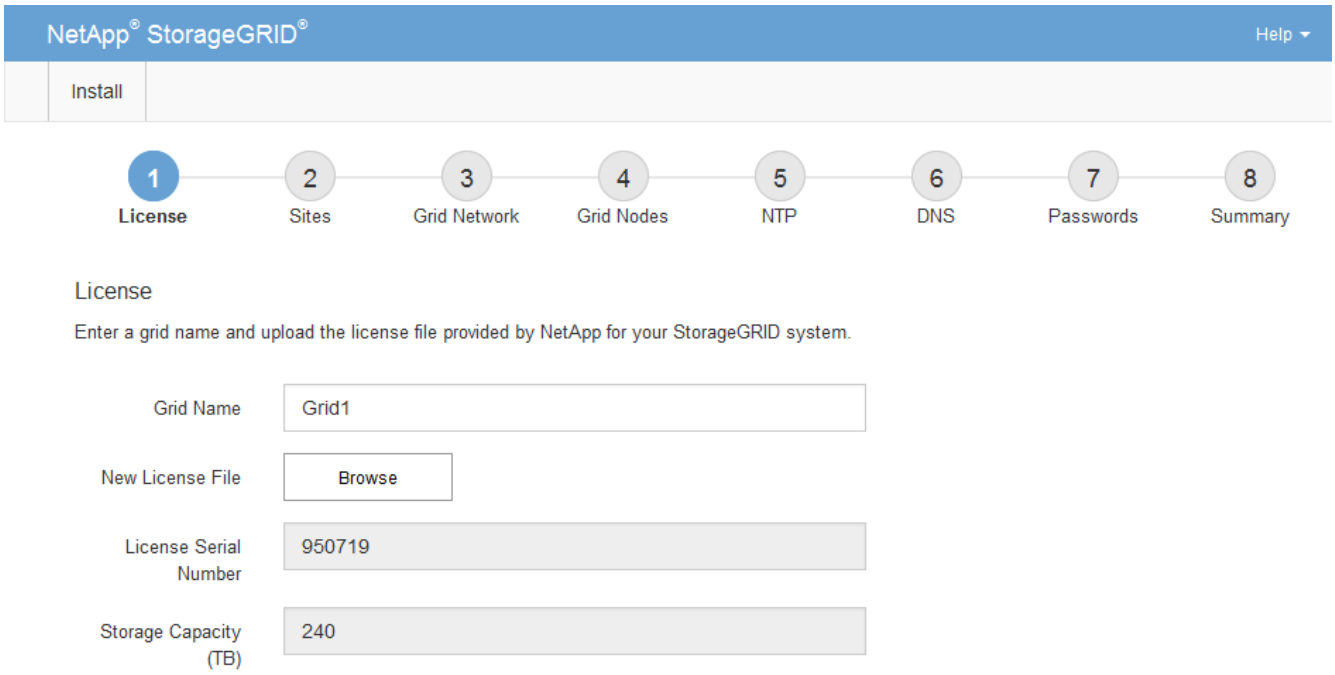
1. En la página Licencia, introduzca un nombre significativo para su sistema StorageGRID en **Nombre de cuadrícula**.

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

2. Haga clic en **Browse**, busque el archivo de licencia de NetApp (`NLFunique_id.txt`) Y haga clic en **Abrir**.

   El archivo de licencia se valida y se muestran el número de serie y la capacidad de almacenamiento con licencia.

   > 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.



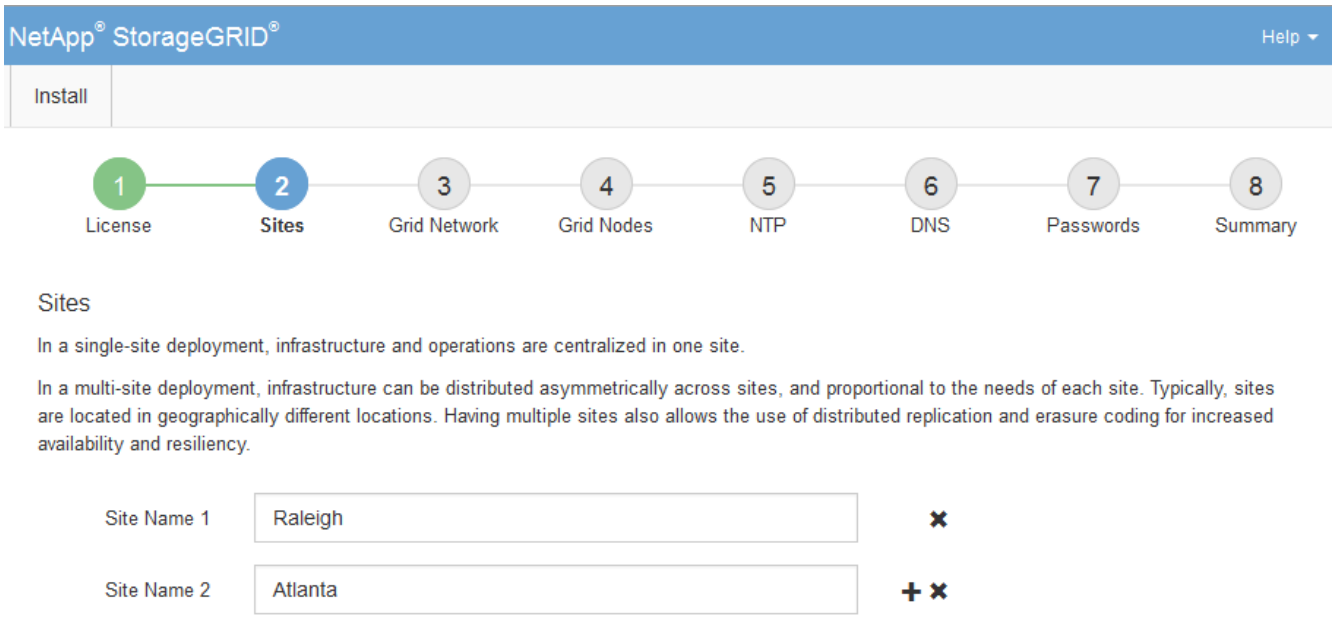
3. Haga clic en **Siguiente**.

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

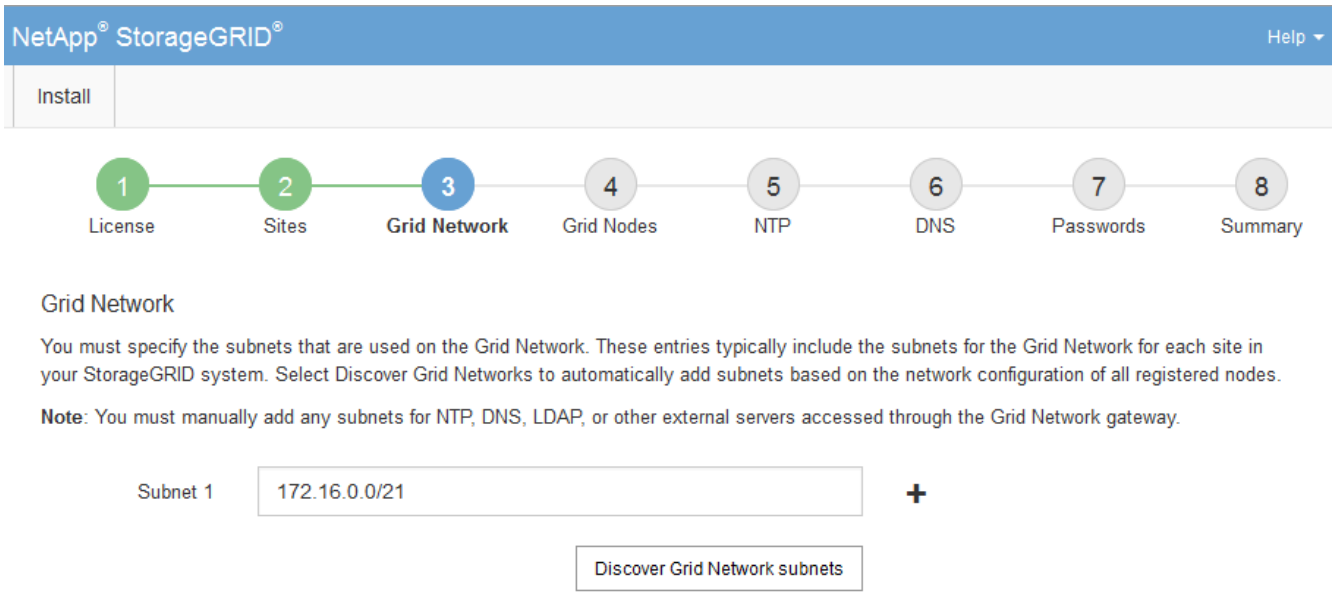
Las entradas de subred incluyen las subredes para la red de cuadrícula de cada sitio del sistema StorageGRID, junto con las subredes a las que se debe acceder a través de la red de cuadrícula.

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.

Lo que necesitará

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

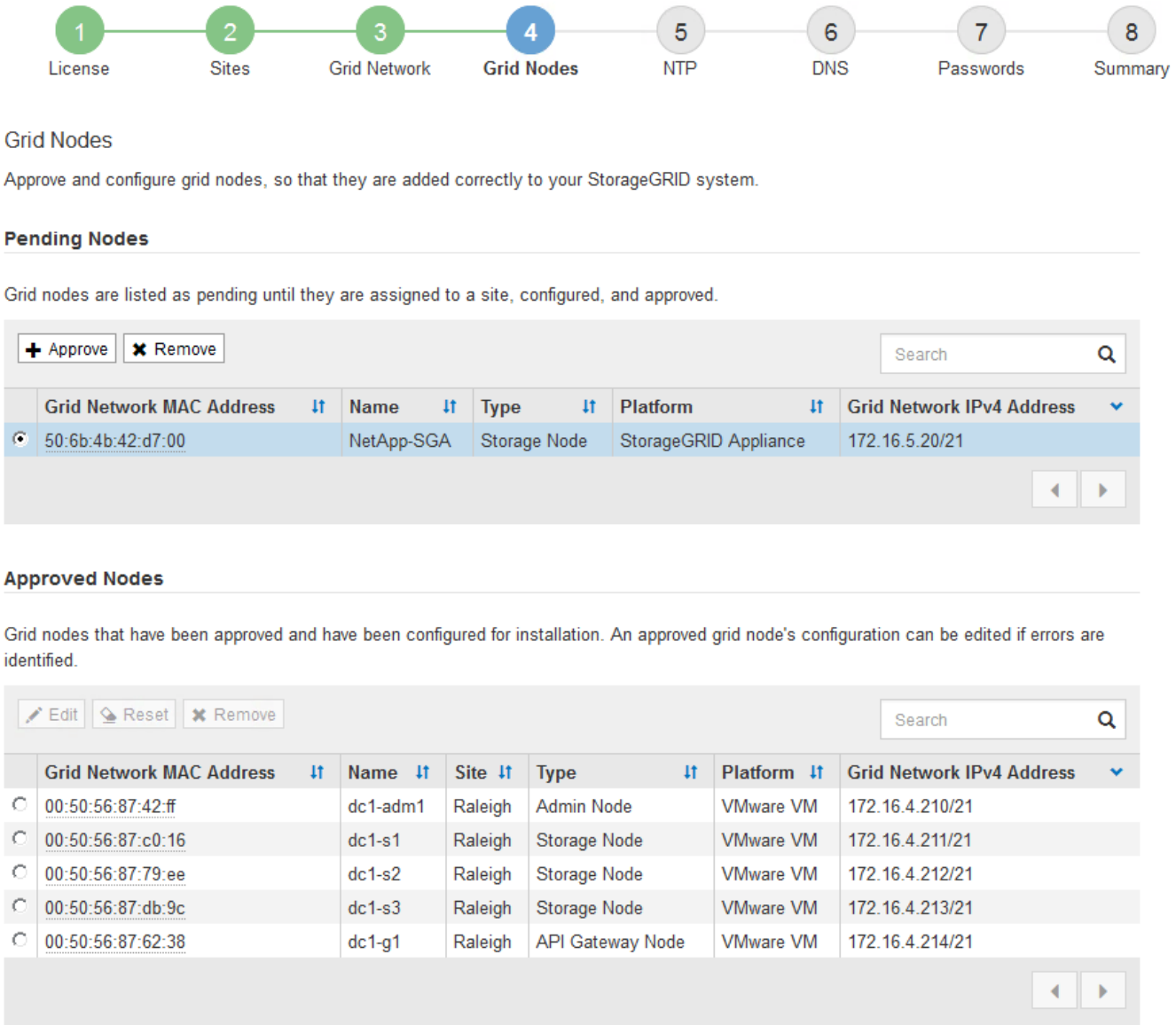
> Es más eficiente realizar una instalación única de todos los nodos, en lugar de instalar algunos ahora y algunos nodos más adelante.

Pasos

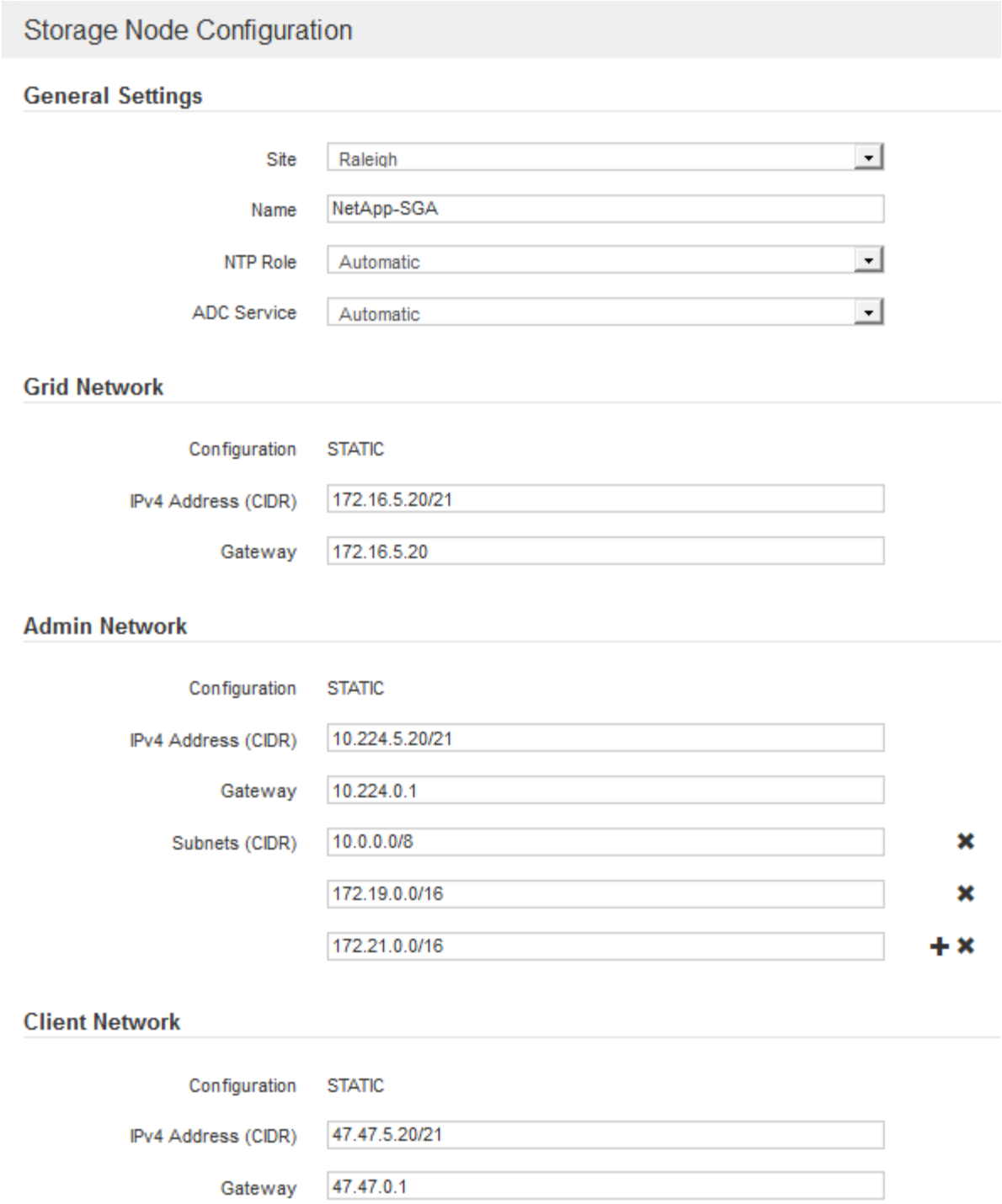
1. Revise la lista Pending Nodes y confirme que se muestran todos los nodos de grid que ha implementado.

   > 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 sitio con el que se asociará este nodo de red.
- **Nombre**: El nombre que se asignará al nodo y el nombre que se mostrará en el Gestor de cuadrícula. El nombre predeterminado es el nombre que especifique cuando configure el nodo. Durante este paso del proceso de instalación, puede cambiar el nombre según sea necesario.

> Una vez finalizada la instalación, no puede cambiar el nombre del nodo.

> 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.

- **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 haberlo implementado.

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 del 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 el Gestor de cuadrícula: Si el nodo aparece en la tabla nodos aprobados, restablezca 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 IP Configuration.

   Para obtener información adicional, consulte las instrucciones de instalación y mantenimiento del 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.

   Dispositivos: 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 del 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 el Gestor de cuadrícula: Si el nodo aparece en la tabla nodos aprobados, restablezca el nodo.

   f. Quite el nodo de la tabla Pending Nodes.

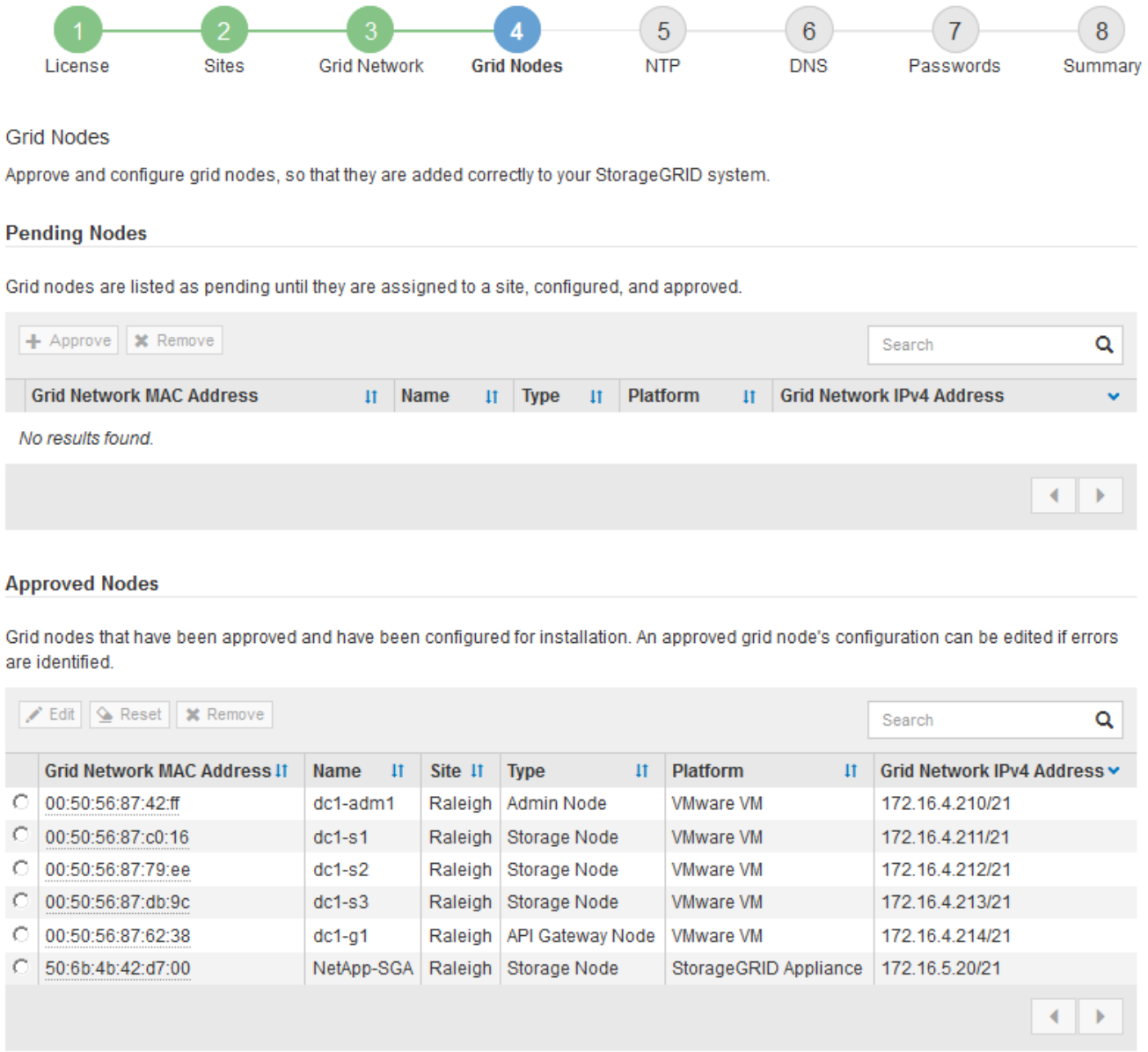
   g. Espere a que el nodo vuelva a aparecer en la lista Pending Nodes.

   h. Confirme que puede configurar las redes adecuadas. Ya deben rellenarse con la información proporcionada en la página IP Configuration.

      Para obtener más información, consulte las instrucciones de instalación y mantenimiento del dispositivo.

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.

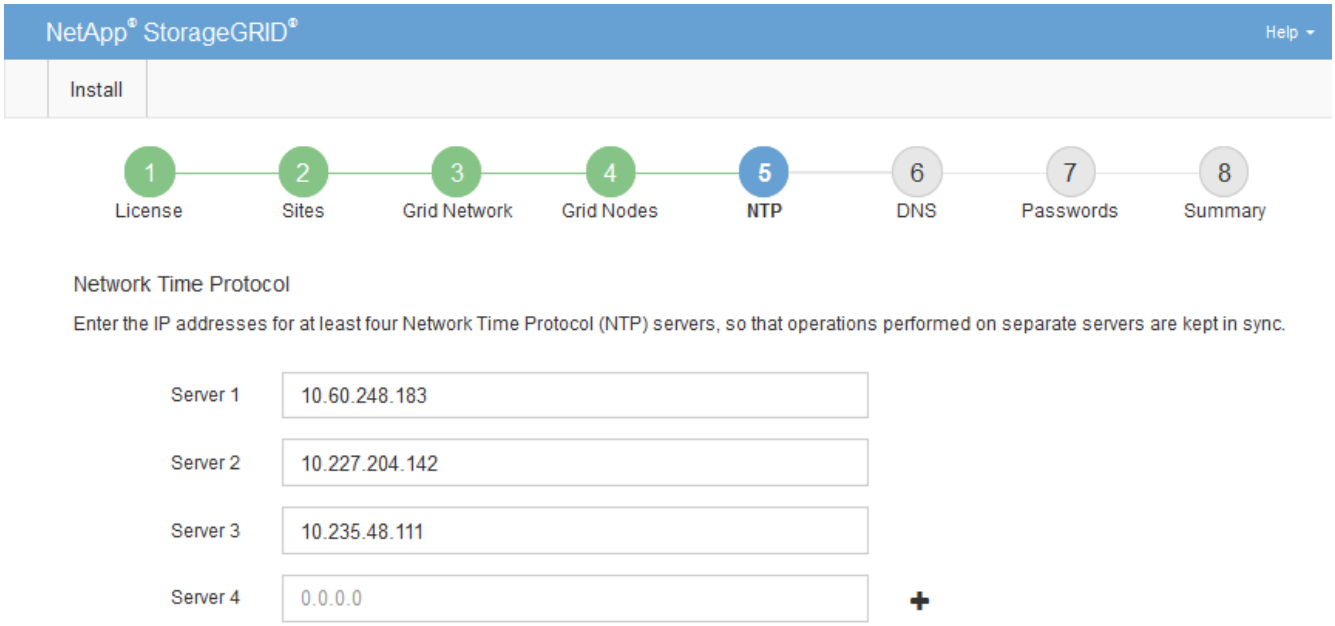
> Al especificar el origen NTP externo para una instalación StorageGRID de nivel de producción, no utilice el servicio de hora de Windows (W32Time) en una versión de Windows anterior a Windows Server 2016. El servicio de tiempo en versiones anteriores de Windows no es lo suficientemente preciso y no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

Debe especificar la información del sistema de nombres de dominio (DNS) para el sistema StorageGRID, de modo que pueda acceder a servidores externos con nombres de host en lugar de direcciones IP.

Acerca de esta tarea

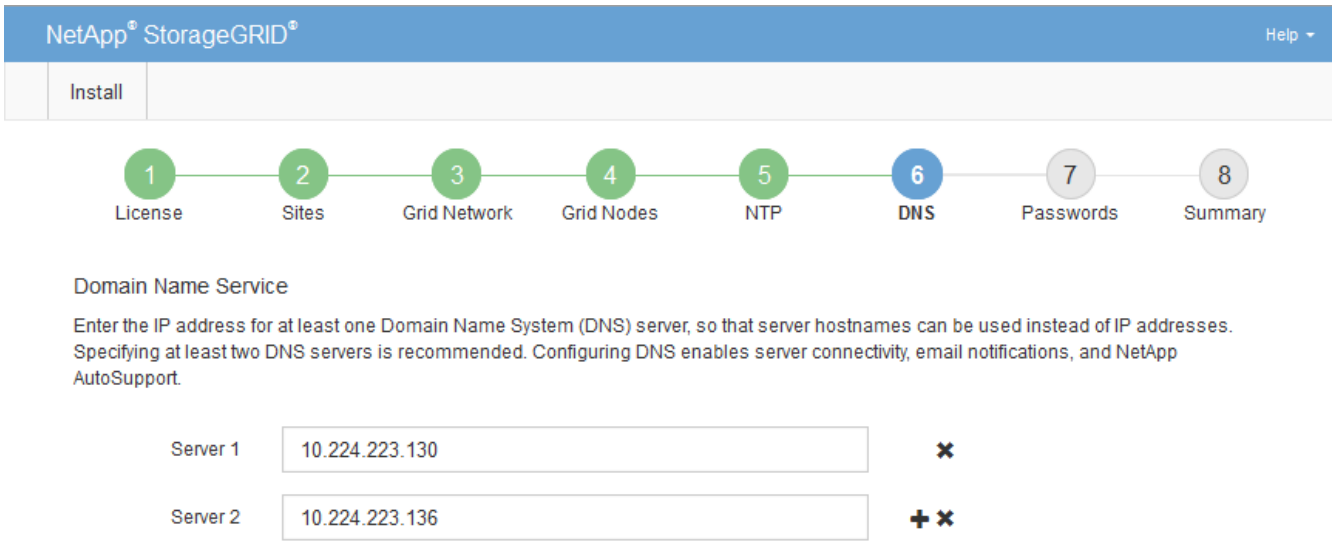
Al especificar la información del servidor DNS, se pueden utilizar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP para las notificaciones de correo electrónico y AutoSupport. Se recomienda especificar al menos dos servidores DNS.

> Proporcione de dos a seis direcciones IPv4 para los servidores DNS. Debe seleccionar los servidores DNS a los que puede acceder cada sitio localmente en el caso de que la red sea de destino. Esto es para asegurar que un sitio de Ilanded siga teniendo acceso al servicio DNS. Después de configurar la lista de servidores DNS para toda la cuadrícula, puede personalizar aún más la lista de servidores DNS para cada nodo. Para obtener detalles, consulte la información sobre cómo modificar la configuración de DNS en las instrucciones de recuperación y mantenimiento.

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 administración de grid se puede cambiar mediante Grid Manager.
- La consola de línea de comandos y las contraseñas SSH generadas aleatoriamente se almacenan en el archivo 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.

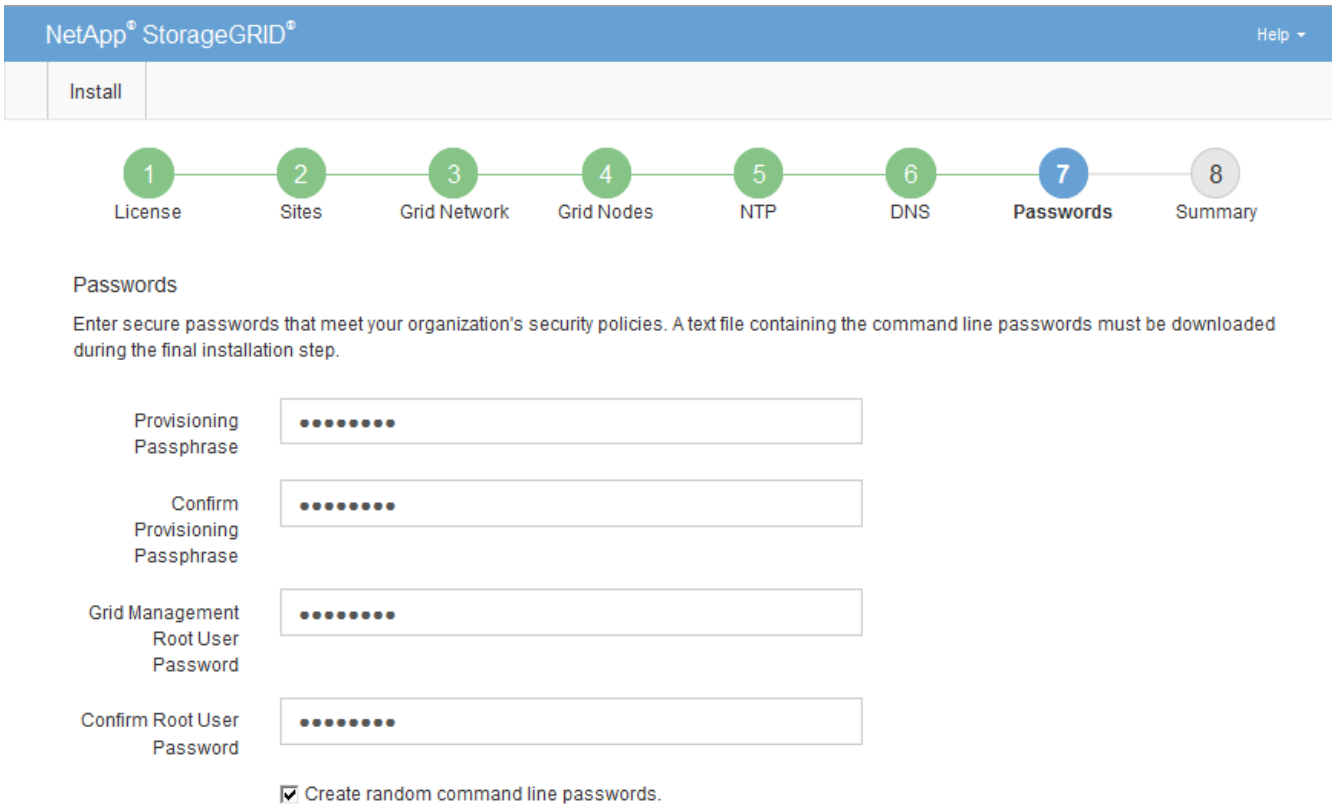
   Almacenar la clave de acceso de aprovisionamiento en un lugar seguro.

   > 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 **Contraseña de usuario raíz de Grid Management**, introduzca la contraseña que desea utilizar 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, anule la selección de 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. Anule la selección de **Crear contraseñas de línea de comandos aleatorias** sólo para cuadrículas de demostración si desea utilizar contraseñas predeterminadas para acceder a nodos de cuadrícula desde la línea de comandos mediante 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 el archivo Passwords.txt, incluido en el archivo Recovery Package.

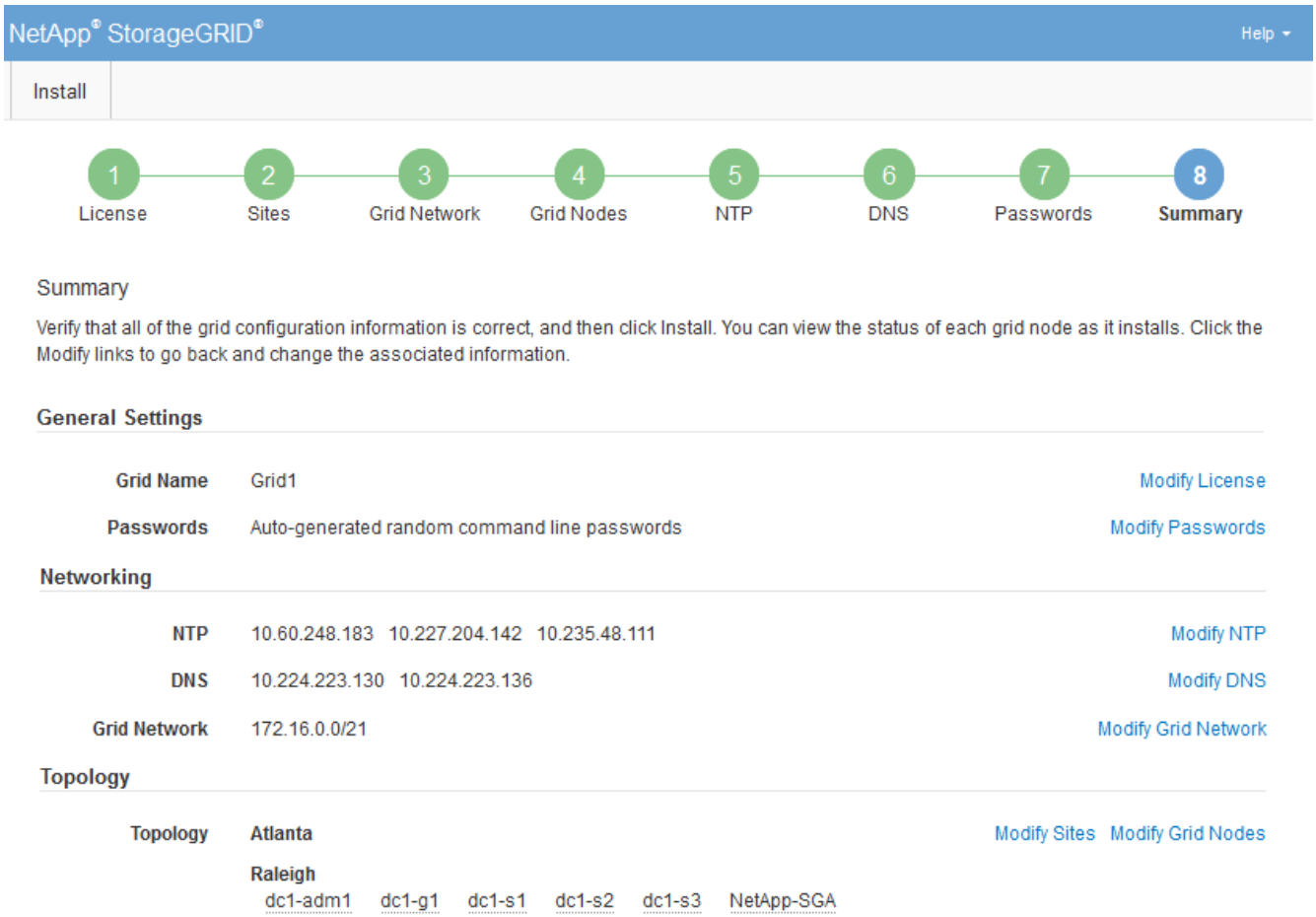
6. Haga clic en **Siguiente**.

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.

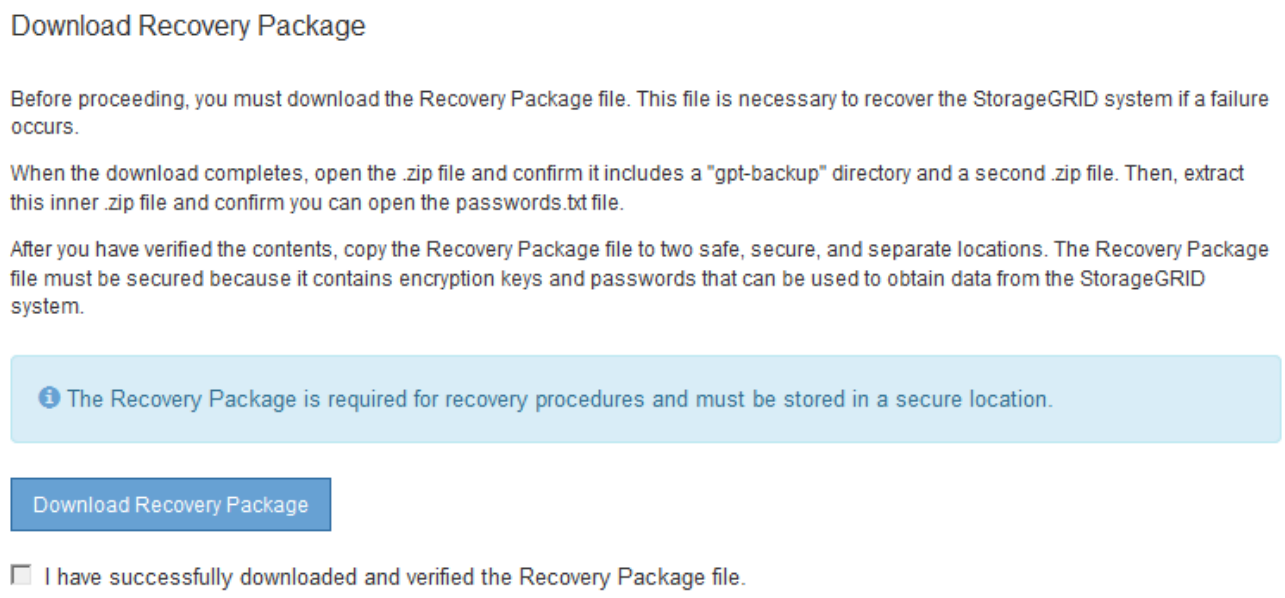
4. Haga clic en **Descargar paquete de recuperación**.

   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 puede completar la instalación y acceder al sistema StorageGRID hasta que descargue y verifique este archivo.

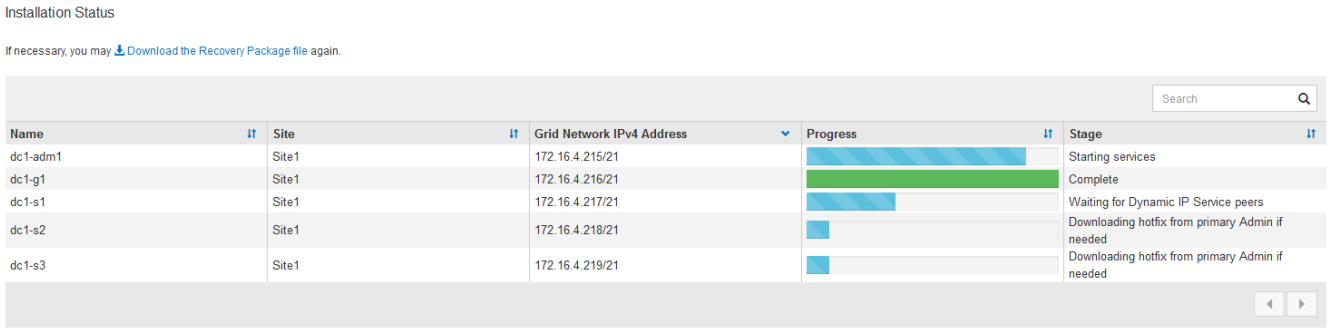
5. Compruebe que puede extraer el contenido del `.zip` archivar y, a continuación, guardarlo en dos ubicaciones seguras, seguras e independientes.

> 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. Active la casilla de verificación **he descargado y verificado correctamente el archivo de 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 es posible 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 volver a establecer estas conexiones.

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

Se proporcionan ejemplos de la función y el libro de aplicaciones de Ansible con el archivo de instalación en la carpeta /extras. 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.

Lo que necesitará

- 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 ha especificado que se deben generar contraseñas aleatorias, debe extraer 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

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 (notación de objetos JavaScript).

> 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 configura inicialmente el sistema StorageGRID y en el caso de que deba realizar una recuperación de nodo de administrador principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de API, vaya a la página web de instalación del nodo de administración principal y seleccione **Ayuda** > **Documentación de 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

Tras completar una instalación, debe realizar una serie de pasos de integración y configuración. Se requieren algunos pasos; otros son opcionales.

Tareas requeridas

- Cree una cuenta de inquilino para cada protocolo de cliente (Swift o S3) que se usará para almacenar objetos en su sistema de StorageGRID.
- Controlar el acceso al sistema configurando grupos y cuentas de usuario. Opcionalmente, puede configurar un origen de identidad federado (como Active Directory u OpenLDAP) para que pueda importar

grupos de administración y usuarios. También puede crear usuarios y grupos locales.

- Integre y pruebe las aplicaciones cliente API S3 o Swift que usará para cargar objetos en el sistema StorageGRID.
- Cuando esté listo, configure las reglas de gestión del ciclo de vida de la información (ILM) y la política de ILM que desee usar para proteger los datos de los objetos.

> Al instalar StorageGRID, se activa la política predeterminada de ILM, la política de copias base 2. Esta política incluye la regla de gestión del ciclo de vida de la información en stock (hacer 2 copias) y se aplica si no se ha activado ninguna otra política.

- Si la instalación incluye nodos de almacenamiento del dispositivo, use el software SANtricity para completar las siguientes tareas:
  - Conéctese a cada dispositivo StorageGRID.
  - Comprobar recepción de datos AutoSupport.
- Si el sistema StorageGRID incluye cualquier nodo de archivado, configure la conexión del nodo de archivado con el sistema de almacenamiento de archivado externo de destino.

> Si algún nodo de archivado utilizará Tivoli Storage Manager como sistema de almacenamiento de archivado externo, también deberá configurar Tivoli Storage Manager.

- Revise y siga las directrices de optimización del sistema StorageGRID para eliminar los riesgos de seguridad.
- Configurar las notificaciones por correo electrónico para las alertas del sistema.

Tareas opcionales

- Si desea recibir notificaciones del sistema de alarmas (heredadas), configure listas de correo y notificaciones por correo electrónico para alarmas.
- Actualice las direcciones IP del nodo de grid si han cambiado desde que planeó la implementación y generó el paquete de recuperación. Consulte información sobre el cambio de direcciones IP en las instrucciones de recuperación y mantenimiento.
- Configurar el cifrado del almacenamiento, si es necesario.
- Configure la compresión del almacenamiento para reducir el tamaño de los objetos almacenados, si es necesario.
- Configure el acceso de los clientes de auditoría. Puede configurar el acceso al sistema para fines de auditoría a través de un recurso compartido de archivos NFS o CIFS. Consulte las instrucciones para administrar StorageGRID.

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

Información relacionada

Administre StorageGRID

Use S3

Use Swift

Gestión de objetos con ILM

Supervisión y solución de problemas

Recuperación y mantenimiento

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG5600

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG6000

Notas de la versión

Endurecimiento del sistema

Revisar los registros de auditoría

Actualizar el software de

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 más información sobre cómo acceder a los archivos de registro, consulte las instrucciones para supervisar y solucionar problemas de StorageGRID. Para obtener ayuda sobre la solución de problemas de instalación del dispositivo, consulte las instrucciones de instalación y mantenimiento de los dispositivos. Si necesita ayuda adicional, póngase en contacto con el soporte técnico.

Información relacionada

Supervisión y solución de problemas

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG5600

"Soporte de NetApp"

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 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 VMware

Instalar VMware: Descripción general

La instalación de un sistema StorageGRID en un entorno de VMware incluye tres pasos principales.

1. **Preparación**: Durante la planificación y preparación, realiza las siguientes tareas:
    - Obtenga información acerca de los requisitos de hardware, software, equipos virtuales, almacenamiento y rendimiento de StorageGRID.
    - Conozca los aspectos específicos de Redes StorageGRID de este modo, puede configurar la red de forma adecuada.
    - Identifique y prepare los servidores físicos que planea utilizar para alojar los nodos de grid StorageGRID.
    - En los servidores que ha preparado:
        - Instale VMware vSphere Hypervisor
        - Configure los hosts ESX
        - Instale y configure VMware vSphere y vCenter

2. **Implementación**: Implemente nodos Grid mediante VMware vSphere Web Client. Cuando se implementan nodos de grid, se crean como parte del sistema StorageGRID y se conectan a una o varias redes.
   a. Utilice VMware vSphere Web Client, un archivo .vmdk y un conjunto de plantillas de archivos .ovf para poner en marcha los nodos basados en software como máquinas virtuales en los servidores que preparó en el paso 1.
   b. Use el instalador de dispositivos StorageGRID para poner en marcha los nodos del dispositivo StorageGRID.

> El procedimiento de instalación de StorageGRID no incluye las instrucciones de instalación e integración específicas de hardware. Para aprender a instalar dispositivos StorageGRID, consulte las instrucciones de instalación y mantenimiento del dispositivo.

3. **Configuración**: Cuando se han implementado todos los nodos, utilice el administrador de grid para configurar la cuadrícula y completar la instalación.

Estas instrucciones recomiendan un enfoque estándar para implementar y configurar un sistema StorageGRID en un entorno de VMware. Consulte también la información acerca de los siguientes enfoques alternativos:

- Use el script deploy-vsphere-ovftool.sh Bash (disponible en el archivo de instalación) para implementar nodos de grid en VMware vSphere.
- Automatice la puesta en marcha y configuración del sistema StorageGRID mediante un script de configuración Python (incluido en el archivo de instalación).
- Automatice la puesta en marcha y configuración de los nodos del grid de los dispositivos con un script de configuración Python (disponible desde el archivo de instalación o desde el instalador de dispositivos de StorageGRID).
- Si es un desarrollador avanzado de implementaciones de StorageGRID, use las API DE REST de instalación para automatizar la instalación de los nodos de grid de StorageGRID.

Planificar y preparar la instalación de VMware

Antes de instalar (VMware)

Antes de implementar nodos de grid y configurar la cuadrícula de StorageGRID, debe estar familiarizado con los pasos y los requisitos para completar el procedimiento.

Los procedimientos de puesta en marcha y configuración de StorageGRID dan por sentado que conoce la arquitectura y la funcionalidad operativa del sistema StorageGRID.

Puede implementar un solo sitio o varios sitios a la vez; sin embargo, todos los sitios deben cumplir con el requisito mínimo de tener al menos tres nodos de almacenamiento.

> StorageGRID no admite el uso de redes de área de almacenamiento virtual (San), ya que la protección de disco subyacente no es RAID de hardware.

Antes de iniciar el procedimiento de implementación y de configuración de grid del nodo, debe:

- Planifique la implementación de StorageGRID.
- Instale, conecte y configure todo el hardware necesario, incluidos los dispositivos StorageGRID, según las especificaciones.

> El procedimiento de instalación de StorageGRID no incluye las instrucciones de instalación e integración específicas de hardware. Para aprender a instalar dispositivos StorageGRID, consulte las instrucciones de instalación y mantenimiento del dispositivo.

- Comprenda el opciones de red disponibles y cómo se debe implementar cada opción de red en los nodos de grid.
- Recopile toda la información de la red con antelación. A menos que utilice DHCP, recopile las direcciones IP para asignar a cada nodo de grid y las direcciones IP de los servidores del sistema de nombres de dominio (DNS) y del protocolo de hora de red (NTP) que se utilizarán.
- Decida qué herramientas de implementación y configuración disponibles desea utilizar.

Información relacionada

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG5600

Materiales requeridos

Antes de instalar StorageGRID, debe recopilar y preparar los materiales necesarios.

Elemento	Notas
Licencia de StorageGRID de NetApp	Debe tener una licencia de NetApp válida y con firma digital. **Nota**: El archivo de instalación de StorageGRID incluye una licencia gratuita que no proporciona ningún derecho de asistencia para el producto.
Archivo de instalación de StorageGRID	Debe Descargue el archivo de instalación de StorageGRID y extraiga los archivos.
Software y documentación de VMware	Durante la instalación, se usa VMware vSphere Web Client para implementar nodos de grid virtual en máquinas virtuales. Para las versiones compatibles, consulte la matriz de interoperabilidad.
Portátil de servicio	El sistema StorageGRID se instala mediante un laptop de mantenimiento.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

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

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 instrucción Caution/MustRead, léala y active 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 para 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.

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.
	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.
	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.

Ruta y nombre de archivo	Descripción
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede utilizar estos esquemas para confirmar que cualquier código que haya escrito para utilizar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no dispone de un entorno StorageGRID que no sea de producción para la comprobación de compatibilidad de actualizaciones.

Información relacionada

Recuperación y mantenimiento

Requisitos de software

Puede usar una máquina virtual para alojar cualquier tipo de nodo de grid StorageGRID. Se necesita una máquina virtual para cada nodo de grid instalado en el servidor VMware.

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 grid de StorageGRID.

Para ver las versiones compatibles del hipervisor VMware vSphere y el software VMware vCenter Server, consulte la matriz de interoperabilidad.

Para conocer los pasos necesarios para instalar estos productos de VMware, consulte la documentación de VMware.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

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.

Para obtener información sobre los servidores admitidos, consulte la matriz de interoperabilidad.

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 cómo gestionar el almacenamiento de metadatos de objetos, aumentar la configuración de espacio reservado de metadatos y supervisar el uso de la CPU y la memoria, consulte las instrucciones para administrar, supervisar 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 la información sobre los requisitos de almacenamiento.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Los requisitos de almacenamiento y rendimiento

Administre StorageGRID

Supervisión y solución de problemas

Actualizar el software de

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 ONTAP de NetApp

Si va a implementar un nodo de StorageGRID como máquina virtual con almacenamiento asignado desde un sistema ONTAP de NetApp, debe confirmar que el volumen no tiene habilitada una política de organización en niveles de FabricPool. 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 máquinas virtuales. 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 puerta de enlace, 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 los nodos de grid StorageGRID deben cumplir con diferentes requisitos, en función de los tipos de nodos.

Las snapshots de disco no se pueden utilizar para restaurar nodos de grid. En su lugar, consulte los procedimientos de recuperación y mantenimiento de 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 puerta de enlace	LUN DE 100 GB PARA SO
Nodo de archivado	LUN DE 100 GB PARA SO

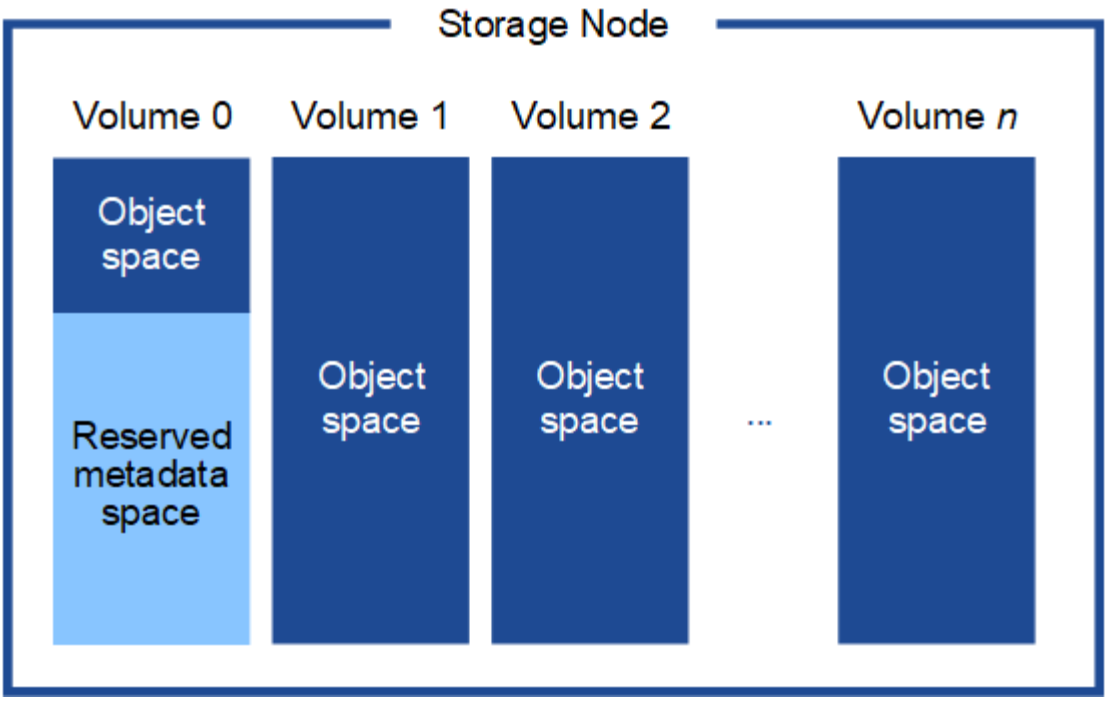
Según el nivel de auditoría configurado, el tamaño de las entradas de usuario, como el nombre de la clave de objeto S3 y la cantidad de datos del registro de auditoría que se deben conservar, es posible que deba aumentar el tamaño de la LUN del registro de auditoría de cada nodo de administración. Como regla general, un grid genera aproximadamente 1 KB de datos de auditoría por operación de S3, lo que significa que una LUN de 200 GB admitirá 70 millones de operaciones diarias 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 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 está instalando un nuevo sistema StorageGRID 11.6 y cada nodo de almacenamiento tiene 128 GB o más de RAM, debe asignar 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.

Información relacionada

Recuperación y mantenimiento

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 host, almacén de datos y red para cada máquina virtual del nodo de grid 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.
- Si no utiliza DHCP, los detalles de red necesarios para cada nodo de grid (dirección IP, puerta de enlace y máscara de red).
- Si no utiliza DHCP, la dirección IP del nodo de administración principal en la red de cuadrícula. Consulte «'Cómo descubren los nodos de grid el nodo de administración principal'» para obtener 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).
- 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 «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 del sistema de nombres de dominio (DNS)

Información relacionada

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

Los requisitos de almacenamiento y rendimiento

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 normalmente a través de 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 cualquier nodo de almacenamiento del dispositivo StorageGRID, consulte las instrucciones de instalación y mantenimiento del dispositivo.

Opcionalmente, puede reasignar puertos de nodo o aumentar la configuración de CPU o memoria del nodo antes de encenderlo.

Lo que necesitará

- 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 manualmente VMware Tools.

- 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-archive.ovf vsphere-archive.mf	El archivo de plantilla y el archivo de manifiesto para un nodo de archivado.
vsphere-gateway.ovf vsphere-gateway.mf	El archivo de plantilla y el archivo de manifiesto para un nodo de puerta de enlace.
vsphere-storage.ovf vsphere-storage.mf	El archivo de plantilla y el archivo de manifiesto para un nodo de almacenamiento.

- 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 máquinas virtuales. 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 va a implementar un nodo de StorageGRID como máquina virtual con almacenamiento asignado desde un sistema ONTAP de NetApp, debe confirmar que el volumen no tiene habilitada una política de organización en niveles de FabricPool. 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 reasignar algunos 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
   sphere-primary-admin.ovf
   sphere-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 del 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 seleccionado para la red de cuadrícula.
   - Si utiliza Client Network, seleccione una red de destino diferente en el entorno de vSphere. Si no utiliza la red de cliente, seleccione el mismo destino seleccionado para la red de cuadrícula.

7. En **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. 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**.

   c. 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 DESHABILITADA e introduzca **0.0.0.0** para la IP de 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 de cliente, seleccione DISABLED (DESACTIVADO) e introduzca **0.0.0.0** para la IP de la red de 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 habitualmente en los entornos de VMware y son más fáciles de gestionar, mientras que los RDM pueden 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 reasigne los puertos utilizados en los puntos finales 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_REMAPP_INBOUND y no especifica un valor para PORT_REMAPP, las comunicaciones salientes para el puerto no se modifican.

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. Seleccione **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.

Lo que necesitará

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

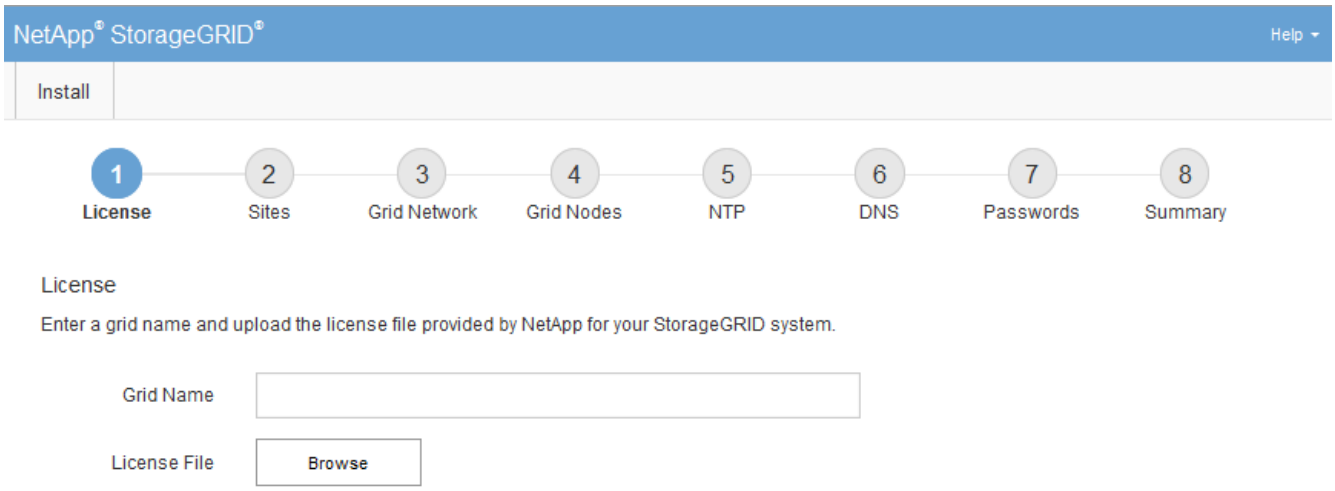
   También puede acceder a Grid Manager en el puerto 8443:

   `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. Haga clic en **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

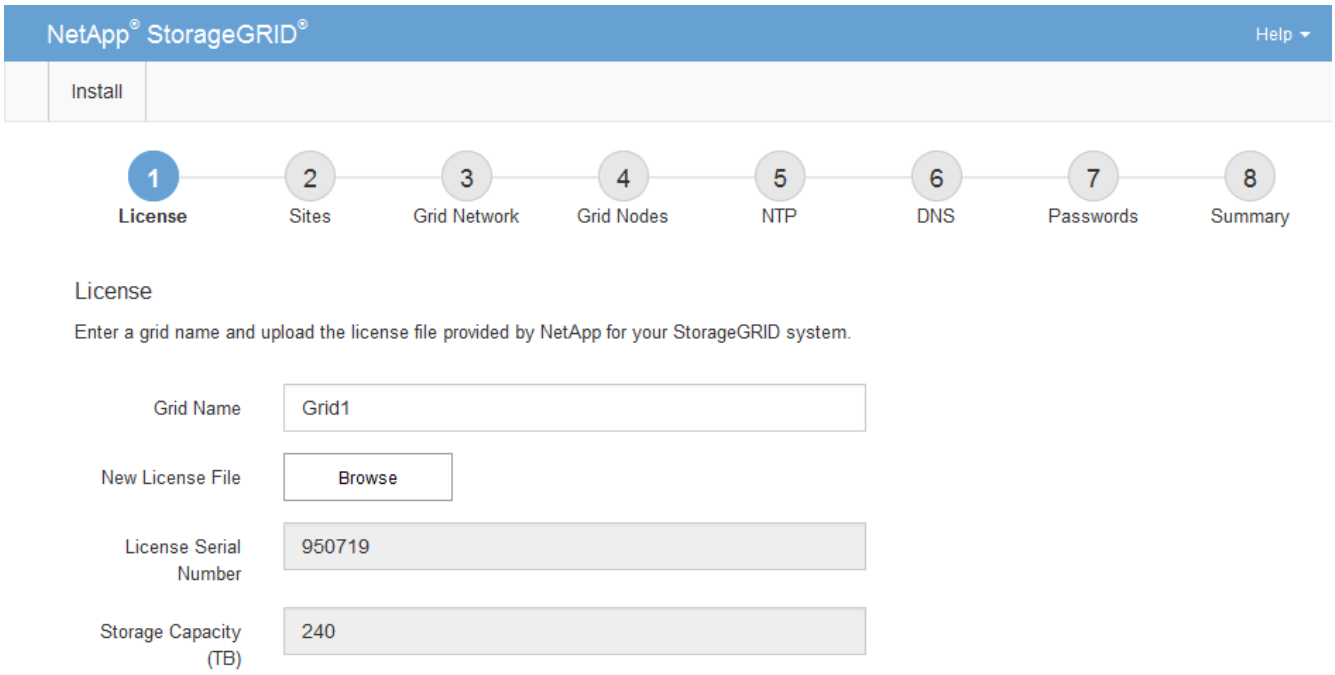
1. En la página Licencia, introduzca un nombre significativo para su sistema StorageGRID en **Nombre de cuadrícula**.

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

2. Haga clic en **Browse**, busque el archivo de licencia de NetApp (`NLFunique_id.txt`) Y haga clic en **Abrir**.

   El archivo de licencia se valida y se muestran el número de serie y la capacidad de almacenamiento con licencia.

   > 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. Haga clic en **Siguiente**.

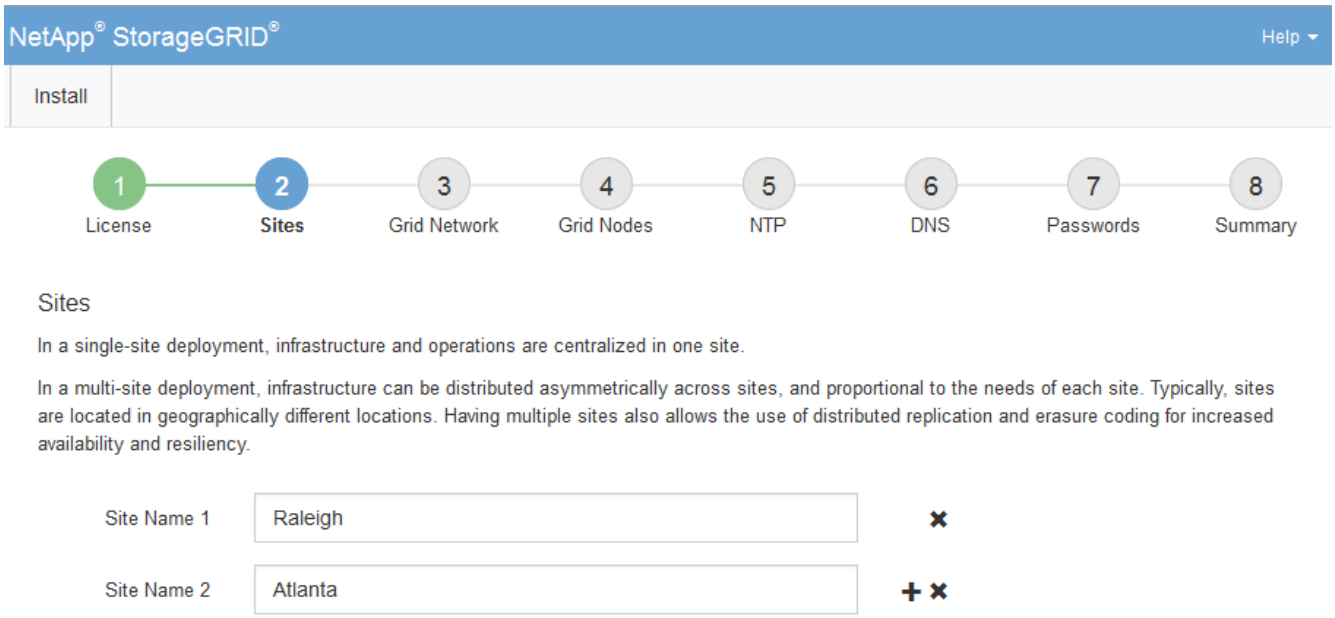
Agregar sitios

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

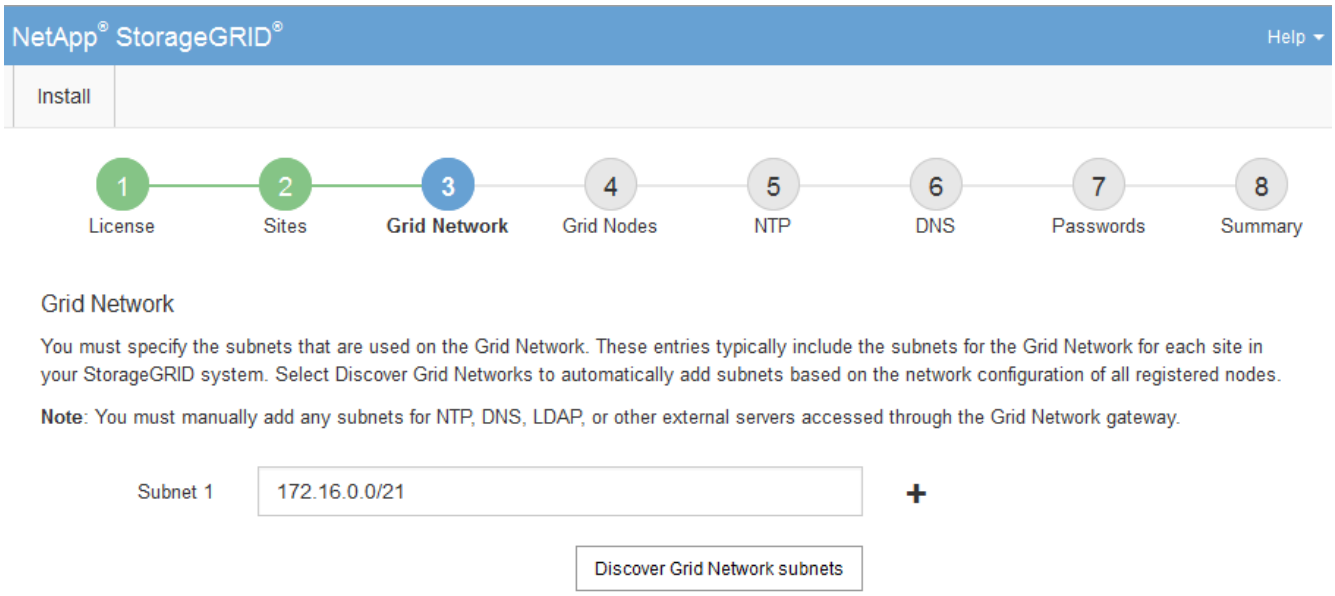
Las entradas de subred incluyen las subredes para la red de cuadrícula de cada sitio del sistema StorageGRID, junto con las subredes a las que se debe acceder a través de la red de cuadrícula.

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.

Lo que necesitará

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

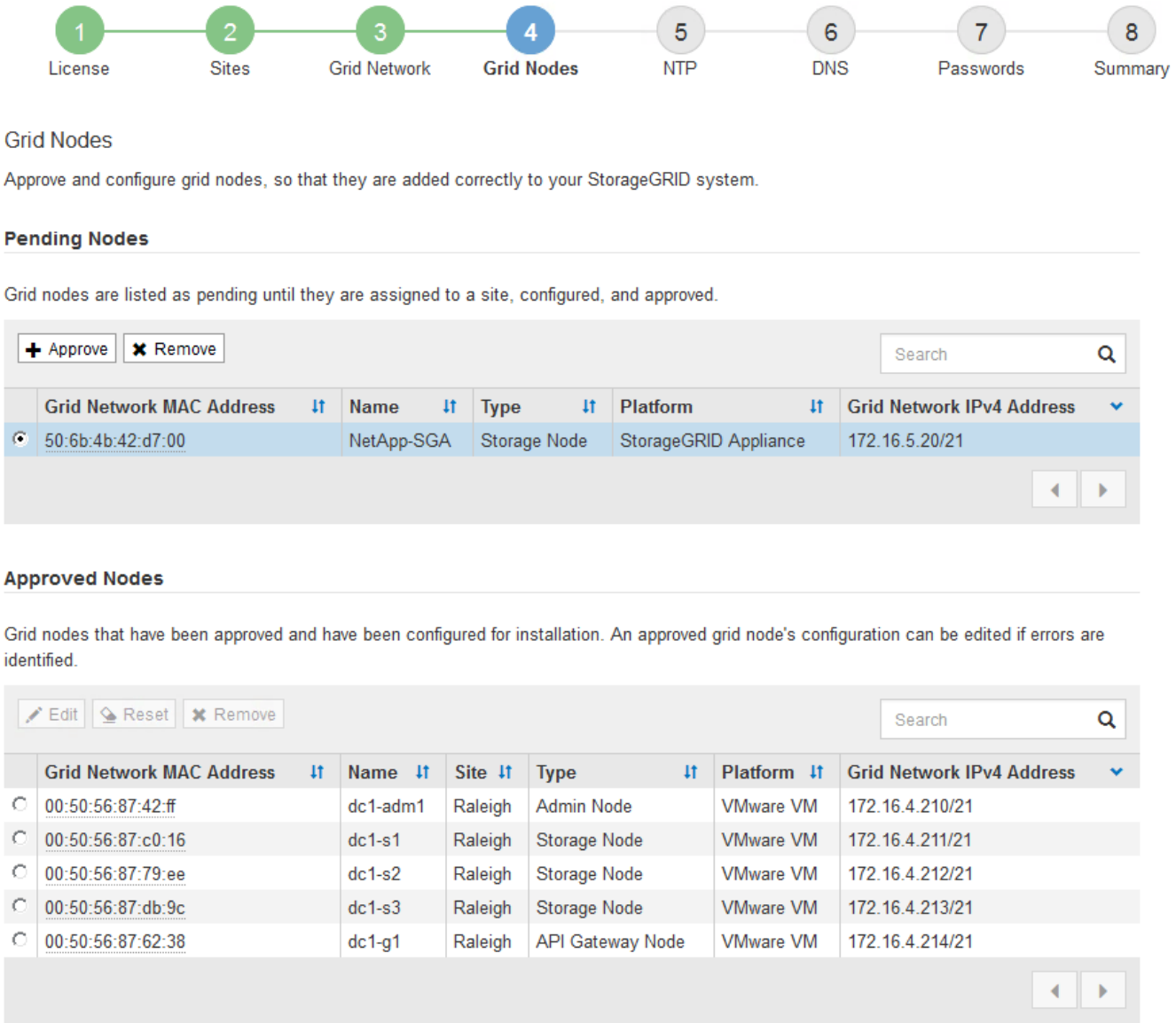
> Es más eficiente realizar una instalación única de todos los nodos, en lugar de instalar algunos ahora y algunos nodos más adelante.

Pasos

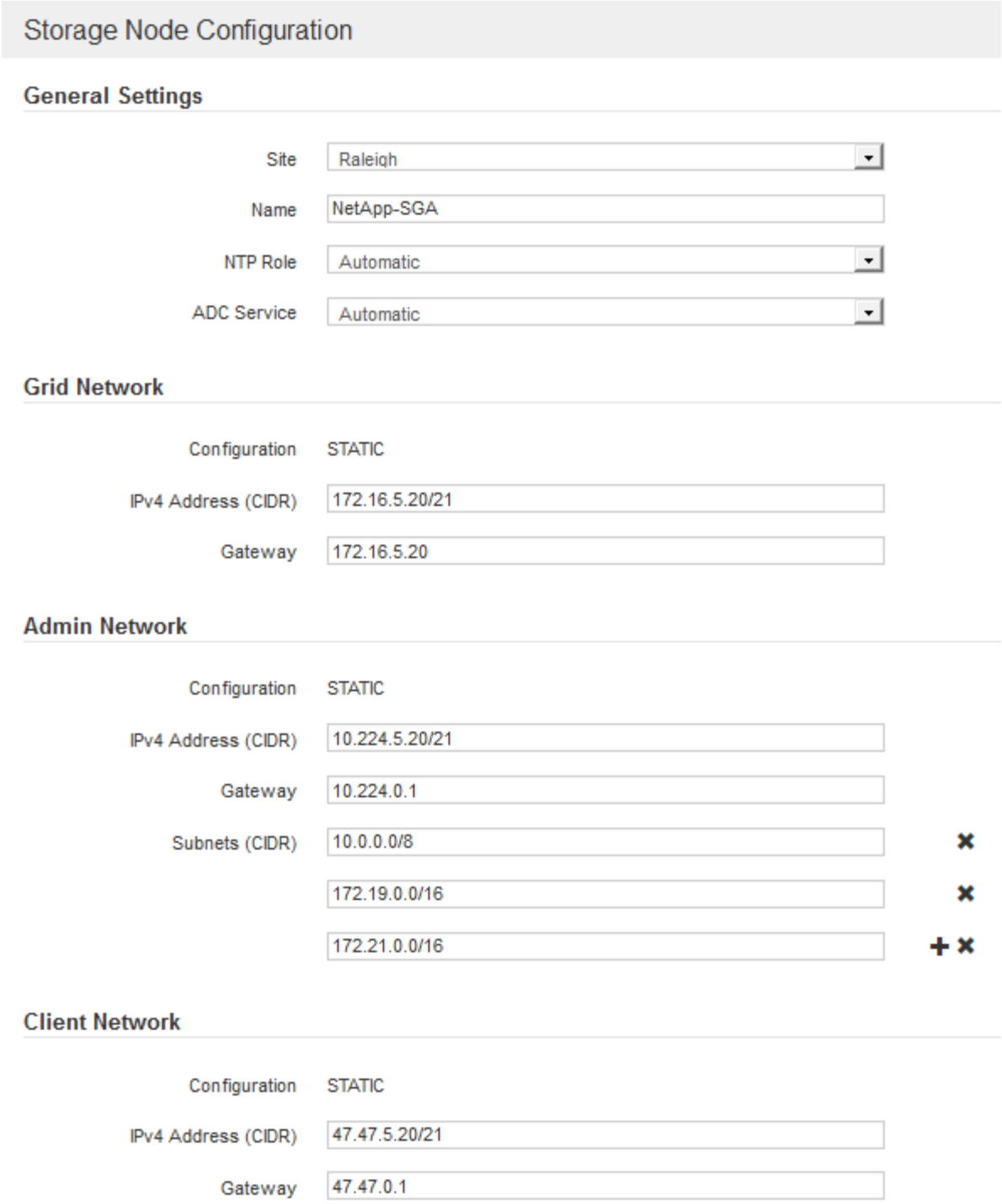
1. Revise la lista Pending Nodes y confirme que se muestran todos los nodos de grid que ha implementado.

   > 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 sitio con el que se asociará este nodo de red.
- **Nombre**: El nombre que se asignará al nodo y el nombre que se mostrará en el Gestor de cuadrícula. El nombre predeterminado es el nombre que especifique cuando configure el nodo. Durante este paso del proceso de instalación, puede cambiar el nombre según sea necesario.

> Una vez finalizada la instalación, no puede cambiar el nombre del nodo.

> 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.

- **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 haberlo implementado.

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 del 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 el Gestor de cuadrícula: Si el nodo aparece en la tabla nodos aprobados, restablezca 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 IP Configuration.

   Para obtener información adicional, consulte las instrucciones de instalación y mantenimiento del 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.

   Dispositivos: 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 del Administrador de grid. En su lugar, debe seguir estos pasos:

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

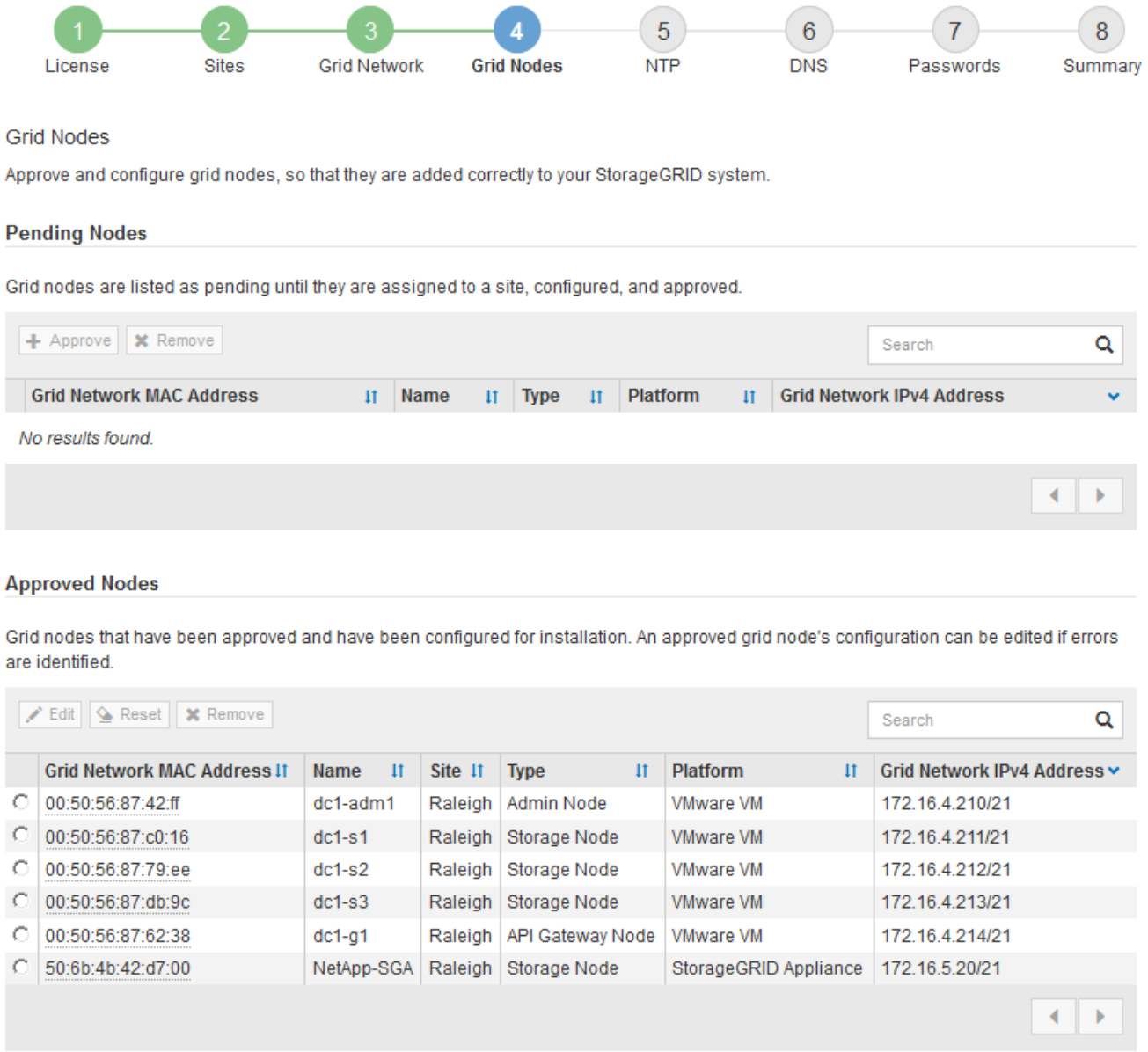
      El reinicio puede tardar varios minutos.

   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 el Gestor de cuadrícula: Si el nodo aparece en la tabla nodos aprobados, restablezca 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 IP Configuration.

      Para obtener más información, consulte las instrucciones de instalación y mantenimiento del dispositivo.

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

"Límite de soporte para configurar el servicio de tiempo de Windows para entornos de alta precisión"

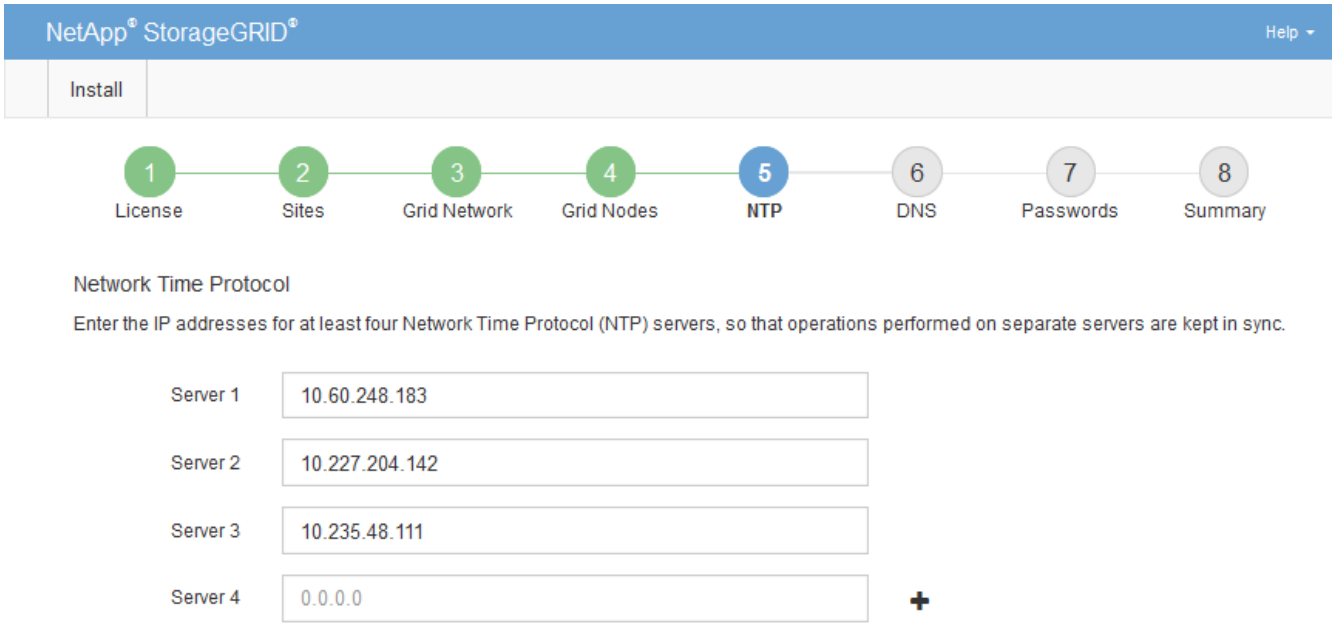
Los nodos a los que asignó previamente roles NTP primarios utilizan los servidores NTP externos.

> 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 del sistema de nombres de dominio

Debe especificar la información del sistema de nombres de dominio (DNS) para el sistema StorageGRID, de modo que pueda acceder a servidores externos con nombres de host en lugar de direcciones IP.

Acerca de esta tarea

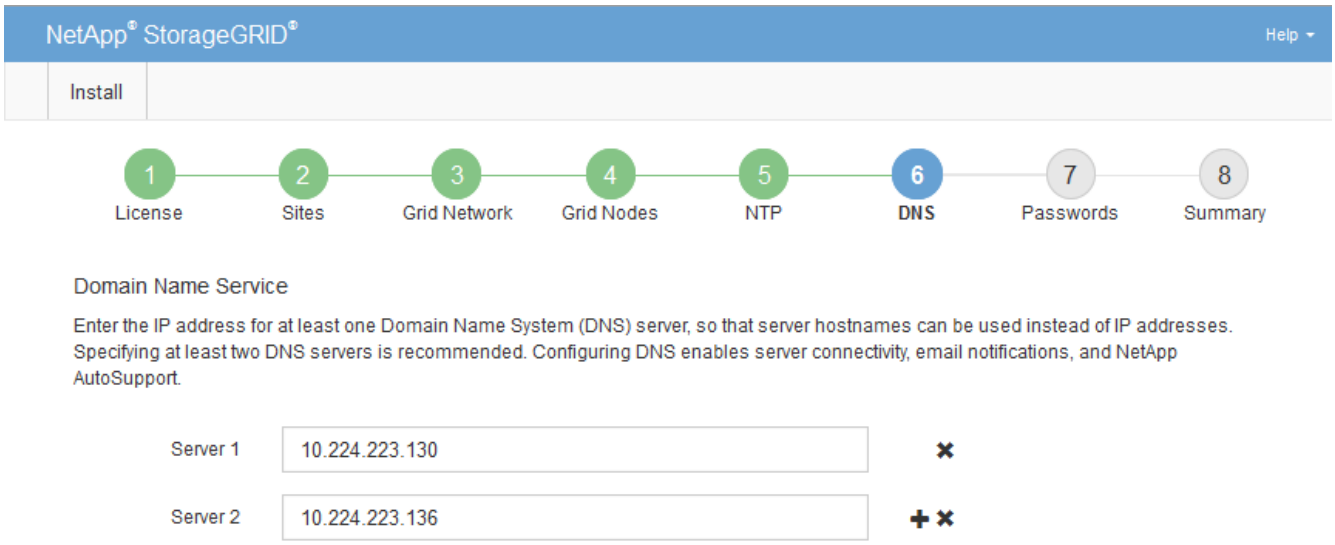
Al especificar la información del servidor DNS, se pueden utilizar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP para las notificaciones de correo electrónico y AutoSupport. Se recomienda especificar al menos dos servidores DNS.

> Proporcione de dos a seis direcciones IPv4 para los servidores DNS. Debe seleccionar los servidores DNS a los que puede acceder cada sitio localmente en el caso de que la red sea de destino. Esto es para asegurar que un sitio de Ilanded siga teniendo acceso al servicio DNS. Después de configurar la lista de servidores DNS para toda la cuadrícula, puede personalizar aún más la lista de servidores DNS para cada nodo. Para obtener detalles, consulte la información sobre cómo modificar la configuración de DNS en las instrucciones de recuperación y mantenimiento.

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**.

Información relacionada

Recuperación y mantenimiento

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 administración 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.

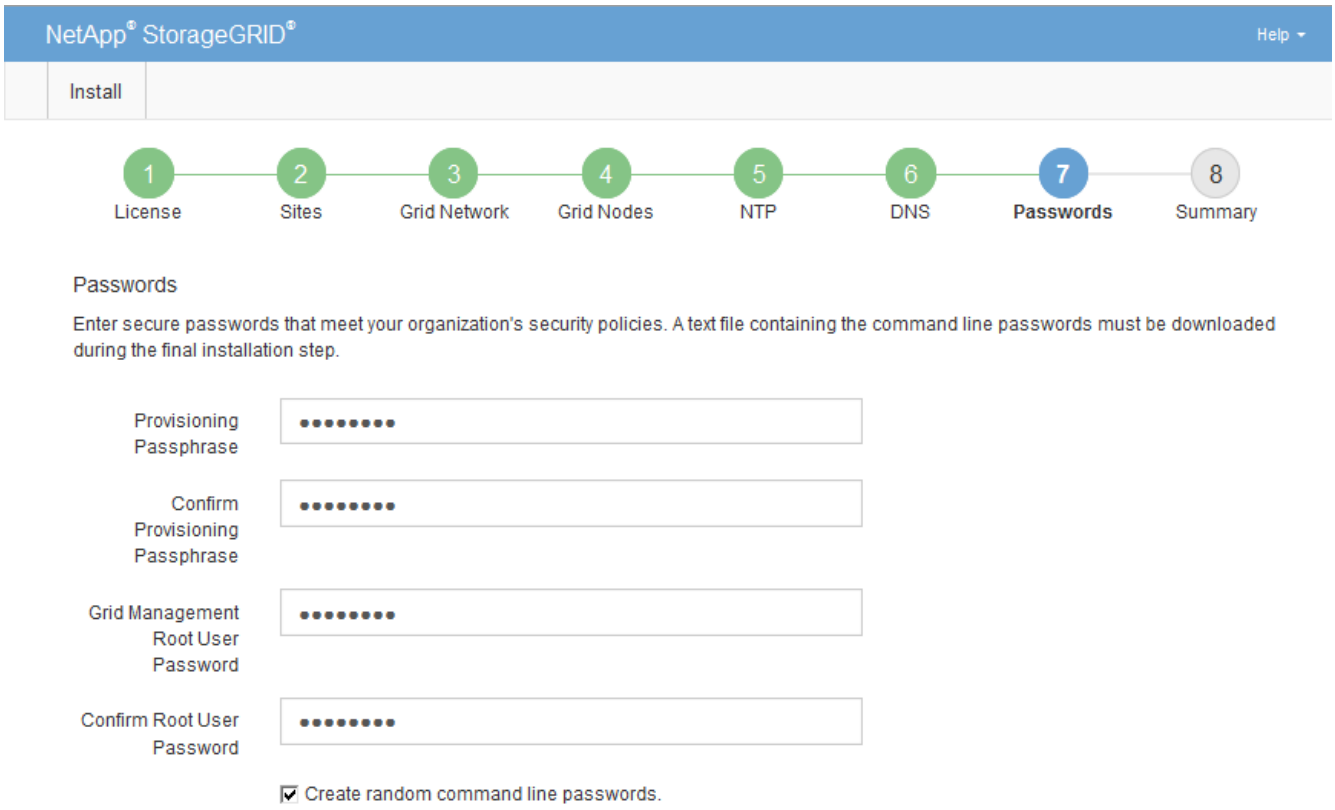
   Almacenar la clave de acceso de aprovisionamiento en un lugar seguro.

   > 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 **Contraseña de usuario raíz de Grid Management**, introduzca la contraseña que desea utilizar 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, anule la selección de 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. Anule la selección de **Crear contraseñas de línea de comandos aleatorias** sólo para cuadrículas de demostración si desea utilizar contraseñas predeterminadas para acceder a nodos de cuadrícula desde la línea de comandos mediante 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.

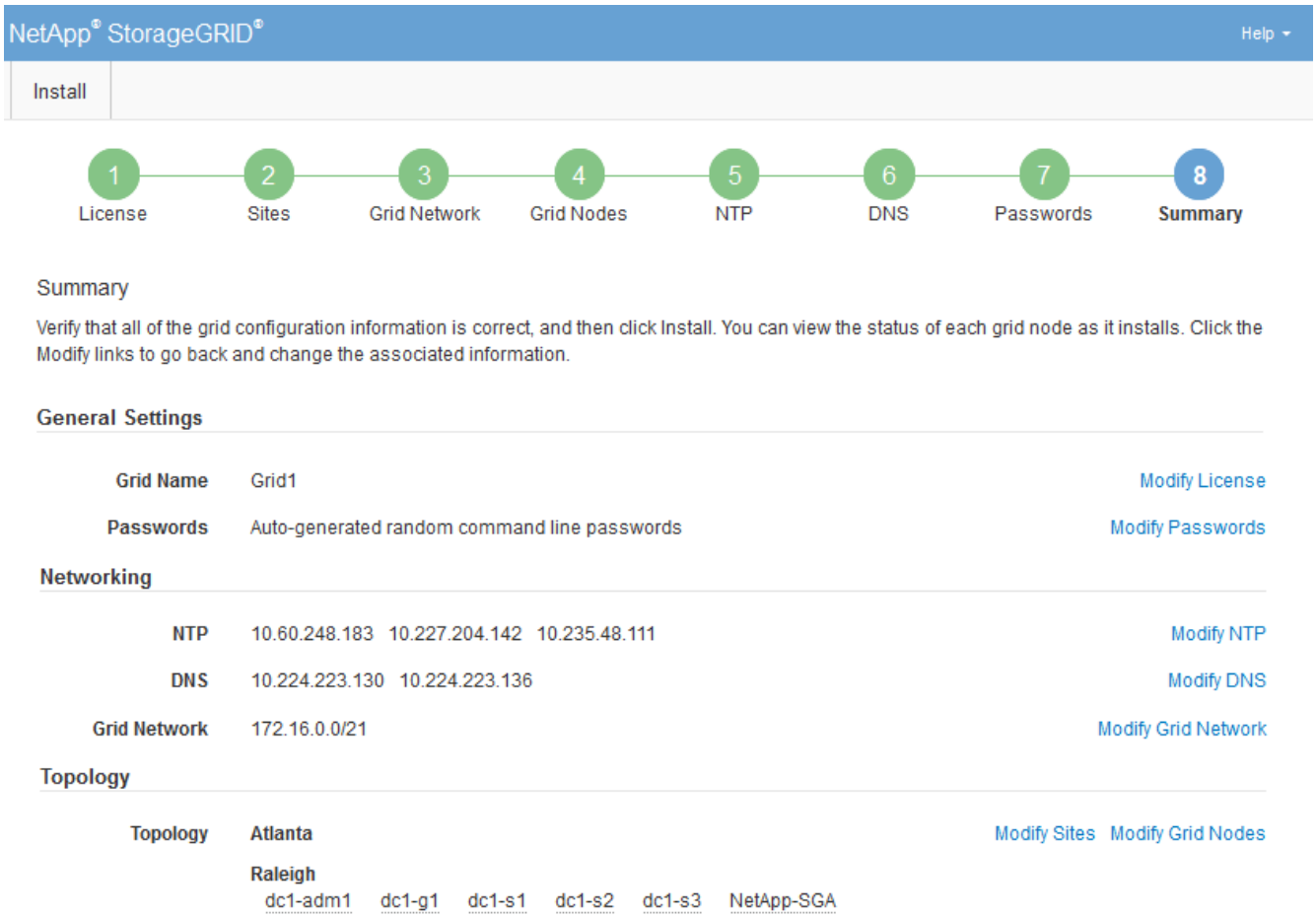
6. Haga clic en **Siguiente**.

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.

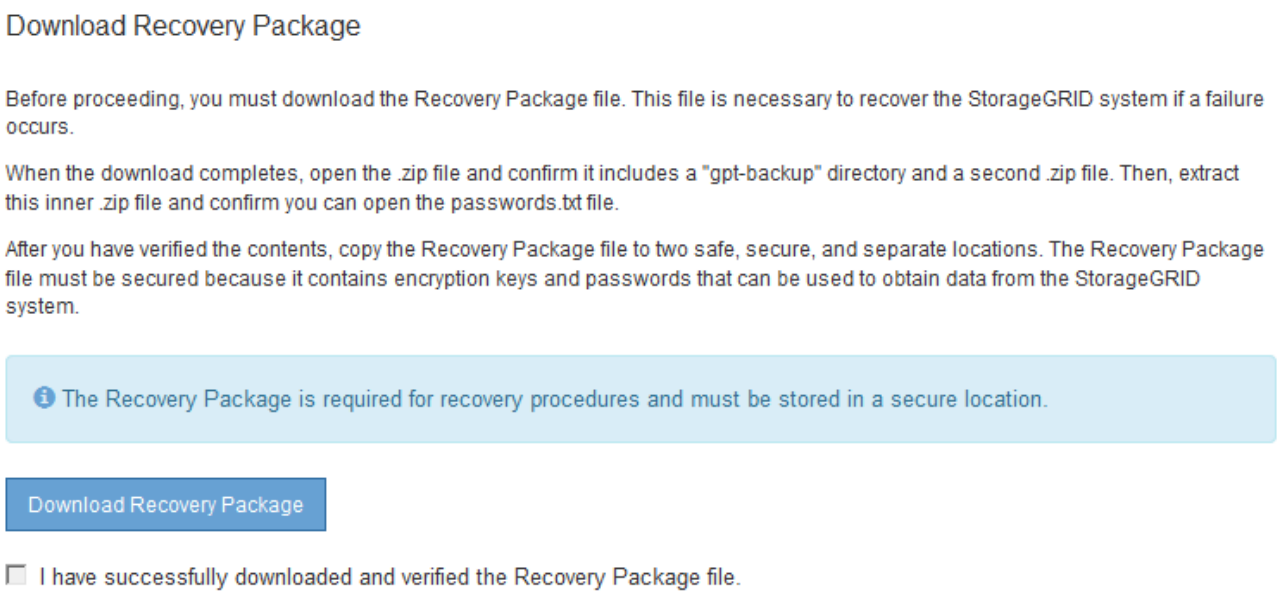
4. Haga clic en **Descargar paquete de recuperación**.

   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 puede completar la instalación y acceder al sistema StorageGRID hasta que descargue y verifique este archivo.

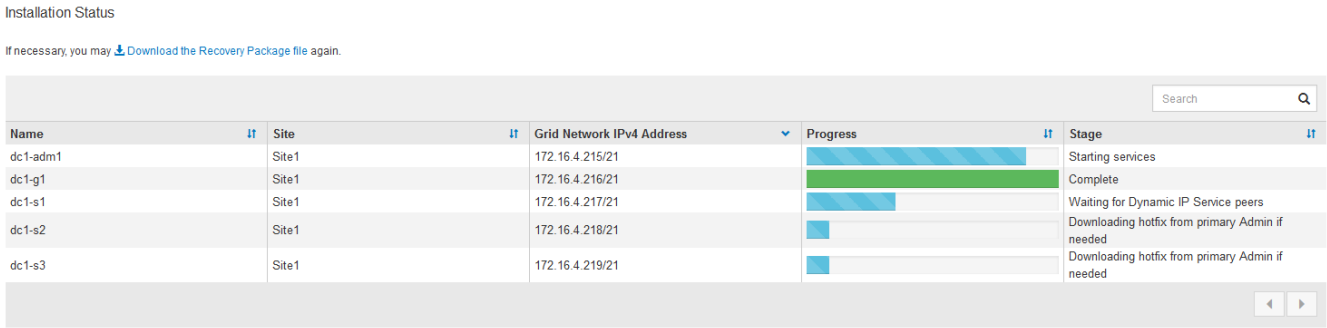
5. Compruebe que puede extraer el contenido del `.zip` archivar y, a continuación, guardarlo en dos ubicaciones seguras, seguras e independientes.

> 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. Active la casilla de verificación **he descargado y verificado correctamente el archivo de 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 es posible 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 volver a establecer estas conexiones.

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

Use VMware vSphere para automatizar la instalación de los nodos de grid.

Lo que necesitará

- 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.

Nombre de archivo	Descripción
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.
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 que se puede 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. Haga 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. Los valores de MTU no tienen que ser iguales 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 reasigne 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_REMAPP_INBOUND pero no especifica un valor para PORT_REMAPP, las comunicaciones salientes para el puerto no se modifican.

> No reasigne 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.

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 de bash y el archivo de configuración deploy-vsphere-ovftool.ini que modificó para automatizar la puesta en marcha de los nodos de grid StorageGRID en VMware vSphere.

Lo que necesitará

- 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
```

El despliegue se completa cuando el estado de cada nodo es "'pasado'".

```
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.

Lo que necesitará

- 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

Nombre de archivo	Descripción
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

Durante el proceso de configuración se genera un archivo .zip del paquete de recuperación que 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 ha especificado que se deben generar contraseñas aleatorias, debe extraer el archivo Passwords.txt y buscar las contraseñas necesarias 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

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 (notación de objetos JavaScript).

> 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 configura inicialmente el sistema StorageGRID y en el caso de que deba realizar una recuperación de nodo de administrador principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de API, vaya a la página web de instalación del nodo de administración principal y seleccione **Ayuda** > **Documentación de 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

Tras completar una instalación, debe realizar una serie de pasos de integración y configuración. Se requieren algunos pasos; otros son opcionales.

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 usará para almacenar objetos en su sistema de StorageGRID.
- Controlar el acceso al sistema configurando grupos y cuentas de usuario. Opcionalmente, puede configurar un origen de identidad federado (como Active Directory u OpenLDAP) para que pueda importar grupos de administración y usuarios. También puede crear usuarios y grupos locales.
- Integre y pruebe las aplicaciones cliente API S3 o Swift que usará para cargar objetos en el sistema StorageGRID.
- Cuando esté listo, configure las reglas de gestión del ciclo de vida de la información (ILM) y la política de ILM que desee usar para proteger los datos de los objetos.

  > Al instalar StorageGRID, se activa la política predeterminada de ILM, la política de copias base 2. Esta política incluye la regla de gestión del ciclo de vida de la información en stock (hacer 2 copias) y se aplica si no se ha activado ninguna otra política.

- Si la instalación incluye nodos de almacenamiento del dispositivo, use el software SANtricity para completar las siguientes tareas:
  - Conéctese a cada dispositivo StorageGRID.
  - Comprobar recepción de datos AutoSupport.
- Si el sistema StorageGRID incluye cualquier nodo de archivado, configure la conexión del nodo de archivado con el sistema de almacenamiento de archivado externo de destino.

Si algún nodo de archivado utilizará Tivoli Storage Manager como sistema de almacenamiento de archivado externo, también deberá configurar Tivoli Storage Manager.

- Revise y siga las directrices de optimización del sistema StorageGRID para eliminar los riesgos de seguridad.
- Configurar las notificaciones por correo electrónico para las alertas del sistema.

Tareas opcionales

- Si desea recibir notificaciones del sistema de alarmas (heredadas), configure listas de correo y notificaciones por correo electrónico para alarmas.
- Actualice las direcciones IP del nodo de grid si han cambiado desde que planeó la implementación y generó el paquete de recuperación. Consulte información sobre el cambio de direcciones IP en las instrucciones de recuperación y mantenimiento.
- Configurar el cifrado del almacenamiento, si es necesario.
- Configure la compresión del almacenamiento para reducir el tamaño de los objetos almacenados, si es necesario.
- Configure el acceso de los clientes de auditoría. Puede configurar el acceso al sistema para fines de auditoría a través de un recurso compartido de archivos NFS o CIFS. Consulte las instrucciones para administrar StorageGRID.

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

Información relacionada

Administre StorageGRID

Use S3

Use Swift

Gestión de objetos con ILM

Supervisión y solución de problemas

Recuperación y mantenimiento

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG5600

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG6000

Notas de la versión

Endurecimiento del sistema

Revisar los registros de auditoría

Actualizar el software de

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)

Para obtener más información sobre cómo acceder a los archivos de registro, consulte Instrucciones para la supervisión y resolución de problemas de StorageGRID. Para obtener ayuda sobre la solución de problemas de instalación del dispositivo, consulte las instrucciones de instalación y mantenimiento de los dispositivos. Si necesita ayuda adicional, póngase en contacto con el soporte técnico.

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG5600

"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 implementando 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.

Realizar la administración del sistema

Administre StorageGRID

Administrar StorageGRID: Descripción general

Siga estas instrucciones para configurar y administrar un sistema StorageGRID.

Acerca de estas instrucciones

Estas instrucciones describen cómo usar Grid Manager para configurar grupos y usuarios, crear cuentas de inquilino para permitir que las aplicaciones de cliente S3 y Swift almacenen y recuperen objetos, configurar y gestionar redes StorageGRID, configurar AutoSupport, gestionar los ajustes de nodo, etc.

Estas instrucciones están dirigidas al personal técnico que configurará, administre y prestará soporte técnico para un sistema StorageGRID después de que se haya instalado.

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.

Empiece a usar StorageGRID

Requisitos del navegador web

Debe utilizar un navegador web compatible.

Navegador Web	Versión mínima admitida
Google Chrome	96
Microsoft Edge	96
Mozilla Firefox	94

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.

Lo que necesitará

- Tiene sus credenciales de inicio de sesión.
- Tiene la dirección URL de Grid Manager.
- Está utilizando un navegador web compatible.
- Las cookies están habilitadas en su navegador web.
- Tiene permisos de acceso específicos.

Acerca de esta tarea

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 del administrador 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.

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.

Pasos

1. Inicie un explorador web compatible.
2. En la barra de direcciones del navegador, introduzca la dirección URL de Grid Manager:

   `https://FQDN_or_Admin_Node_IP/`

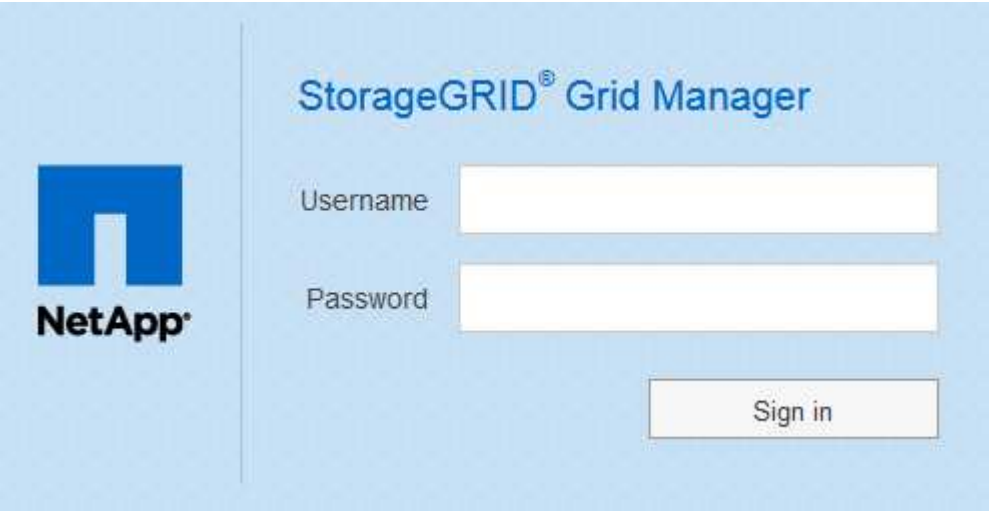
   donde *`FQDN_or_Admin_Node_IP`* Es un nombre de dominio completo o la dirección IP de un nodo de administrador o la dirección IP virtual de un grupo ha de nodos de administrador.

   Si debe acceder a Grid Manager en un puerto distinto del puerto estándar para HTTPS (443), introduzca lo siguiente, donde *`FQDN_or_Admin_Node_IP`* Es un nombre de dominio completo o una dirección IP y el puerto es el número de puerto:

   `https://FQDN_or_Admin_Node_IP:port/`

3. Si se le solicita una alerta de seguridad, instale el certificado mediante el asistente de instalación del explorador (consulte Acerca de los certificados de seguridad).
4. Inicie sesión en Grid Manager:
   - Si su sistema StorageGRID no utiliza el inicio de sesión único (SSO):
     i. Introduzca su nombre de usuario y contraseña para el administrador de grid.

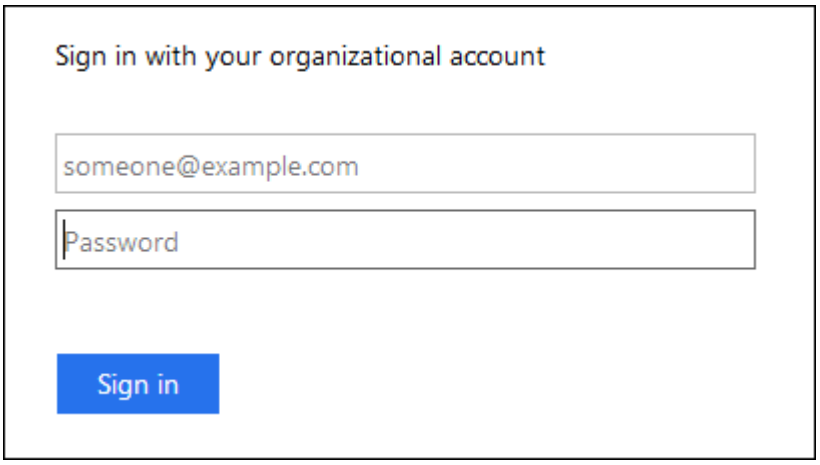
ii. Seleccione **Iniciar sesión**.



- Si SSO está habilitado para el sistema StorageGRID y esta es la primera vez que accede a la URL en este navegador:

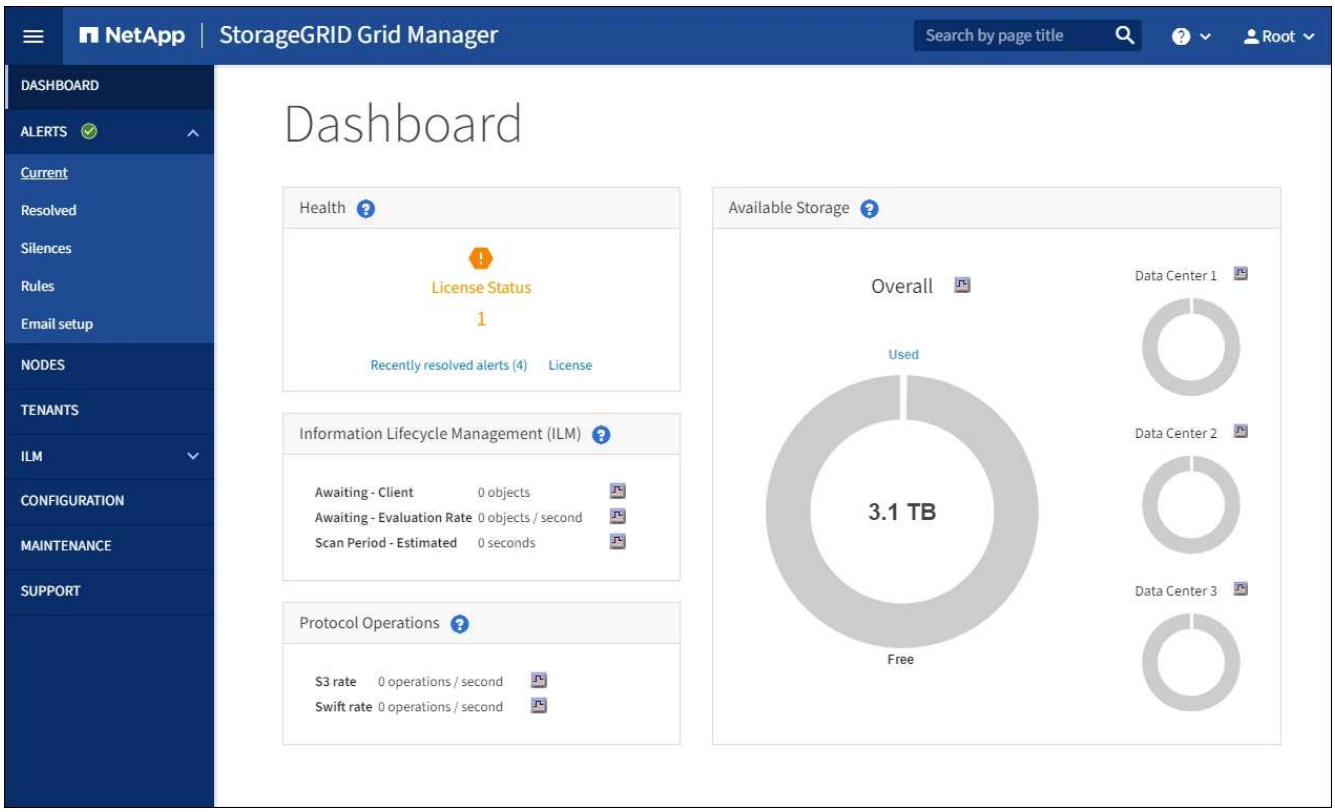
  i. Seleccione **Iniciar sesión**. Puede dejar el campo ID de cuenta en blanco.

  ii. Introduzca sus credenciales de SSO estándar en la página de inicio de sesión con SSO de su organización. Por ejemplo:



- Si SSO está habilitado para el sistema StorageGRID y ya ha accedido previamente a Grid Manager o a una cuenta de inquilino:
  i. Realice una de las siguientes acciones:
    - Introduzca **0** (el ID de cuenta de Grid Manager) y seleccione **Iniciar sesión**.
    - Seleccione **Grid Manager** si aparece en la lista de cuentas recientes y seleccione **Iniciar sesión**.

  ii. Inicie sesión con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización. Cuando haya iniciado sesión, aparecerá la página de inicio de Grid Manager, que incluye el Panel. Para saber qué información se proporciona, consulte Consulte la consola.



5. Si desea iniciar sesión en otro nodo de administración:

Opción	Pasos
SSO no está habilitado	a. 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. b. Introduzca su nombre de usuario y contraseña para el administrador de grid. c. Seleccione **Iniciar sesión**.
SSO habilitado	En la barra de direcciones del navegador, introduzca el nombre de dominio completo o la dirección IP del otro nodo de administración. Si inició sesión en un nodo de administrador, puede acceder a otros nodos de administrador sin tener que volver a iniciar sesión. Sin embargo, si su sesión SSO caduca, se le solicitará de nuevo sus credenciales. **Nota:** SSO no está disponible en el puerto restringido de Grid Manager. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autentiquen con inicio de sesión único.

Información relacionada

- Controlar el acceso mediante firewalls
- Configurar el inicio de sesión único
- Gestione los grupos de administradores
- Gestión de grupos de alta disponibilidad
- Usar una cuenta de inquilino
- Supervisión y solución de problemas

Cierre la sesión en Grid Manager

Cuando haya terminado de trabajar con Grid Manager, deberá 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. Seleccione **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 activado y también ha iniciado sesión en el Administrador de arrendatarios, también debe cerrar sesión en la cuenta de arrendatario para cerrar sesión en SSO.

Información relacionada

- Configurar el inicio de sesión único
- Usar una cuenta de inquilino

Cambie la contraseña

Si es un usuario local de Grid Manager, puede cambiar su propia contraseña.

Lo que necesitará

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 activado 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**.

Cambie el tiempo de espera de la sesión del explorador

Puede controlar si los usuarios de Grid Manager y de arrendatario Manager han cerrado la sesión si están inactivos durante más de un cierto período de tiempo.

Lo que necesitará

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

Acerca de esta tarea

El valor predeterminado de tiempo de espera de inactividad de la interfaz gráfica de usuario es 900 segundos (15 minutos). Si la sesión del explorador de un usuario no está activa durante este período de tiempo, se agota el tiempo de espera de la sesión.

Según sea necesario, puede aumentar o reducir el tiempo de espera mediante la configuración de la opción de visualización tiempo de espera de inactividad de la interfaz gráfica de usuario.

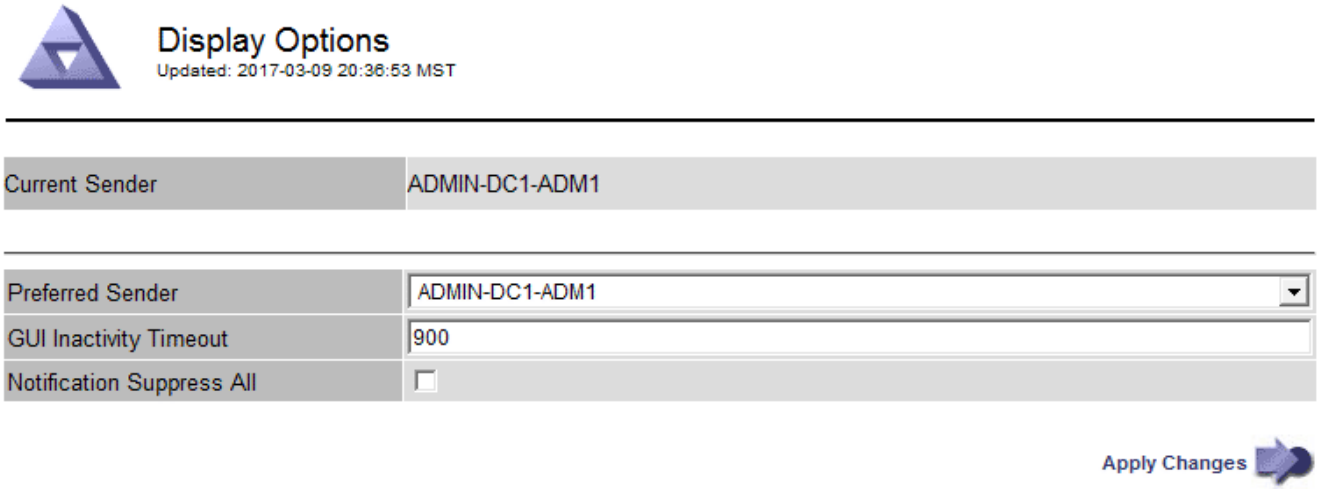
Si se activa el inicio de sesión único (SSO) y se agota el tiempo de espera de la sesión del explorador de un usuario, el sistema se comporta como si el usuario seleccionara **Cerrar sesión** manualmente. El usuario debe volver a introducir sus credenciales de SSO para volver a acceder a StorageGRID. Consulte Configurar el inicio de sesión único.

> El tiempo de espera de la sesión de usuario también puede controlarse por lo siguiente:
>
> - Temporizador StorageGRID independiente no configurable, que se incluye para la seguridad del sistema. De forma predeterminada, 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 cierra automáticamente, incluso si no se ha alcanzado el valor de tiempo de espera de inactividad de la interfaz gráfica de usuario. Para renovar el token, el usuario debe volver a iniciar sesión.
> - Se ha agotado el tiempo de espera de la configuración del proveedor de identidades, suponiendo que SSO esté habilitado para StorageGRID.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de pantalla**.
2. Para **tiempo de espera de inactividad de la GUI**, introduzca un período de tiempo de espera de 60 segundos o más.

   Configure este campo en 0 si no desea utilizar esta funcionalidad. Los usuarios se firman 16 horas después de iniciar sesión, cuando caducan sus tokens de autenticación.



3. Seleccione **aplicar cambios**.

   La nueva configuración no afecta a los usuarios que han iniciado sesión actualmente. Los usuarios deben iniciar sesión de nuevo o actualizar sus exploradores para que la nueva configuración de tiempo de espera tenga efecto.

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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

Acerca de esta tarea

Si se produce un problema con la licencia de software para este sistema StorageGRID, el panel Estado del Panel incluye un icono de estado de licencia y un enlace **Licencia**. El número indica cuántos problemas relacionados con la licencia existen.

Paso

Para ver la licencia, realice una de las siguientes acciones:

- En el panel Estado del panel, seleccione el icono de estado de la licencia o el enlace **Licencia**. Este vínculo sólo aparece si hay un problema con la licencia.

- Seleccione **MANTENIMIENTO** > **sistema** > **Licencia**.

Aparece la página Licencia y proporciona la siguiente información de sólo lectura acerca 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
- Capacidad de almacenamiento bajo licencia del grid
- Fecha de finalización de la licencia del software
- Fecha de finalización del contrato de servicio de soporte
- Contenido del archivo de texto de licencia

> Para las licencias emitidas antes de StorageGRID 10.3, la capacidad de almacenamiento con licencia no está incluida en el archivo de licencia y se muestra un mensaje "Ver acuerdo de licencia" en lugar de un valor.

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.

Lo que necesitará

- Tiene un nuevo archivo de licencia que se aplicará al sistema StorageGRID.
- Tiene permisos de acceso específicos.
- Tiene la clave de acceso de aprovisionamiento.

Pasos

1. Seleccione **MANTENIMIENTO** > **sistema** > **Licencia**.
2. Introduzca la frase de acceso de aprovisionamiento del sistema StorageGRID en el cuadro de texto **frase de paso** de aprovisionamiento.
3. Seleccione **examinar**.
4. En el cuadro de diálogo Abrir, busque y seleccione el nuevo archivo de licencia (`.txt`) Y seleccione **Abrir**.

   El nuevo archivo de licencia se valida y muestra.

5. Seleccione **Guardar**.

Utilice 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.

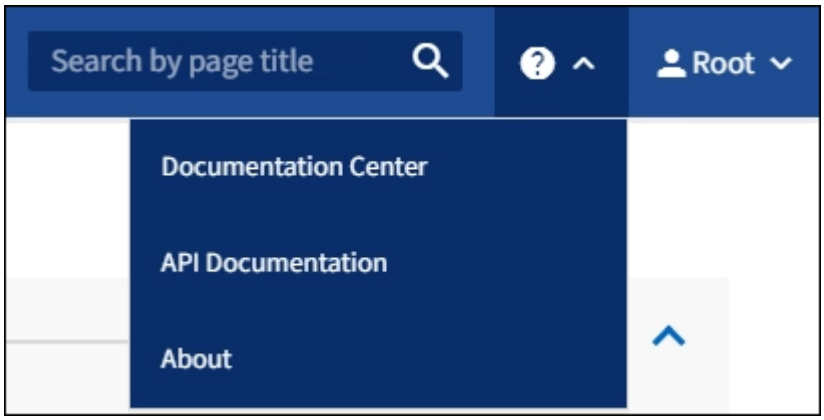
Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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, seleccione el icono de ayuda y seleccione **Documentación de API**.



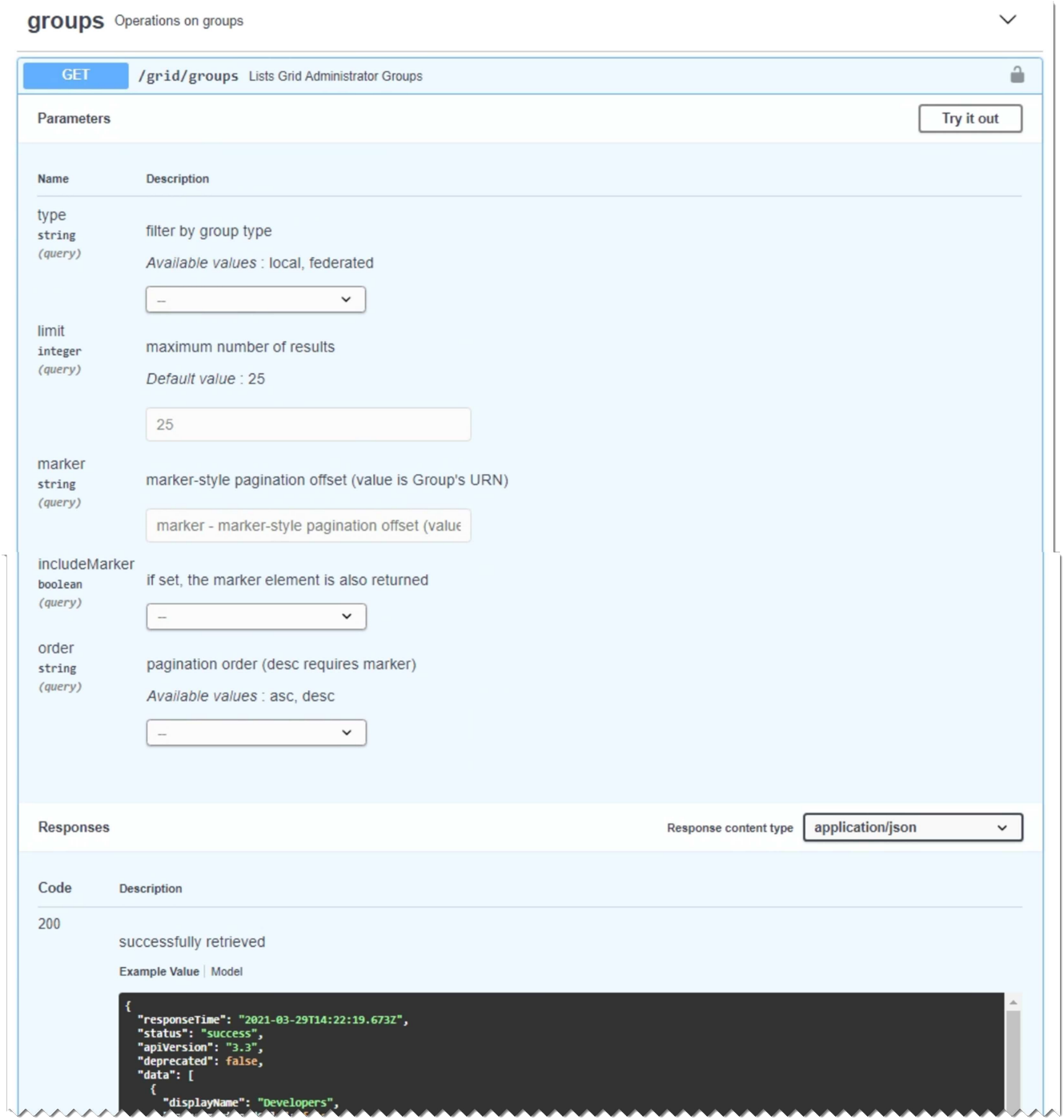
2. Para realizar una operación con la API privada, seleccione **Ir a documentación de API privada** en la página API de administración de StorageGRID.

   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 arrendatarios de almacenamiento, incluyendo la creación de cuentas nuevas y la recuperación del uso del almacenamiento para una cuenta determinada.
- **Alarms** — Operaciones para enumerar las 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 los nodos.
- **Historial de alertas** — Operaciones en alertas resueltas.
- **ALERT-receptores** — Operaciones en receptores de notificación de alertas (correo electrónico).
- **Reglas de alerta** — Operaciones en reglas de alerta.
- **Silencios de alerta** — Operaciones en silencios de alerta.
- **Alertas** — Operaciones en alertas.
- **Audit** — Operaciones para enumerar 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*").

  > 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 está activado el inicio de sesión único"."

  Consulte «"Protección contra la falsificación de solicitudes entre sitios"» para obtener información sobre la mejora de la seguridad de la autenticación.

- **Certificados cliente** — Operaciones para configurar certificados de cliente de modo que se pueda acceder a StorageGRID de forma segura utilizando herramientas de supervisión externas.
- **Config** — Operaciones relacionadas con la versión del producto y las versiones de la API de gestión 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.
- **Características desactivadas** — Operaciones para ver las funciones que podrían haberse desactivado.
- **servidores dns** — Operaciones para enumerar y cambiar los servidores DNS externos configurados.
- **Nombres-dominio-terminal** — Operaciones para enumerar y cambiar los nombres de dominio de punto

final.

- **Codificación de borrado** — Operaciones en perfiles de codificación de borrado.
- **Expansión** — Operaciones de expansión (nivel de procedimiento).
- **Nodos de expansión** — Operaciones en expansión (a nivel de nodo).
- **Expansion-sites** — Operaciones en expansión (a nivel de sitio).
- **Grid-Networks** — Operaciones para enumerar y cambiar la Lista de redes Grid.
- **Grid-password** — Operaciones para la gestión de contraseñas de grid.
- **Grupos** — Operaciones para administrar grupos de administradores de grid locales y recuperar grupos de administradores de grid federados desde un servidor LDAP externo.
- **Identity-source** — Operaciones para configurar un origen de identidad externo y sincronizar manualmente la información del grupo federado y del usuario.
- **ilm** — Operaciones en la gestión del ciclo de vida de la información (ILM).
- **Licencia** — Operaciones para recuperar y actualizar la licencia de StorageGRID.
- **Logs** — Operaciones para recopilar y descargar archivos de registro.
- **Métricas** — Operaciones en métricas StorageGRID incluyendo consultas métricas instantáneas en un único punto en el tiempo y consultas métricas de rango en 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.

- **Detalles del nodo** — Operaciones en los detalles del nodo.
- **Estado del nodo** — Operaciones en el estado del nodo.
- **ntp-Server** — Operaciones para enumerar o actualizar servidores de Protocolo de tiempo de redes (NTP) externos.
- **Objetos** — Operaciones en objetos y metadatos de objetos.
- **Recuperación** — Operaciones para el procedimiento de recuperación.
- **Paquete de recuperación** — 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 certificados de servidor de Grid Manager.
- **snmp** — Operaciones en la configuración actual de SNMP.
- **Traffic-claes** — Operaciones para directivas de clasificación de tráfico.
- **Red-cliente-no confiable** — Operaciones en la configuración de 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 3 de la API.

`https://hostname_or_ip_address/api/v3/authorize`

La versión principal de la API de administración de arrendatarios se bONTAP cuando se realizan cambios que son ***no compatibles*** con versiones anteriores. La versión menor de la API de administración de arrendatarios se bONTAP cuando se hacen cambios que ***are sea compatible*** 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, sólo se activa la versión más reciente de la API de gestión de grid. 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 utilizar la API de gestión de grid para configurar las versiones compatibles. Consulte la sección «'config'» de la documentación de API de Swagger para obtener más información. Debe desactivar la compatibilidad con la versión anterior después de actualizar todos los clientes de la API de Grid Management para que utilicen 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 v1 API at POST "/api/v1/authorize"
```

Determine qué versiones de API son compatibles con la versión actual

Utilice la siguiente solicitud de API para devolver una lista de las versiones principales de API admitidas:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Especifique una versión API para una solicitud

Puede especificar la versión de API mediante un parámetro path (`/api/v3`) o un encabezado (`Api-Version: 3`). Si proporciona ambos valores, el valor de encabezado anula el valor de ruta de acceso.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" 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 harán cumplir el `"Content-Type: application/json"` Encabezado para cualquier solicitud que espera un cuerpo de solicitud JSON como protección adicional contra 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.

Lo que necesitará

- 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 o CentOS, `./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 la sesión de la API de StorageGRID simplemente cerrando la sesión en la página única de cierre de sesión de su empresa. 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 `cookie "sso=true"` En 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 `cookie "sso=true"` No proporciona, el usuario 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

Lo que necesitará

- 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 o CentOS, `./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.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
*******************************************************************************

Watch for and approve a 2FA authorization request
*******************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

> La secuencia de comandos asume que la MFA se realiza utilizando Microsoft Authenticator. Es posible que deba modificar el script para admitir otras formas de MFA (como introducir un código recibido a través de 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

Lo que necesitará

- 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 o CentOS, `./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 la sesión de la API de StorageGRID simplemente cerrando la sesión en la página única de cierre de sesión de su empresa. 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 `cookie "sso=true"` En 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 `cookie "sso=true"` No proporciona, el usuario 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
```

Control del acceso a StorageGRID

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.

Lo que necesitará

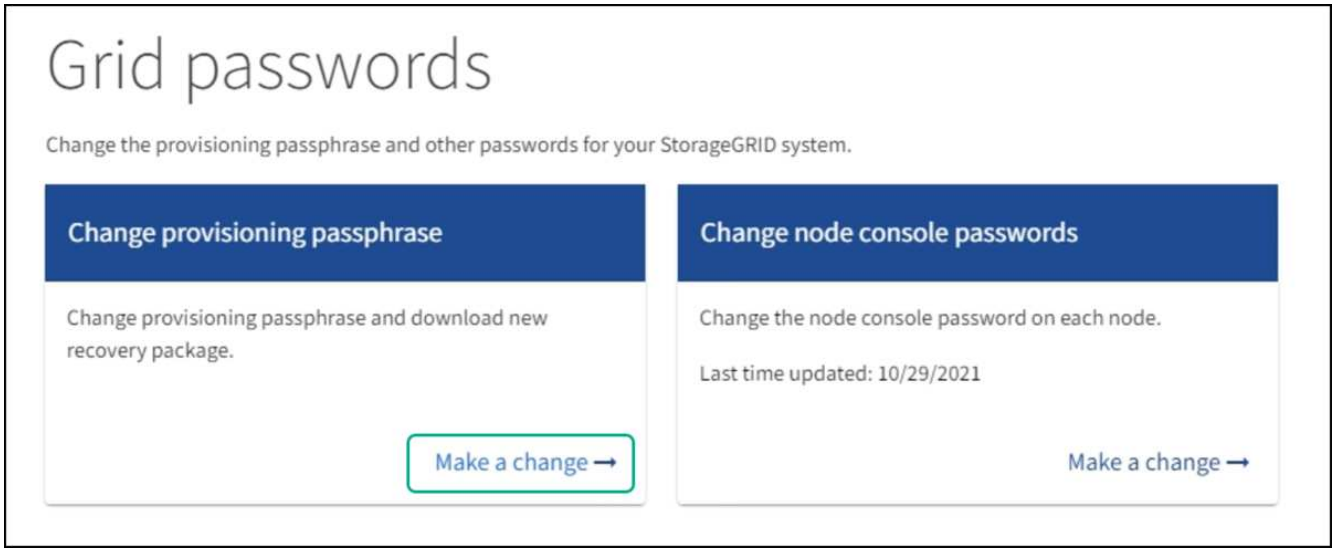
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso raíz o de mantenimiento.
- Tiene la clave de acceso de aprovisionamiento actual.

Acerca de esta tarea

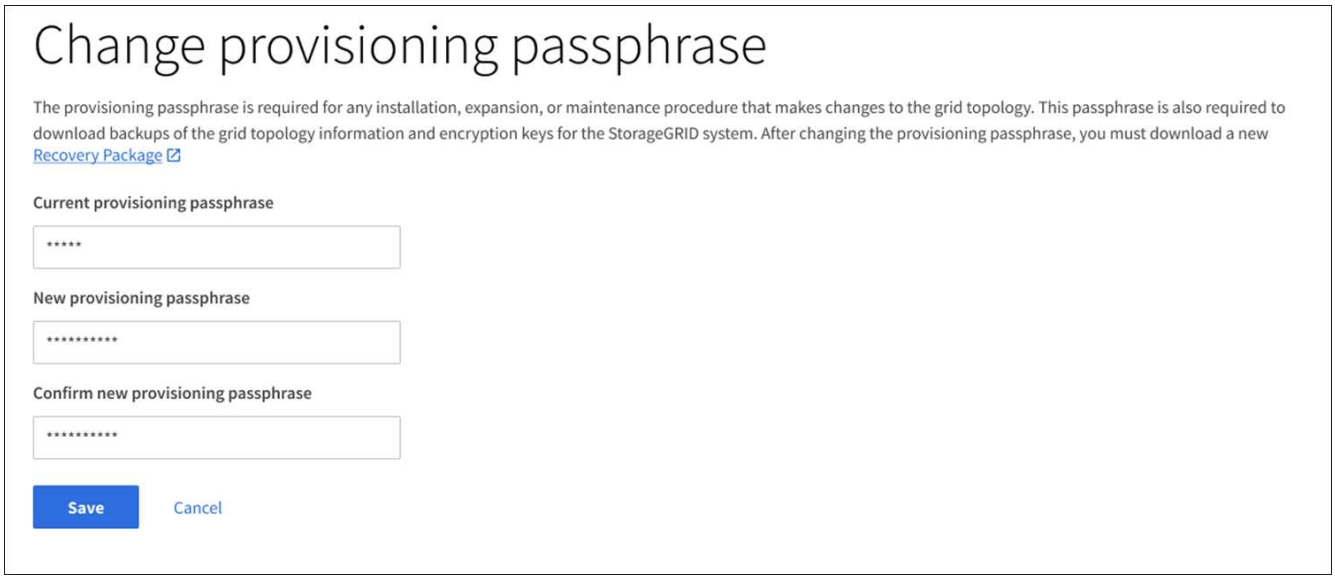
La clave de acceso de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para Descarga del paquete de recuperación. La clave de acceso de aprovisionamiento no aparece en la `Passwords.txt` archivo. Asegúrese de documentar la frase de acceso de aprovisionamiento y mantenerla en una ubicación segura.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso**> **contraseñas de cuadrícula**.

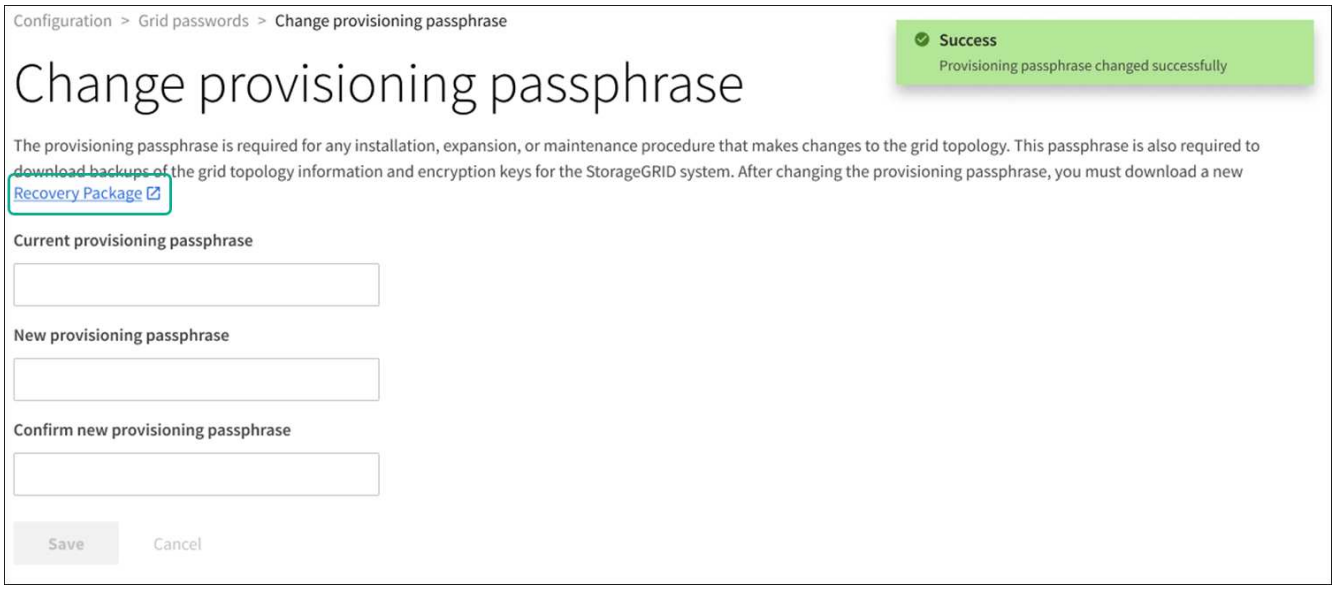


2. Seleccione **hacer un cambio** en **Cambiar contraseña de aprovisionamiento**.



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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tiene el 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 “admin” mediante SSH o en el usuario root en una conexión de la consola física/VM. 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 figuran en la columna Password de la `Passwords.txt` archivo.

> Hay contraseñas de acceso SSH separadas para las claves SSH que se usan para la comunicación entre nodos. Este procedimiento no cambia 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 de nodos, 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 usar 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 de Recovery Package (`.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 usar para obtener datos del sistema StorageGRID.

4. Active la casilla de verificación para indicar que ha descargado el nuevo paquete de recuperación y que ha 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 descargado.
7. Opcionalmente, utilice el enlace **paquete de recuperación** para descargar una copia adicional del nuevo

paquete de recuperación.

Controlar el acceso mediante firewalls

Cuando desee controlar el acceso a través de firewalls, puede abrir o cerrar puertos específicos en el firewall externo.

Controlar el acceso al 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.

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 la API de administración no pueden acceder a Grid Manager ni a la API de gestión 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

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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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 para usar 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.

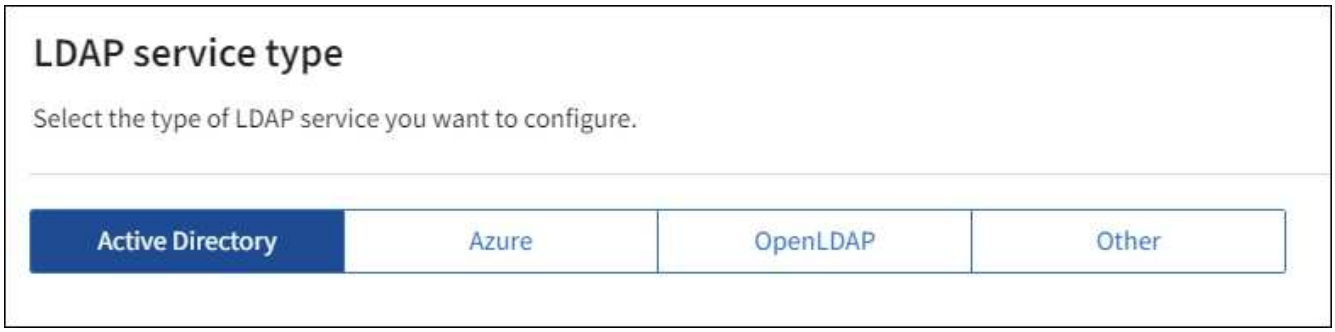
Acerca de esta tarea

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

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.
- **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 Bind** (opcional): El patrón de nombre de usuario predeterminado StorageGRID debe utilizar 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.

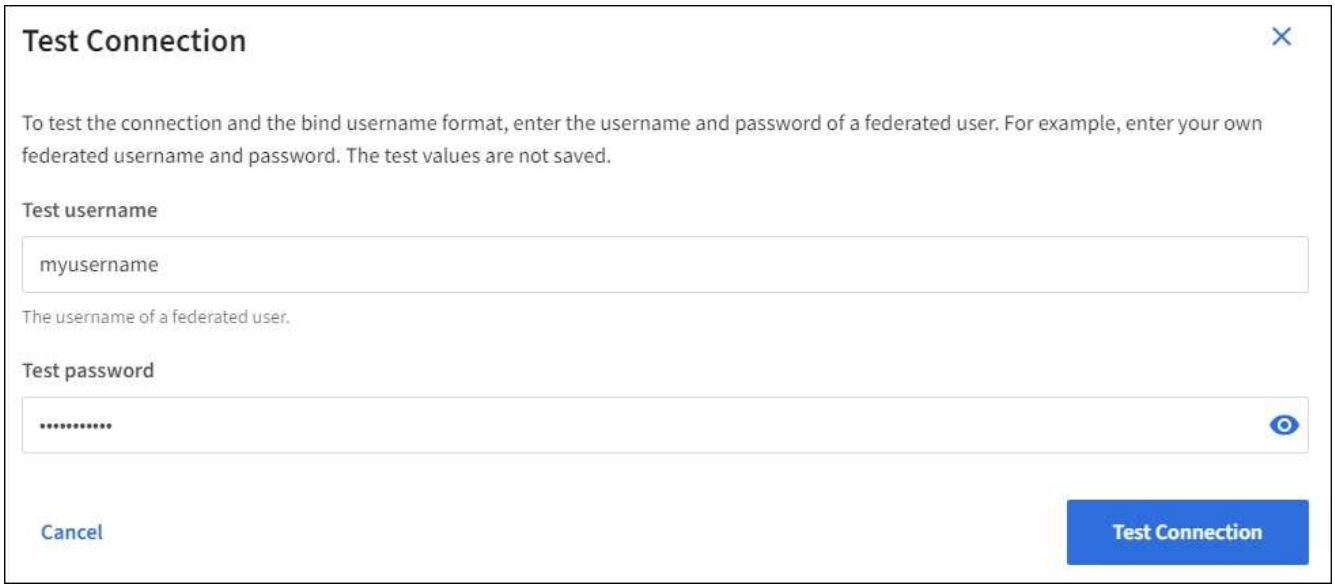
      Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto del certificado de CA.

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.

1. Seleccione **probar conexión**.
2. Si no se proporciona un formato de nombre de usuario de enlace:
    - Aparecerá el mensaje «"probar conexión correcta"» si los ajustes de conexión son válidos. Seleccione **Guardar** para guardar la configuración.
    - Aparece el mensaje «"no se ha podido establecer la conexión de prueba"» si los ajustes de conexión no son válidos. 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 /.



    - Aparecerá el mensaje «"probar conexión correcta"» si los ajustes de conexión son válidos. 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 **Activar federación de identidades** está desactivada si el inicio de sesión único (SSO) está establecido en **activado** o **modo Sandbox**. 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. Desactive la casilla de verificación **Activar federación de identidades**.

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.

> Para los orígenes de identidad que no son 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 del usuario y quite el 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 enhttp://www.openldap.org/doc/admin24/index.html["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 lahttp://www.openldap.org/doc/admin24/index.html["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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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

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

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 se podrá actualizar más adelante.
4. Seleccione **continuar**.

Grupo federado

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

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 en la API de gestión 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.

   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)

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. ConsulteGestionar 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 del grupo. b. Seleccione **acciones** > **Ver detalles del grupo**.	Seleccione el nombre del grupo en la tabla.
Editar nombre para mostrar (sólo grupos locales)	a. Seleccione la casilla de verificación del 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 del grupo. b. Seleccione **acciones** > **Ver detalles del grupo**. c. Si lo desea, cambie el modo de acceso del grupo. d. Opcionalmente, seleccione o anule la selección Permisos de grupo. 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 anule la selección Permisos de grupo. d. Seleccione **Guardar cambios**.

Duplicar un grupo

1. Seleccione la casilla de verificación del 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.

1. En la página grupos, active la casilla de verificación de cada grupo que desee quitar.

2. Seleccione **acciones** > **Eliminar grupo**.
3. Seleccione **Eliminar grupos**.

Permisos de grupo

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
- Consulte 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)
- Vea cierta información en las páginas 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
- **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 permiso de mantenimiento pueden ver, pero no editar, estas páginas:

- **MANTENIMIENTO** > **Red**:
  - Servidores DNS

    - Red Grid
    - Servidores NTP
- **MANTENIMIENTO** > **sistema**:
    - Licencia
- **CONFIGURACIÓN** > **Seguridad**:
    - Certificados
    - Nombres de dominio
- **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 permite acceder a la página **SUPPORT** > **Tools** > **Metrics**. Este permiso también proporciona acceso a consultas de métricas Prometheus personalizadas mediante la sección **Metrics** de la API de gestión de grid.

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** > **Red**:
    - Coste del enlace
- **CONFIGURACIÓN** > **sistema**:
    - Opciones de visualización
    - Opciones de cuadrícula
    - Opciones de almacenamiento
- **SOPORTE** > **Alarmas (heredado)**:
    - Eventos personalizados
    - Alarmas globales
    - Configuración de correo electrónico heredado

Administrador de dispositivos de almacenamiento

Este permiso proporciona acceso al System Manager de SANtricity E-Series en dispositivos de almacenamiento a través de Grid Manager.

Cuentas de inquilino

Este permiso proporciona acceso a la página arrendatarios, donde puede crear, editar y quitar cuentas de arrendatario. Este permiso también permite a los usuarios ver las directivas de clasificación de tráfico existentes.

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 **Cambiar contraseña raíz de arrendatario** ya no aparece en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña raíz de un inquilino fallará con "'403 Prohibido".

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 } }
> ```

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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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 quitar el usuario raíz.

Si está habilitado el inicio de sesión único (SSO), los usuarios locales no podrán iniciar sesión en StorageGRID.

Acceda al asistente

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **usuarios de administración**.
2. Seleccione **Crear usuario**.

Introduzca las credenciales de usuario

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

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. ConsulteGestione 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 mediante la opción **Cambiar contraseña** del banner de Grid Manager.

Tarea	Menú Actions	Detalles
Ver los detalles del usuario	a. Seleccione la casilla de verificación del 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 verificación del 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**.
Denegar o permitir el acceso a StorageGRID	a. Seleccione la casilla de verificación del 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 verificación del 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**.

Tarea	Menú Actions	Detalles
Cambiar grupos (sólo usuarios locales)	a. Seleccione la casilla de verificación del 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.

1. Seleccione la casilla de verificación del 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 raíz.

1. En la página Users (usuarios), seleccione la casilla de verificación de cada usuario que desee quitar.
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.

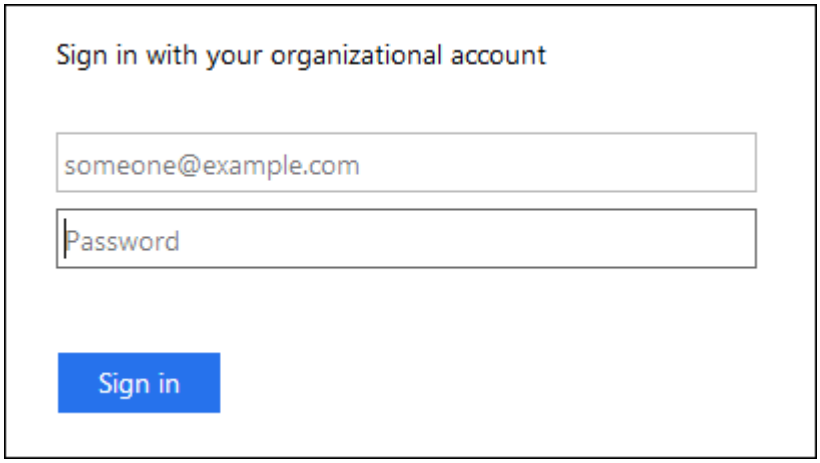
   - Si es la primera vez que accede a la URL en este navegador, se le pedirá un ID de cuenta:

   - 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 sus 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. Busque el enlace **Cerrar sesión** en la esquina superior derecha de la interfaz de usuario.
2. Seleccione **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 para usar el inicio de sesión único

Antes de habilitar el inicio de sesión único (SSO) para un sistema StorageGRID, revise los requisitos en esta sección.

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

Se ha configurado el tipo de servicio LDAP	Opciones para el proveedor de identidades SSO
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.

- AD FS 3.0, incluido con la actualización de Windows Server 2012 R2 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

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 Controlar el acceso mediante firewalls.

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.

Lo que necesitará

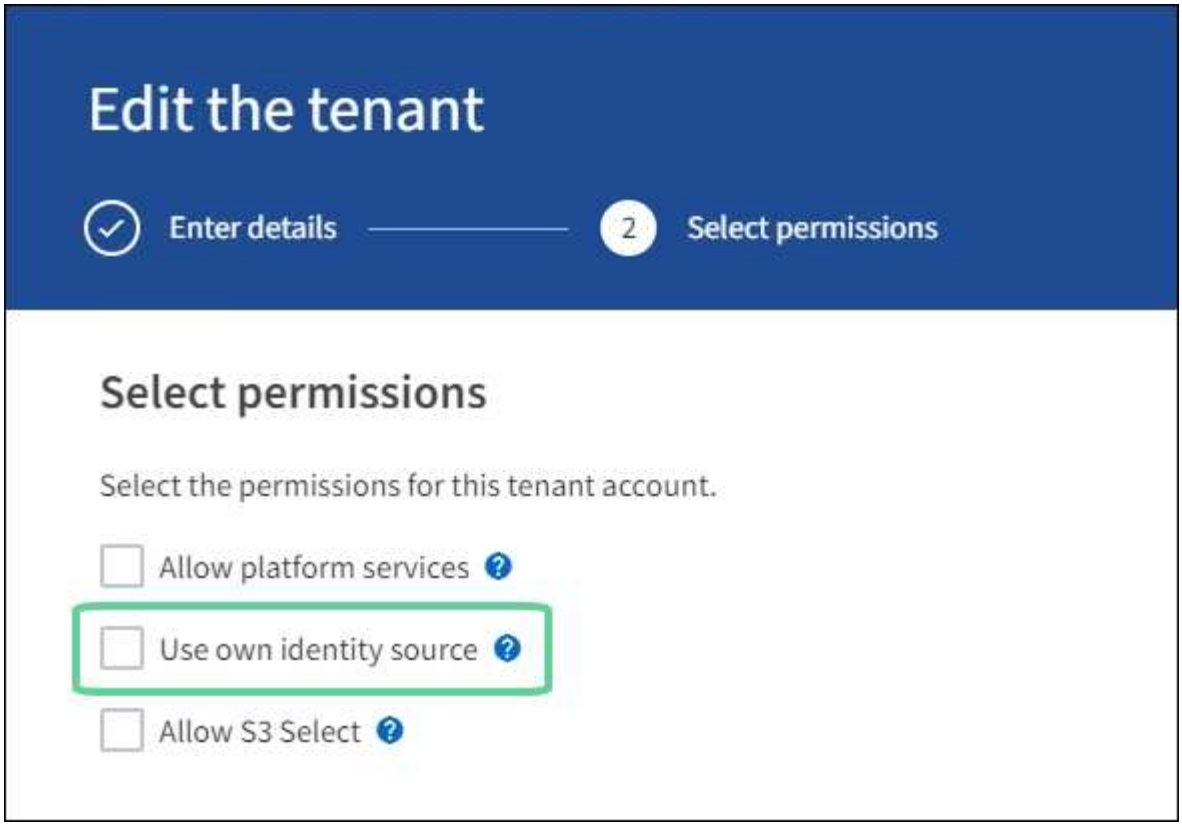
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ya ha configurado la federación de identidades.

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 **Activar federación de identidades** no está activada.
   d. Si es así, confirme que los grupos federados que podrían estar en uso para esta cuenta de arrendatario ya no son necesarios, anule la selección de 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 origen de identidad propio** está activada, desactive 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 para usar 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso 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).

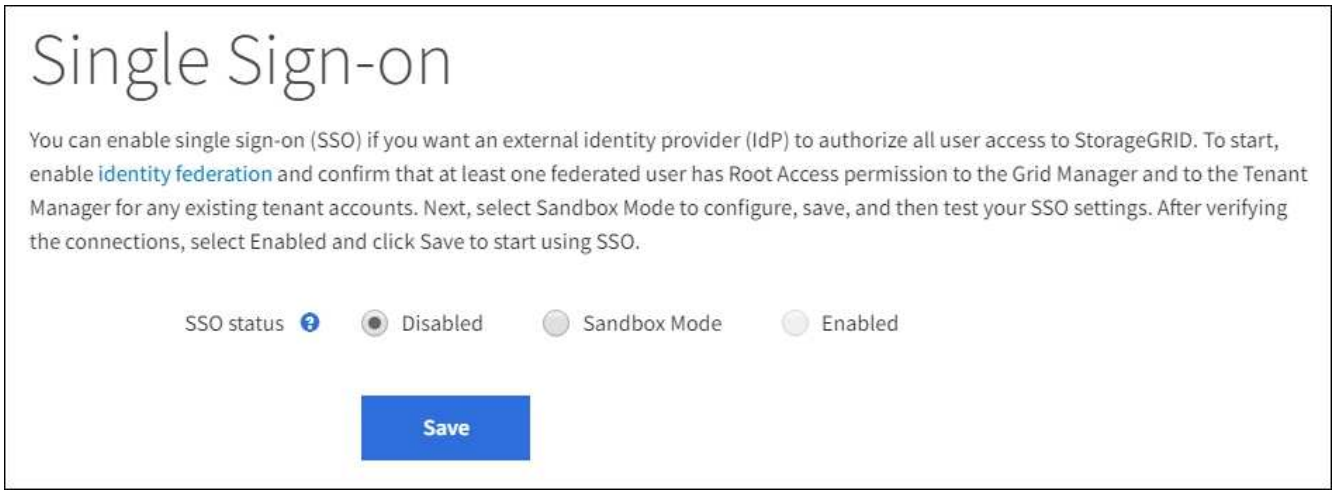
Para permitir que StorageGRID (el proveedor de servicios) y el proveedor de identidades SSO se comuniquen de forma segura acerca de las solicitudes de autenticación de usuarios, debe configurar determinados ajustes en StorageGRID. A continuación, debe utilizar el software del proveedor de identidades 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. Cuando se utiliza el modo Sandbox, los usuarios no pueden iniciar sesión mediante SSO.

Acceder al modo de recinto de seguridad

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.

   Aparece la página Inicio de sesión único, con la opción **Desactivado** seleccionada.



> Si no aparecen las opciones de estado de SSO, confirme que ha configurado el proveedor de identidades como origen de identidad federado. Consulte Requisitos para usar el inicio de sesión único.

2. Seleccione **modo Sandbox**.

   Aparece la sección Proveedor de identidades.

Introduzca los detalles del proveedor de identidades

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.
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 administrador y no prevé añadir más nodos de administrador 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.

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 administrador y no prevé añadir más nodos de administrador 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.

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 administrador y no prevé añadir más nodos de administrador 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

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

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

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.

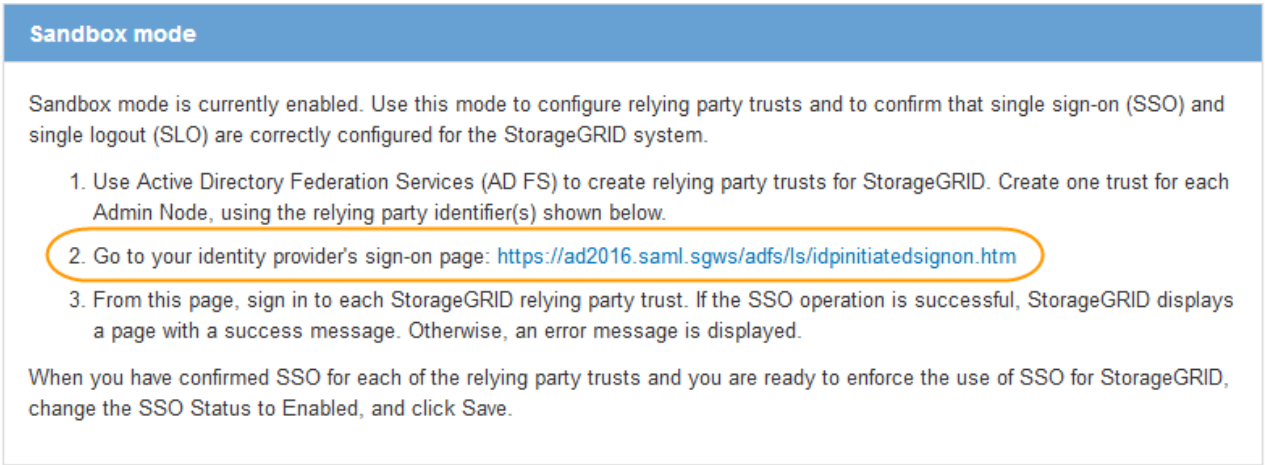
Probar conexiones SSO

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.

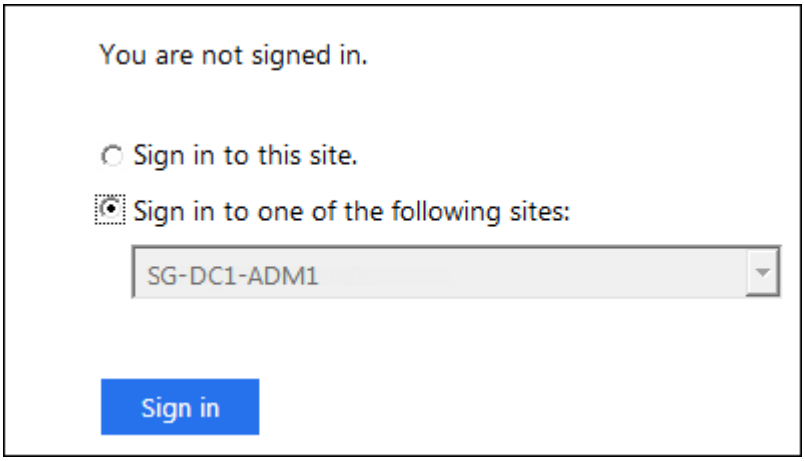
Active Directory

1. En la página Inicio de sesión único de StorageGRID, localice el vínculo en el mensaje modo Sandbox.

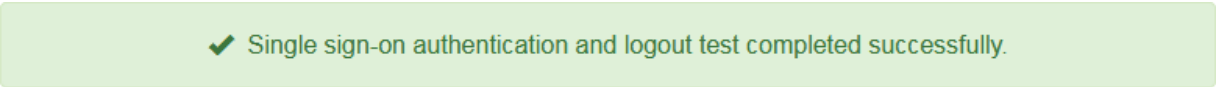
   La dirección URL se deriva del valor introducido en el campo **Nombre de servicio de Federación**.

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

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

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.

   Sandbox mode

   Sandbox mode is currently enabled. Use this mode to configure service provider (SP) connections and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

   1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
   2. Test SSO and SLO by selecting the link for each Admin Node:
      - https:// /idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69
      - https:// /idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73
   3. StorageGRID displays a success or error message for each test.

   When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

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.

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.

Lo que necesitará

- 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**.

f. Para el almacén de atributos, seleccione **Active Directory**.

g. En la columna atributo LDAP de la tabla Mapping, escriba **objectGUID**.

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 metadatos, confirme que la dirección de metadatos de la Federación es correcta o simplemente 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**.

e. Para el almacén de atributos, seleccione **Active Directory**.

f. En la columna atributo LDAP de la tabla Mapping, escriba **objectGUID**.

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 metadatos, confirme que la dirección de metadatos de la Federación es correcta o simplemente 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, active la casilla de verificación **Activar compatibilidad con 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**.

c. Para el almacén de atributos, seleccione **Active Directory**.

d. En la columna atributo LDAP de la tabla Mapping, escriba **objectGUID**.

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 administrador, vaya al `/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.

Lo que necesitará

- 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

1. Inicie sesión en el "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 utilizar 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.

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 el cuadro **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.

Repita estos pasos para cada nodo de administrador:

1. Inicie sesión en StorageGRID desde el nodo de administrador.
2. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Single Sign-On**.
3. Seleccione el botón para descargar los metadatos de SAML de ese nodo de administración.
4. 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:

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.

Lo que necesitará

- 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 lahttps://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html["Guía de referencia del administrador"^] Para PingFederate Server. La documentación de PingFederate proporciona instrucciones detalladas paso a paso y explicaciones.
- Tiene el permiso Admin 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.

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.

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

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

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 de la ficha 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

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

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 el atributo **objectGUID** y añádalo.
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 ficha cumplimiento de contrato de atributo, seleccione **LDAP (atributo)** en la lista desplegable origen y seleccione **objectGUID** 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

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 ficha vinculaciones SAML permitidas, anule la selección de **ARTEFACTO** y **SOAP**. Sólo se requieren **POST** y **REDIRECT**.
5. En la ficha Directiva de firma, deje las casillas de verificación **requerir firma de solicitudes** y **siempre firmar confirmación** activadas.
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

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.

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.

Lo que necesitará

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

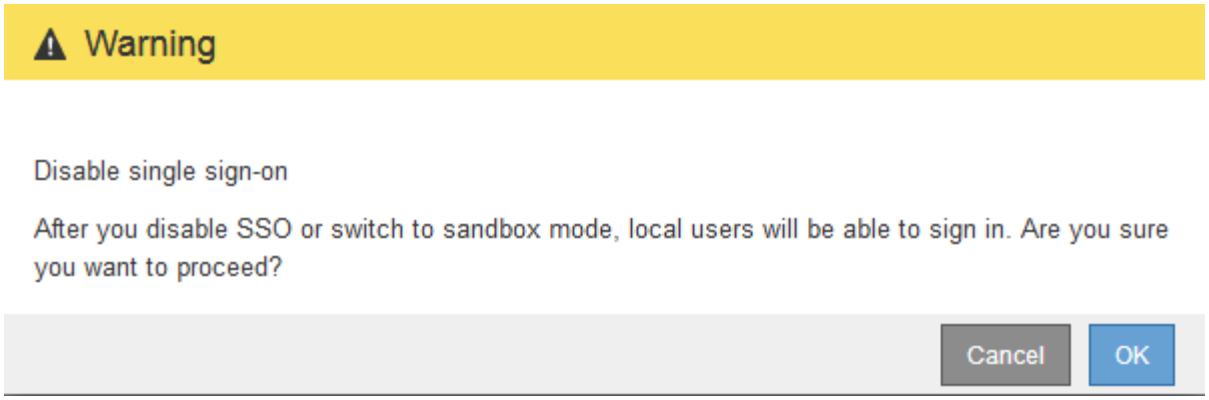
Pasos

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.

Lo que necesitará

- Tiene 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 **Activar SSO** de la página de inicio de sesión único de Grid Manager permanece seleccionada y se mantienen todas las configuraciones de SSO existentes a menos que se actualicen.

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.

Administrar la configuración de seguridad

Gestionar certificados

Acerca de los certificados de seguridad

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. Las conexiones no seguras que no tienen ningún certificado también se admiten, pero no se recomienda.

- Los certificados de CA personalizados no quitan 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 optimización del sistema para certificados de servidor.
- StorageGRID admite la agrupación de certificados de una CA en un único archivo (conocido como paquete de certificados de CA).

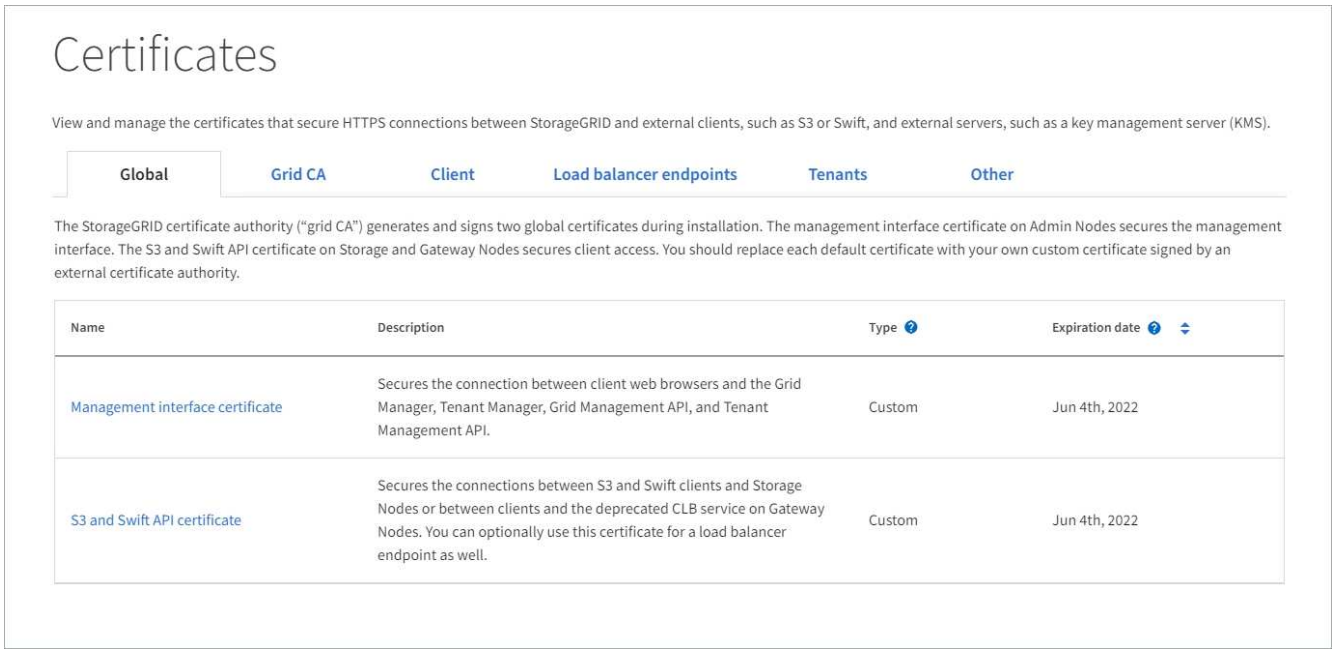
> StorageGRID también incluye certificados de CA del sistema operativo que son los mismos en todos los entornos Grid. En los entornos de producción, asegúrese de especificar un certificado personalizado firmado por una entidad de certificación externa en lugar del certificado de CA del sistema operativo.

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.

1. En Grid Manager, seleccione **CONFIGURATON** > **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. Sólo puede acceder a una ficha si tiene el permiso adecuado.

   - **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. + debe usar siempre un certificado personalizado para mejorar la seguridad de la cuadrícula.
- **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 conexiones de nodo de almacenamiento, servicio CLB (obsoleto) y extremo de equilibrador de carga (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 puede cambiarlo.

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, Que cargue o genere, proteja las conexiones entre los clientes S3 y Swift y el servicio StorageGRID Load Balancer en los nodos de puerta de enlace 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:

- Seleccione un nombre de extremo para abrir una ficha de explorador con información sobre el extremo de equilibrio de carga, incluidos los detalles de su 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 federación de identidades
- Certificados de Cloud Storage Pool
- Certificados de servidor de gestión de claves (KMS)
- Certificados de inicio de sesión único
- Certificados de notificación de alertas por correo electrónico
- Certificados de servidor de syslog externos

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 dispone del permiso correspondiente.

Podrá:

- Ver y editar un certificado de federación de identidades
- Cargar certificados de servidor de gestión de claves (KMS) y de cliente
- Especifique un certificado de Cloud Storage Pool para S3, C2S S3 o Azure
- Especifique manualmente un certificado SSO para la confianza de la parte que confía
- Especifique un certificado para notificaciones de alertas por correo electrónico
- Especifique un certificado de servidor de syslog externo

Detalles del certificado de seguridad

A continuación se describe cada tipo de certificado de seguridad, con vínculos a artículos que contienen 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 con un nodo de almacenamiento, en el servicio Connection Load Balancer (CLB) obsoleto en un nodo de puerta de enlace y extremos de equilibrador 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 conexiones de equilibrador de carga, no es necesario cargar ni generar un certificado independiente para cada extremo de 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 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 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 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 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 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

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** > **Supervisión** > **servidor de auditoría y syslog** y, a continuación, seleccione **Configurar servidor de syslog externo**	Configure un servidor de syslog externo

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).

Para obtener más información sobre cómo protege StorageGRID las conexiones de cliente para la API DE REST, consulte Use S3 o. Use 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 asegurarse de que las operaciones no se ven interrumpidas por un certificado de servidor con errores, la alerta **caducidad del certificado de servidor para la interfaz de administración** se activa cuando este certificado de servidor está a punto de caducar. 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 personalizada se utiliza para todas las nuevas conexiones posteriores a la API de Grid Manager, de arrendatario Manager, de Grid Manager o de arrendatario 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:

   - **Nombre de dominio**: Uno o más nombres de dominio completamente cualificados que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
   - **IP**: Una o varias direcciones IP que se incluirán en el certificado.
   - **Asunto**: X.509 asunto o nombre distinguido (DN) del propietario del certificado.

- **Días válidos**: Número de días después de la creación que expira el certificado.

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 personalizada se utiliza para todas las nuevas conexiones posteriores a la API de Grid Manager, de arrendatario Manager, de Grid Manager o de arrendatario 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 de 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.

Lo que necesitará

- Tiene 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 usa para conexiones de clientes S3 o Swift a nodos de almacenamiento, el servicio Connection Load Balancer

(CLB) obsoleto en los nodos de puerta de enlace o para cargar extremos de equilibrador. 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 asegurarse de que las operaciones no se ven interrumpidas por un certificado de servidor con errores, la alerta **caducidad del certificado de servidor global para API de S3 y Swift** se activa cuando el certificado de servidor raíz está a punto de caducar. 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:

   - **Nombre de dominio**: Uno o más nombres de dominio completamente cualificados que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
   - **IP**: Una o varias direcciones IP que se incluirán en el certificado.
   - **Asunto**: X.509 asunto o nombre distinguido (DN) del propietario del certificado.
   - **Días válidos**: Número de días después de la creación que expira el certificado.

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

Es posible revertir a usar el certificado API S3 y Swift predeterminado para conexiones de clientes S3 y Swift a nodos de almacenamiento, así como el servicio CLB obsoleto en los nodos de puerta de enlace. Sin embargo, no puede utilizar el certificado API S3 y Swift predeterminado para un extremo de equilibrio 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 API global S3 y Swift, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar desde el sistema. El certificado API S3 y Swift predeterminado se utilizará para las conexiones de clientes S3 y Swift posteriores a los nodos de almacenamiento, así como para el servicio CLB obsoleto en los nodos de puerta de enlace.

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 S3
- Use Swift
- Configure los nombres de dominio de extremo API de 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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

En el caso de clientes S3 que realizan una validación de nombre de host estricta y no admiten la deshabilitación de la validación estricta de nombre de host, como clientes ONTAP que utilizan FabricPool, puede generar o cargar un certificado de servidor al configurar el extremo del equilibrador de carga.

Lo que necesitará

- Tiene 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.

> El servicio de equilibrador de carga de conexión (CLB) independiente en los nodos de puerta de enlace queda obsoleto y no se recomienda su uso con 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 la información acerca de uso general de certificados de seguridad y.. configuración de certificados de servidor personalizados.

> Para asegurarse de que las operaciones no se ven interrumpidas por un certificado de servidor con errores, 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.

Lo que necesitará

- 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

Siga el procedimiento para agregar un certificado de cliente a su escenario:

- 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 que contenga al menos 1 y no más de 32 caracteres.
4. Para acceder a las métricas Prometheus mediante su herramienta de supervisión externa, seleccione **permitir Prometheus**.
5. En la sección **Tipo de certificado**, cargue el certificado de interfaz de administración `.pem` archivo.
   a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
   b. Cargue el archivo de certificado de interfaz de gestión (`.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.

6. 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.

   f. 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.

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 que contenga al menos 1 y no más de 32 caracteres.
5. Para acceder a las métricas Prometheus mediante su herramienta de supervisión externa, seleccione **permitir Prometheus**.

6. En la sección **Tipo de certificado**, cargue el certificado de cliente, la clave privada y el paquete de CA `.pem` archivos:
   a. Seleccione **cargar certificado** y, a continuación, seleccione **continuar**.
   b. Cargue un certificado de cliente, una clave privada y 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.
7. 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.
   f. 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.

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 que contenga al menos 1 y no más de 32 caracteres.
4. Para acceder a las métricas Prometheus mediante su herramienta de supervisión externa, seleccione **permitir Prometheus**.
5. En la sección **Tipo de certificado**, seleccione **generar certificado**.
6. Especifique la información del certificado:
   - **Nombre de dominio**: Uno o más nombres de dominio completos del nodo de administración que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
   - **IP**: Una o más direcciones IP del nodo de administración que se incluirán en el certificado.
   - **Asunto**: X.509 asunto o nombre distinguido (DN) del propietario del certificado.
7. Seleccione **generar**.
8. 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.
9. Seleccione **Crear** para guardar el certificado en Grid Manager.

   El nuevo certificado aparece en la ficha Cliente.
10. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Global**.
11. Seleccione **Certificado de interfaz de administración**.
12. Seleccione **utilizar certificado personalizado**.
13. 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 **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la ficha Cliente.

14. 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 cliente de interfaz de gestión para **CA Cert** y **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.

    f. 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 que contenga al menos 1 y no más de 32 caracteres.
5. Para acceder a las métricas Prometheus mediante su herramienta de supervisión externa, 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:

   - **Nombre de dominio**: Uno o más nombres de dominio completamente cualificados que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
   - **IP**: Una o varias direcciones IP que se incluirán en el certificado.
   - **Asunto**: X.509 asunto o nombre distinguido (DN) del propietario del certificado.
   - **Días válidos**: Número de días después de la creación que expira el certificado.

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.

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.

¿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 los volúmenes del dispositivo se han cifrado, no podrá acceder a ningún dato en el 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.

Consulte los métodos de cifrado de StorageGRID

StorageGRID proporciona una serie de opciones para cifrar 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	Configure un servidor de administración de claves para el sitio StorageGRID (**CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**) y active 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. La gestión de claves de cifrado con un KMS solo es compatible con los nodos de almacenamiento y los dispositivos de servicio.
Drive Security en SANtricity System Manager	Si la función Drive Security está habilitada para un dispositivo de almacenamiento, es posible usar SANtricity System Manager para crear y gestionar la clave de seguridad. Se requiere la clave para acceder a los datos en las unidades seguras.	Dispositivos de almacenamiento con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Todos los datos de las unidades seguras están protegidos frente a la pérdida física o eliminación del centro de datos. No se puede utilizar con algunos dispositivos de almacenamiento ni con ningún dispositivo de servicio. • Dispositivos de almacenamiento SG6000 • Dispositivos de almacenamiento SG5700 • Dispositivos de almacenamiento SG5600
Opción de cuadrícula de cifrado de objetos almacenados	La opción **cifrado de objetos almacenados** se puede activar en Grid Manager (**CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**). Cuando se habilita esta opción, todos los objetos nuevos que no se cifran a nivel de bloque o de objeto se cifran durante el procesamiento.	Datos de objetos S3 y Swift recientemente procesados. Los objetos almacenados existentes no están cifrados. Los metadatos de objetos y otros datos confidenciales no se cifran. • Configurar el cifrado de objetos almacenados

Opción de cifrado	Cómo funciona	Se aplica a.
Cifrado de bloques de S3	Se emite una solicitud DE cifrado PUT Bucket para habilitar el cifrado en el bloque. Los objetos nuevos que no se cifren en el nivel de objeto se cifran durante el procesamiento.	Solo datos de objetos S3 procesados recientemente. Debe especificarse el cifrado para el bloque. Los objetos de bloque existentes no están cifrados. Los metadatos de objetos y otros datos confidenciales no se cifran. • Use S3
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 objetos y otros datos confidenciales no se cifran. StorageGRID gestiona las claves. • Use S3
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 objetos y otros datos confidenciales no se cifran. Las claves se gestionan fuera de StorageGRID. • Use S3
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:

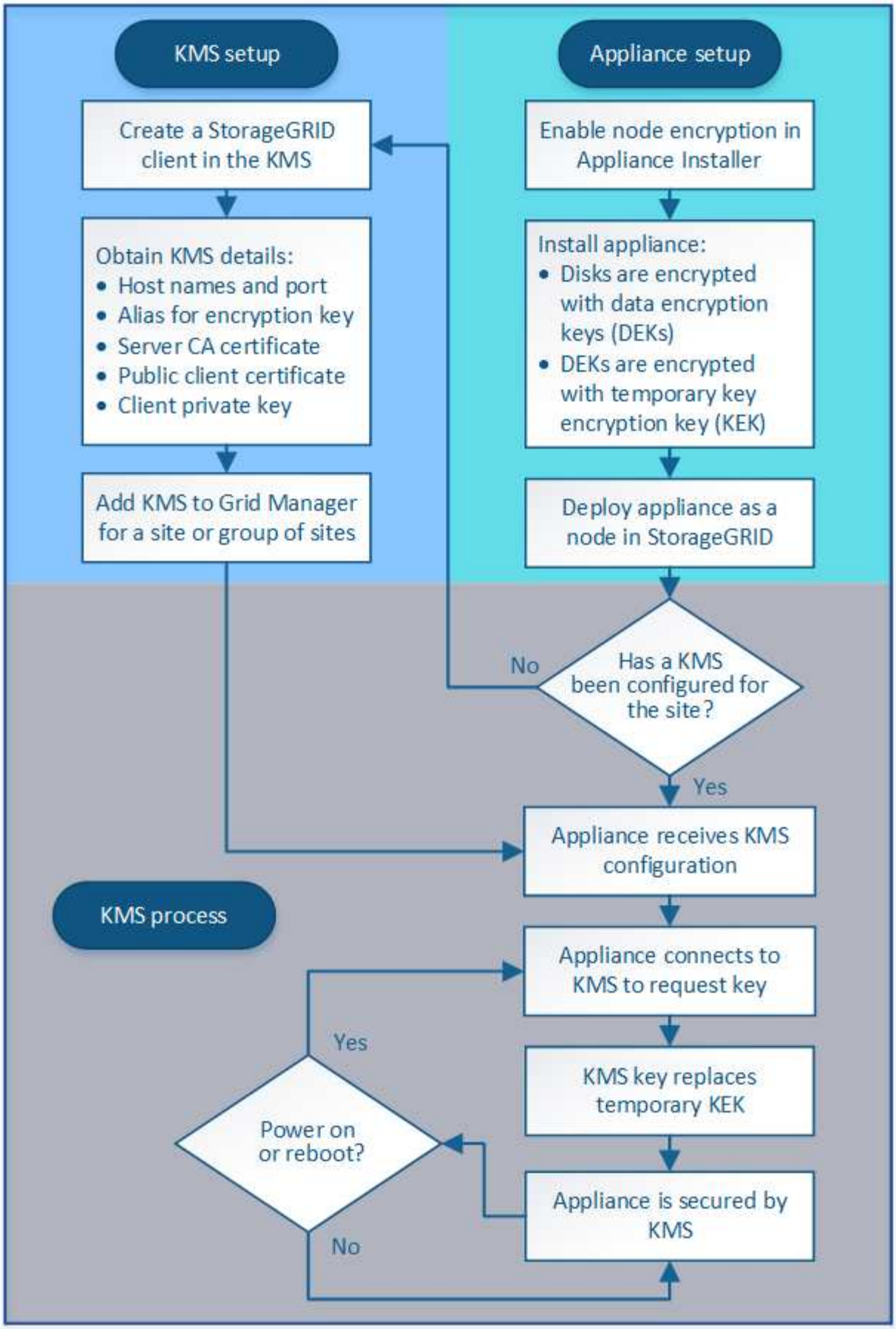
- Puede utilizar un KMS para proteger los nodos de dispositivos y también para usar la función de seguridad de unidades de System Manager de SANtricity a fin de «doble cifrado» de datos de las unidades de autocifrado de los mismos dispositivos.
- Puede usar un KMS para proteger los datos en los nodos del dispositivo y también puede usar la opción de cuadrícula 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.

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
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 activar el ajuste **cifrado de nodos** después de agregar un dispositivo a la cuadrícula y no puede utilizar 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 utilizando el cifrado de disco de Linux Unified Key Setup (LUKS) en el sistema operativo 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.

Si quiere más información, consulte lo siguiente:

- Servicios de aplicaciones SG100 y SG1000
- Dispositivos de almacenamiento SG6000
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG5600

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 tecla, que se guarda en la memoria volátil, no puede sobrevivir a una pérdida de energía o un reinicio.

Consideraciones y requisitos para usar un servidor de gestión de claves

Antes de configurar un servidor de gestión de claves (KMS) externo, debe comprender las consideraciones y los requisitos.

¿Cuáles son los requisitos de KMIP?

StorageGRID admite la versión KMIP 1.4.

"Especificación del protocolo de interoperabilidad de gestión de claves versión 1.4"

Las comunicaciones entre los nodos del dispositivo y el KMS configurado utilizan conexiones TLS seguras. StorageGRID admite los siguientes cifrados TLS v1.2 para KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

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.

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.

¿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 nodos después de que se añade un dispositivo a la cuadrícula y no se puede usar la gestión de claves externa en los dispositivos que no tienen el cifrado de nodos habilitado.

Puede usar el KMS configurado para los siguientes dispositivos StorageGRID y nodos de dispositivos:

Dispositivo	Tipo de nodo
Aplicación de servicios SG1000	El nodo de administrador o el nodo de puerta de enlace
Servicio de atención al cliente SG100	El nodo de administrador o el nodo de puerta de enlace
Dispositivo de almacenamiento SG6000	Nodo de almacenamiento
Dispositivo de almacenamiento SG5700	Nodo de almacenamiento
Dispositivo de almacenamiento SG5600	Nodo de almacenamiento

No puede usar el KMS configurado para nodos basados en software (sin dispositivo), 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?

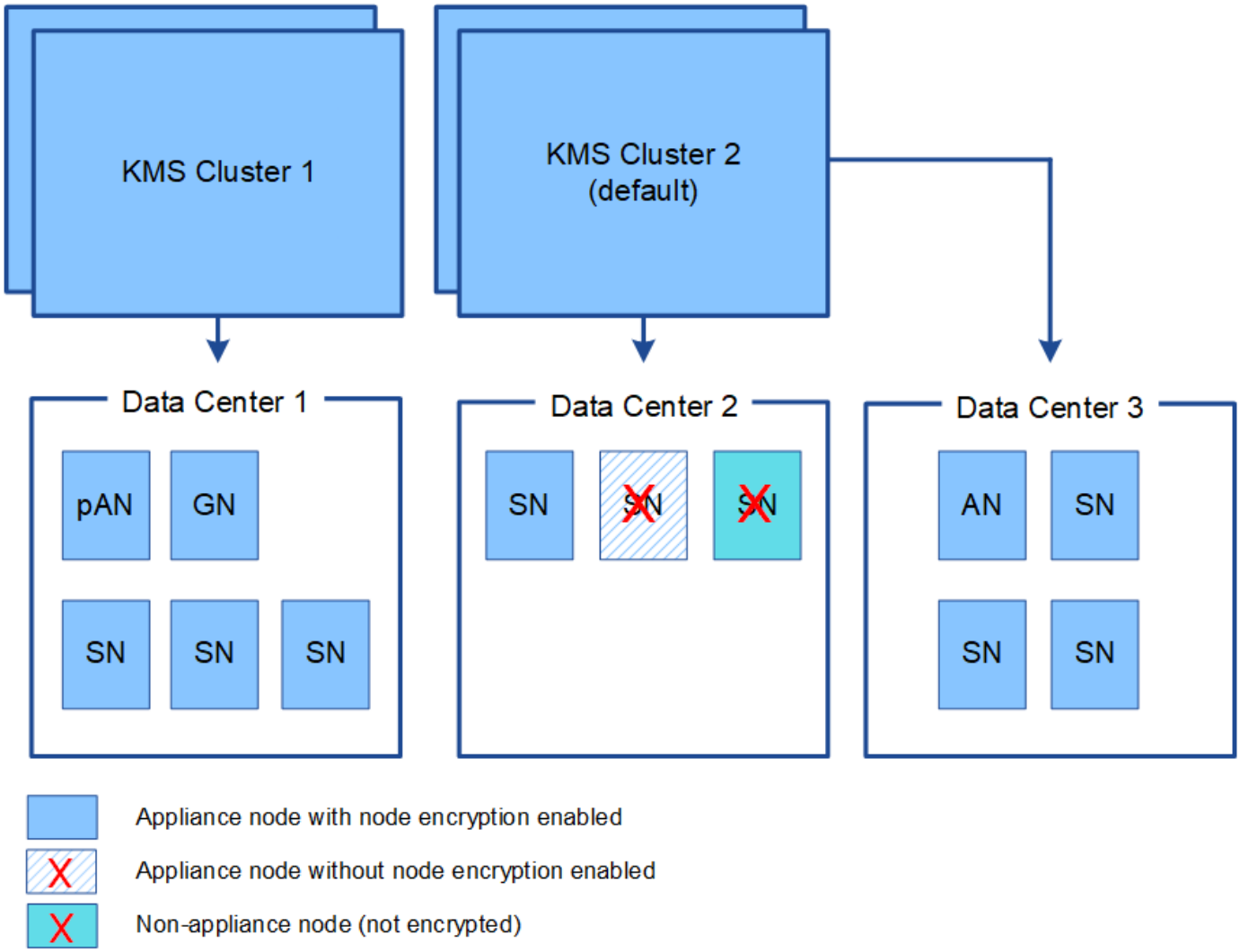
Puede configurar uno o varios servidores de gestión de claves externos para proporcionar claves de cifrado a los nodos de dispositivos en el sistema StorageGRID. Cada KMS proporciona una única clave de cifrado a los nodos de dispositivos StorageGRID en un único sitio o a un grupo de sitios.

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 utilizar KMS para nodos que no son de dispositivo ni para los que no tenían activada la configuración de **cifrado de nodos** durante la instalación.



¿Qué ocurre cuando se gira una clave?

Como práctica recomendada para la seguridad, debe girar periódicamente la clave de cifrado utilizada por cada KMS configurado.

Al girar la clave de cifrado, utilice el software KMS para pasar 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 en el Gestor de cuadrícula. En su lugar, gire la clave actualizando la versión de la clave en el software KMS. Utilice el mismo alias de clave para las claves nuevas que se usaron para las claves anteriores. Si cambia el alias de clave para un KMS configurado, es posible que StorageGRID no pueda descifrar los datos.

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 **error de rotación de clave de cifrado KMS** 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 usar el instalador del dispositivo StorageGRID para borrar 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.

Información relacionada

- Servicios de aplicaciones SG100 y SG1000
- Dispositivos de almacenamiento SG6000
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG5600

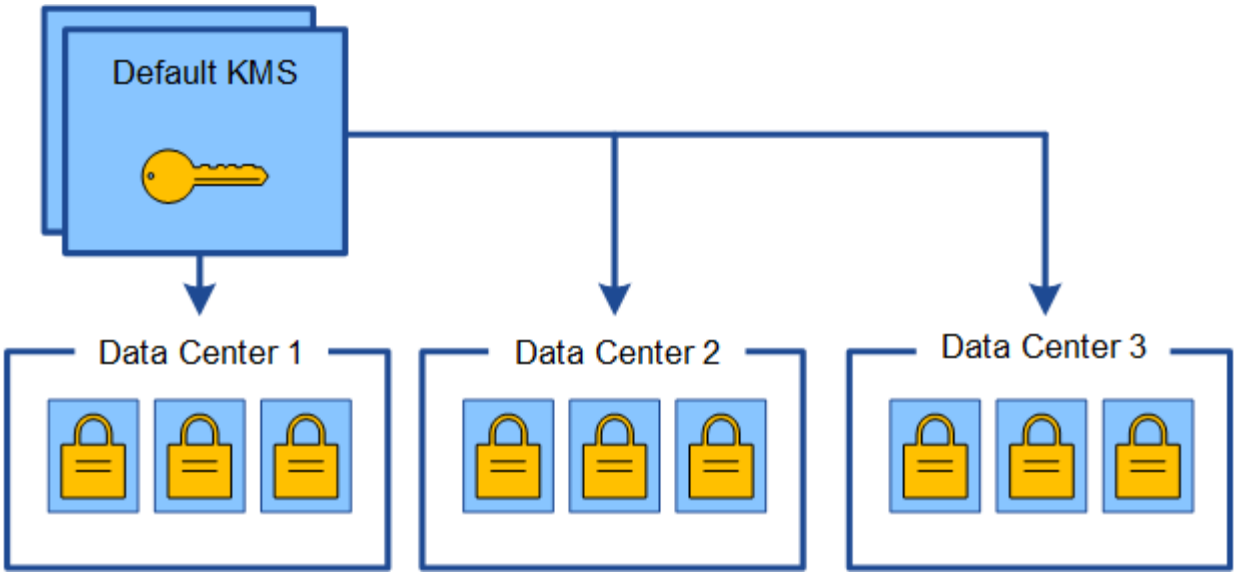
Consideraciones para cambiar el KMS de un sitio

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.

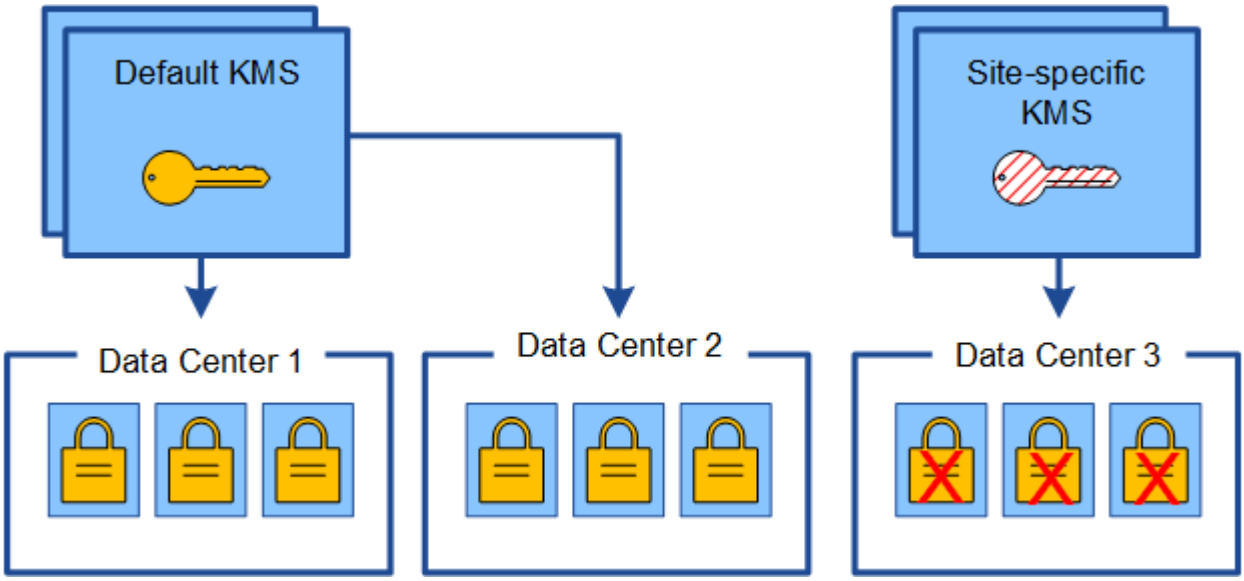
Si cambia el KMS utilizado para un sitio, debe asegurarse de que los nodos del dispositivo cifrados anteriormente en ese sitio se puedan descifrar utilizando la clave almacenada en el nuevo KMS. En algunos casos, es posible que necesite copiar la versión actual de la clave de cifrado del KMS original 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:

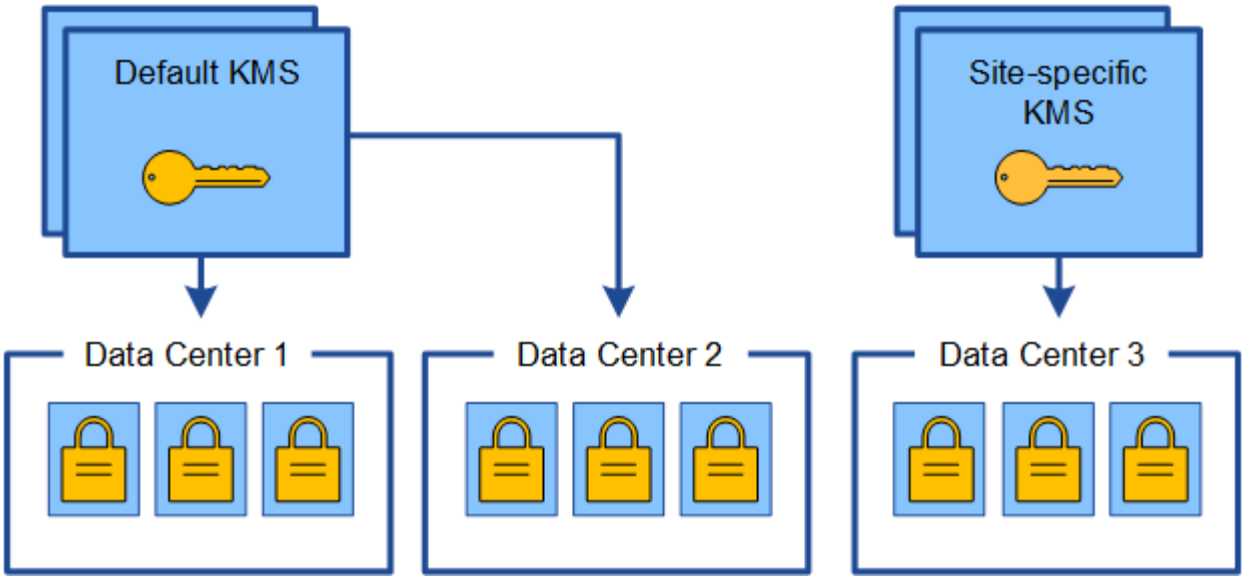
1. Inicialmente, configura un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos de dispositivo que tienen activada la configuración de **cifrado de nodos** se conectan al KMS y solicitan la clave de cifrado. Esta clave se usa 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)

Caso de uso para cambiar el KMS de un sitio	Pasos requeridos
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.

Acerca de esta tarea

Estas instrucciones se aplican a Thales CipherTrust Manager k170v, versiones 2.0, 2.1 y 2.2. Si tiene preguntas sobre el uso de un servidor de gestión de claves diferente con StorageGRID, póngase en contacto con el soporte técnico.

"Thales CipherTrust Manager"

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. Desde el software KMS, cree una clave de cifrado AES para cada clúster KMS o KMS.

   La clave de cifrado debe ser exportable.

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.

   > La clave de cifrado ya debe existir en el KMS. StorageGRID no crea ni gestiona claves 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.

Lo que necesitará

- Ha revisado el consideraciones y requisitos para usar un servidor de gestión de claves.
- Ya tienes Se ha configurado StorageGRID como cliente en el KMSY tiene la información necesaria para cada clúster KMS o KMS.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso 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.

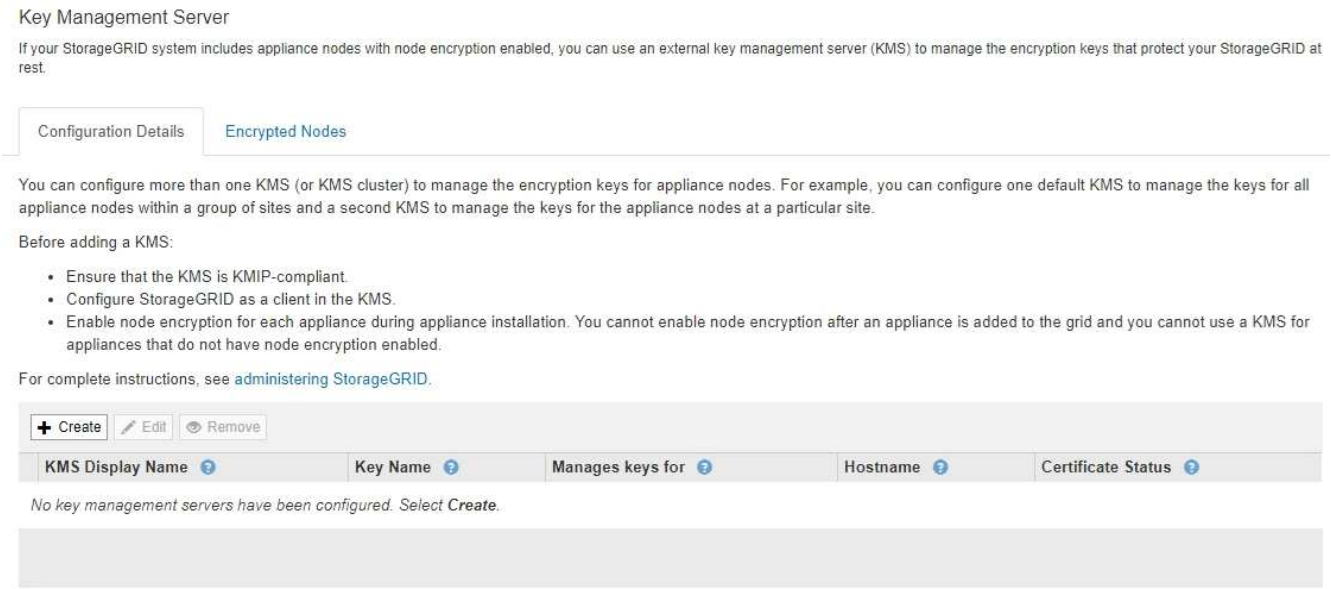
Paso 1: Introduzca los detalles de KMS

En el paso 1 (introducir detalles de KMS) del asistente para agregar un servidor de administración de claves, se proporcionan detalles sobre el clúster KMS o KMS.

Pasos

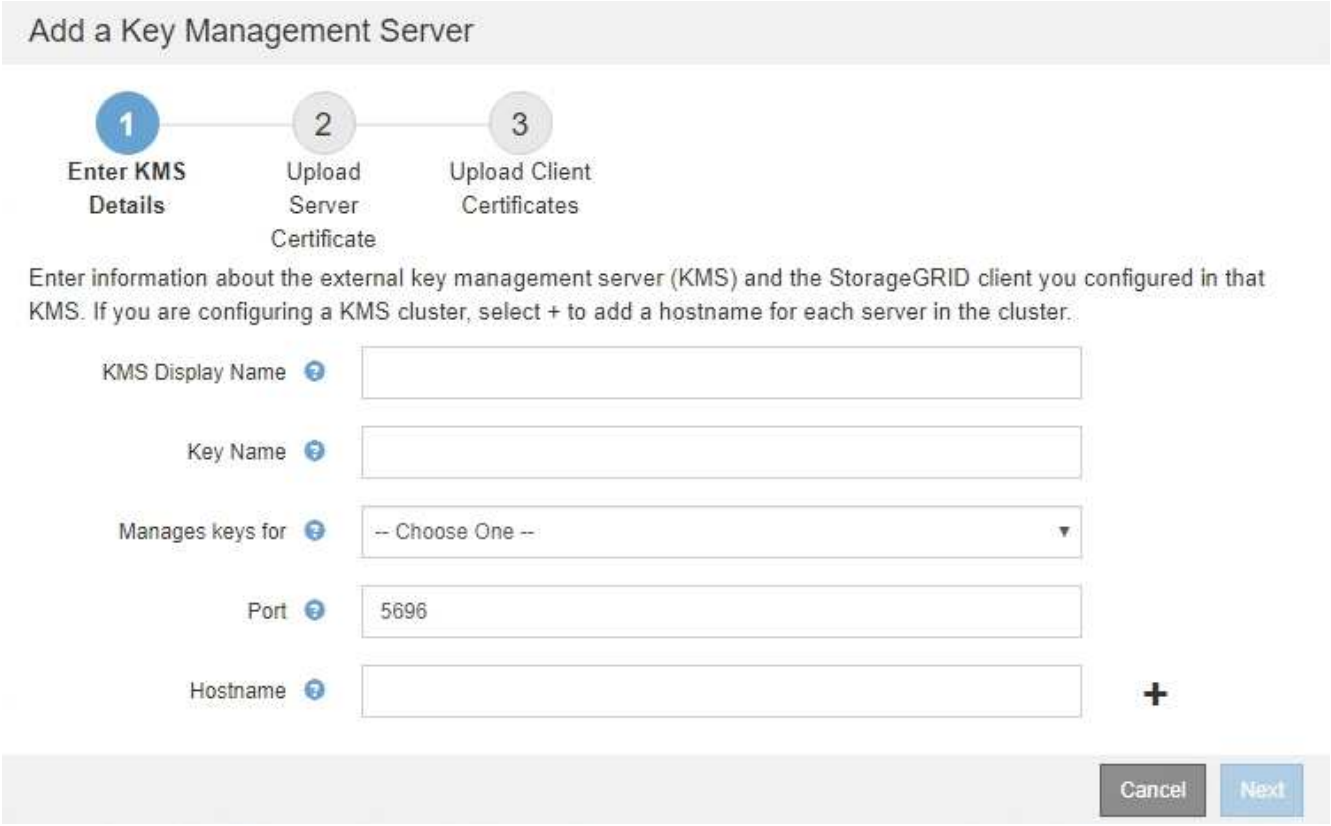
1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Se muestra la página servidor de gestión de claves con la pestaña Detalles de configuración seleccionada.



2. Seleccione **Crear**.

   Paso 1 (introducir detalles de KMS) del asistente Añadir un servidor de gestión de claves aparece.



3. Introduzca la siguiente información para el KMS y el cliente StorageGRID que configuró en ese KMS.

Campo	Descripción
Nombre de visualización DE KMS	Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres.

Campo	Descripción
Nombre de la clave	El alias de clave exacto del cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres.
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 administrados por otro KMS (KMS predeterminado)** 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.
Nombre del hostl	El nombre de dominio completo o la dirección IP del KMS. **Nota:** el campo SAN del certificado de 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 va a utilizar un clúster de KMS, seleccione el signo más ➕ para agregar un nombre de host para cada servidor del clúster.
5. Seleccione **Siguiente**.

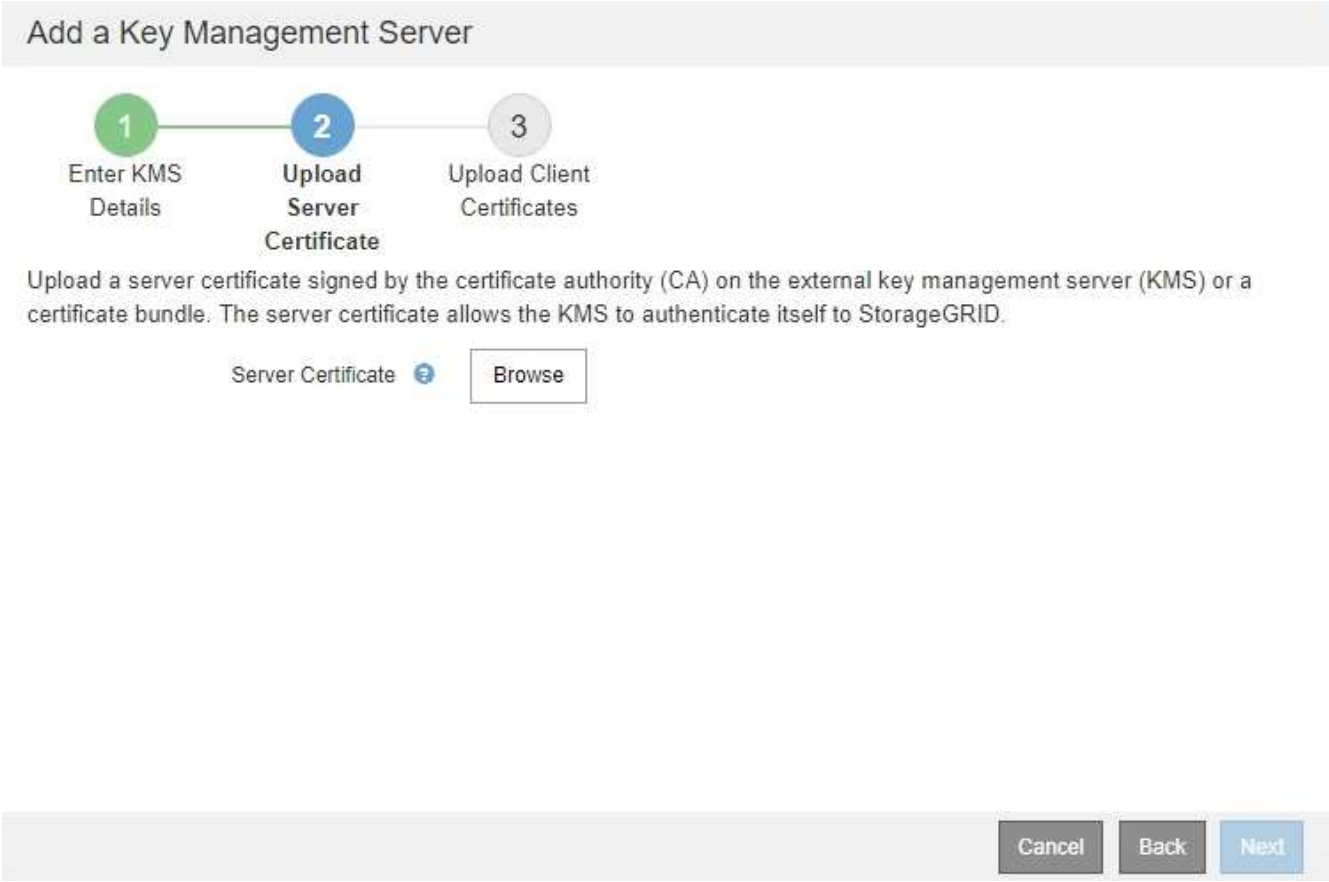
Paso 2: Cargar certificado de servidor

En el paso 2 (cargar certificado de servidor) del asistente Agregar un servidor de gestión de claves, carga el certificado de servidor (o el paquete de certificados) para el KMS. El certificado de servidor permite que el

KMS externo se autentique en StorageGRID.

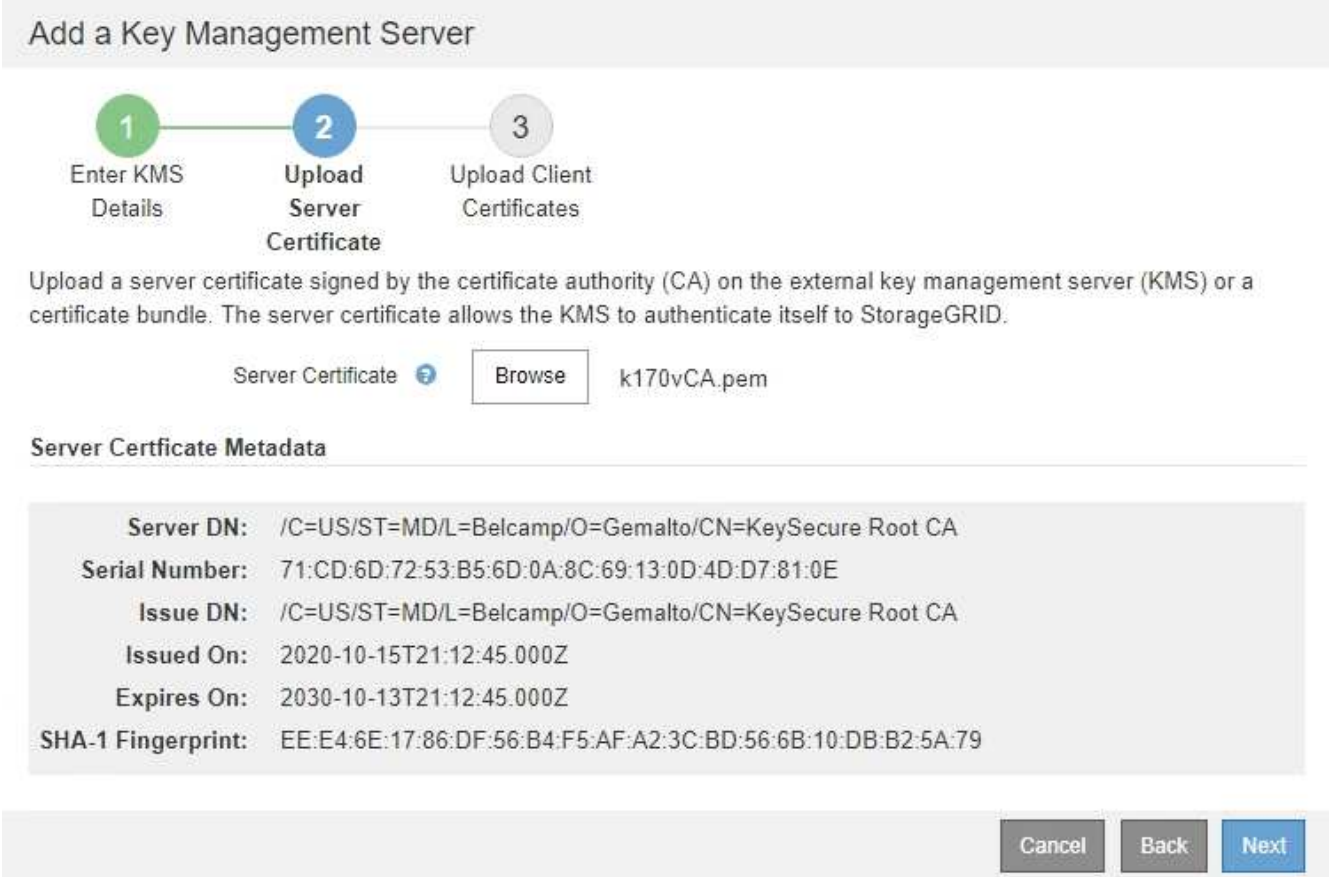
Pasos

1. Desde **Paso 2 (cargar certificado de servidor)**, vaya a la ubicación del certificado de servidor o del paquete de certificados guardados.



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.

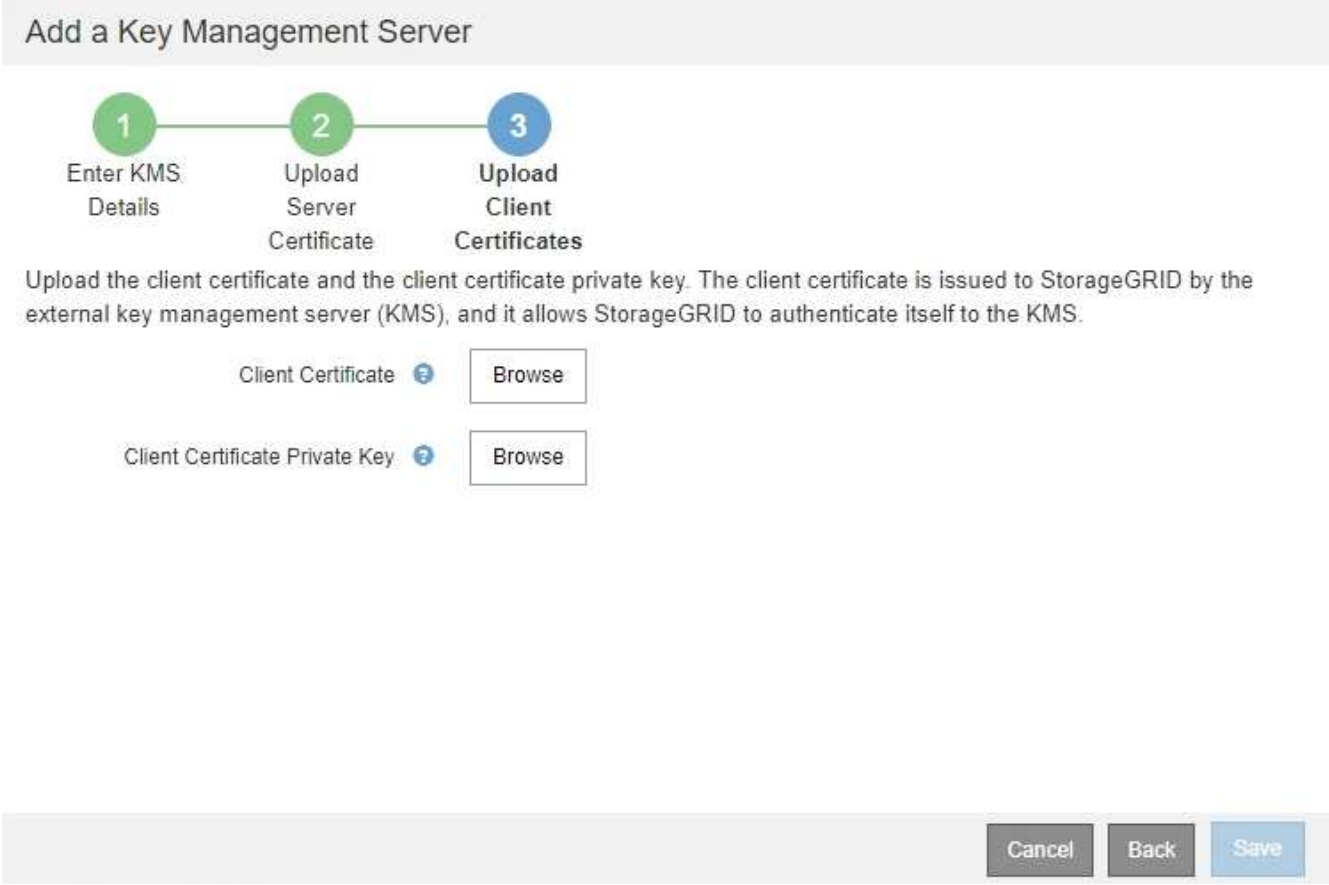
3. Seleccione **Siguiente**.

Paso 3: Cargar certificados de cliente

En el paso 3 (cargar certificados de cliente) del asistente Agregar un servidor de gestión de claves, carga el certificado de cliente y la clave privada del certificado de cliente. El certificado de cliente permite que StorageGRID se autentique en el KMS.

Pasos

1. Desde **Paso 3 (cargar certificados de cliente)**, vaya a la ubicación del certificado de cliente.

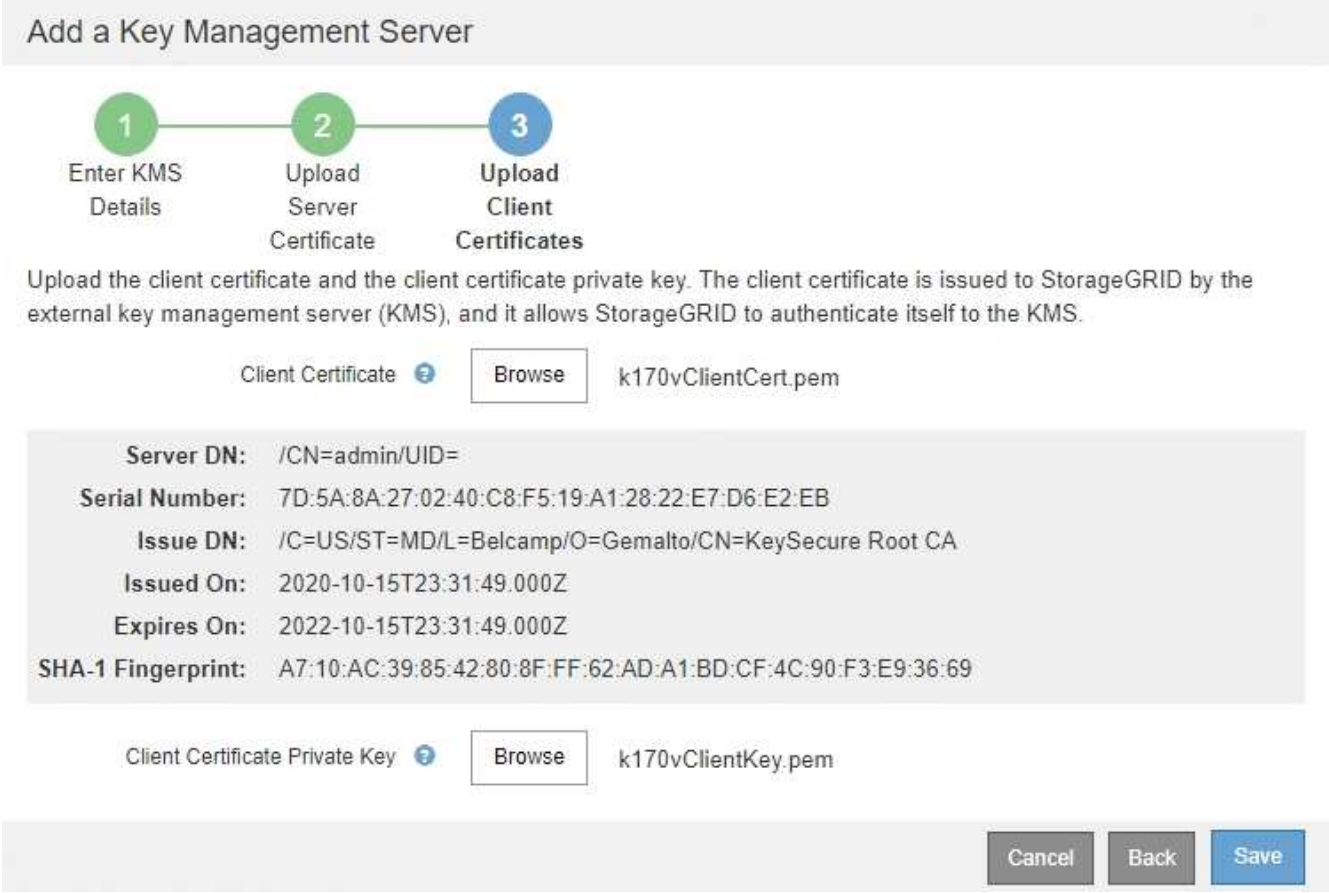


2. Cargue el archivo de certificado de cliente.

   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.

   Aparecen los metadatos del certificado de cliente y la clave privada del certificado de cliente.



5. Seleccione **Guardar**.

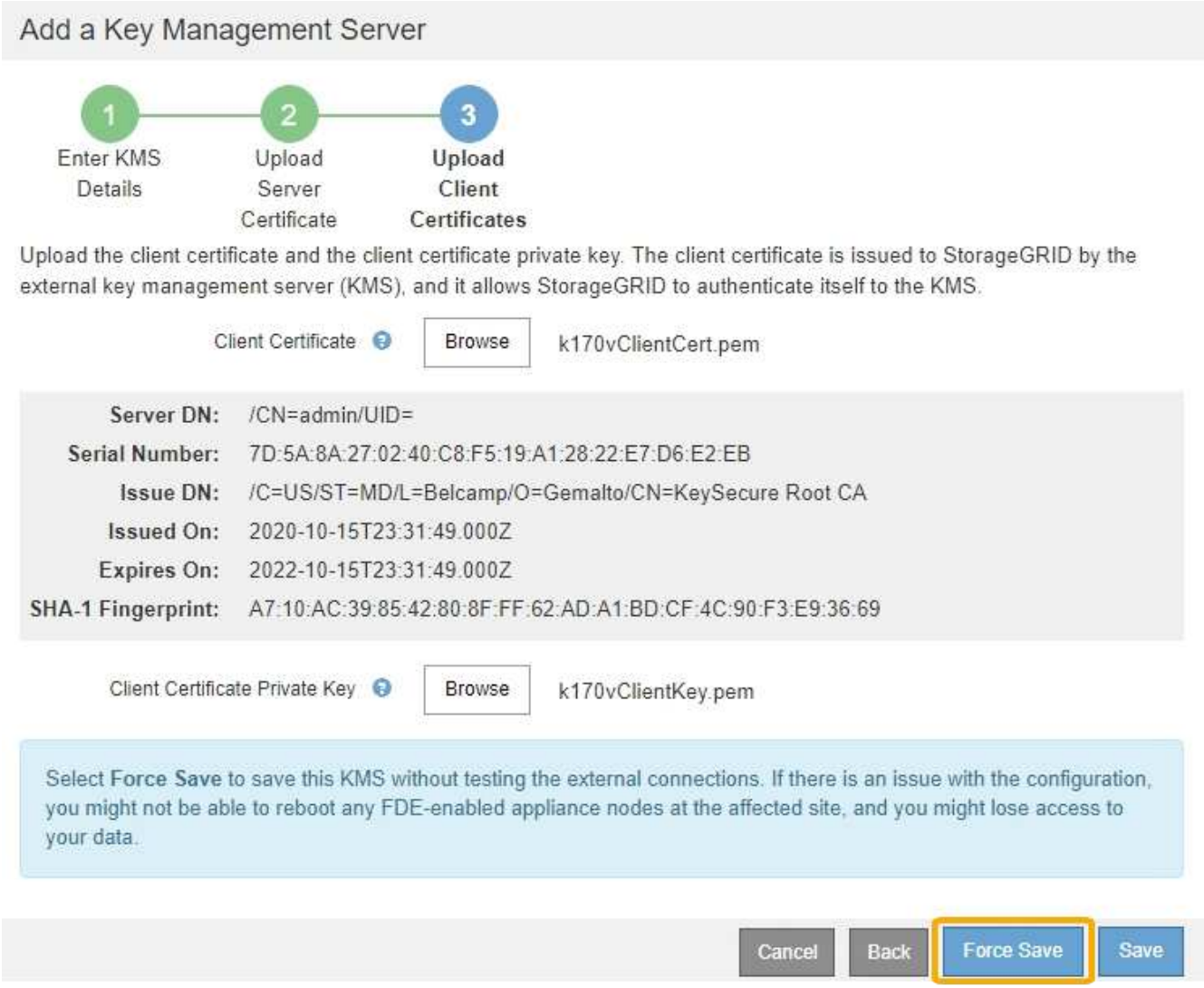
   Se prueban las conexiones entre el servidor de gestión de claves y los nodos del dispositivo. Si todas las conexiones son válidas y se encuentra la clave correcta en el KMS, el servidor de gestión de claves nuevo se añade a la tabla de la página del servidor de gestión de claves.

   > 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 **Guardar**, revise los detalles del mensaje y seleccione **Aceptar**.

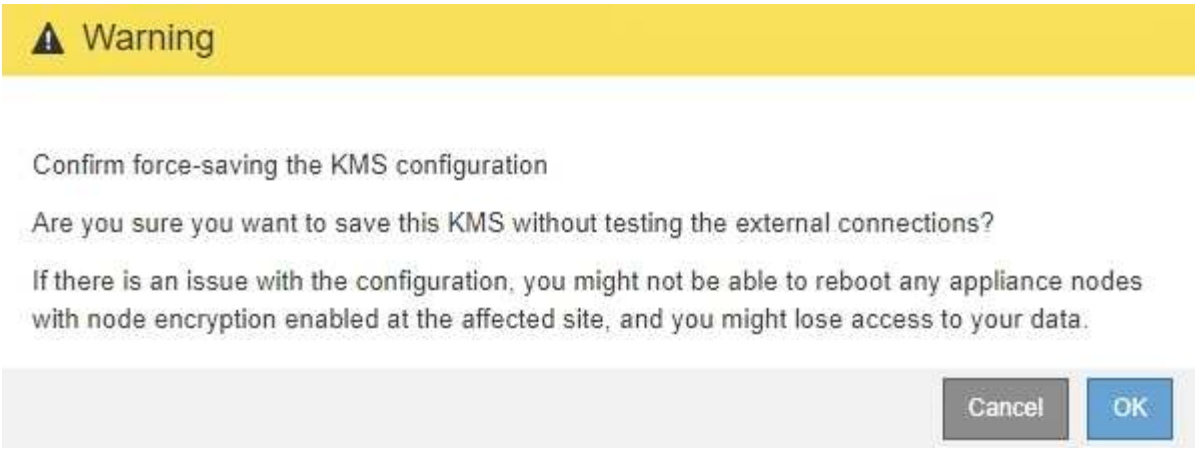
   Por ejemplo, puede recibir un error 422: Entidad no procesable si se produjo un error en una prueba de conexión.

7. Si necesita guardar la configuración actual sin probar la conexión externa, seleccione **Force Save**.



> 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.

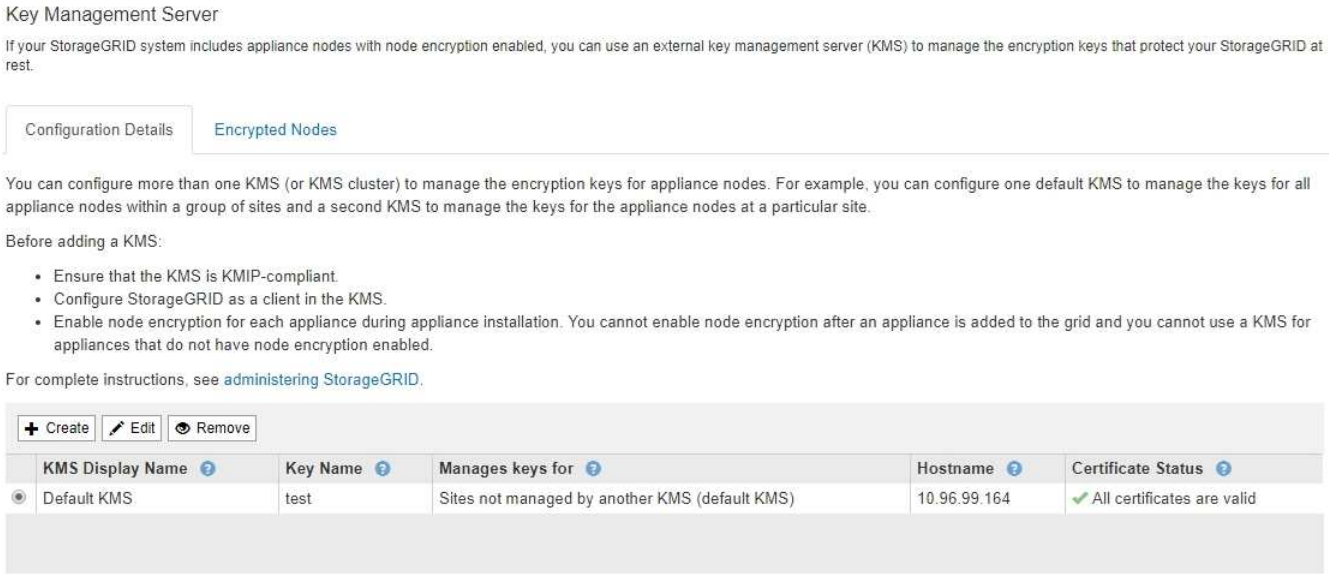
Ver detalles de KMS

Puede ver información sobre cada servidor de gestión de claves (KMS) del sistema StorageGRID, incluidos el estado actual de los certificados de servidor y de cliente.

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 cualquier servidor de gestión de claves configurado.



2. Revise la información de la tabla de cada KMS.

Campo	Descripción
Nombre de visualización DE KMS	Nombre descriptivo del KMS.
Nombre de la clave	El alias clave del cliente StorageGRID en el KMS.

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, a continuación, seleccione **Editar**.
Estado del certificado	Estado actual del certificado de servidor, del certificado de CA opcional y del certificado de cliente: Válido, caducado, casi espirado o desconocido. **Nota:** puede que StorageGRID tarde hasta 30 minutos en obtener actualizaciones del estado del certificado. Debe actualizar el navegador web para ver los valores actuales.

3. Si el estado de certificado es desconocido, espere hasta 30 minutos y, a continuación, actualice el explorador web.

> 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 explorador web para ver el estado real.

4. Si la columna Estado del certificado indica que un certificado ha caducado o está a punto de expirar, envíe el Lo antes posible. del problema.

   Consulte las acciones recomendadas para las alertas **KMS CA de vencimiento**, **KMS de vencimiento** del certificado de cliente* y **KMS de vencimiento** del certificado de servidor* en las instrucciones para Supervisión y solución de problemas de StorageGRID.

Debe solucionar cualquier problema con los certificados Lo antes posible. para mantener el acceso a los datos.

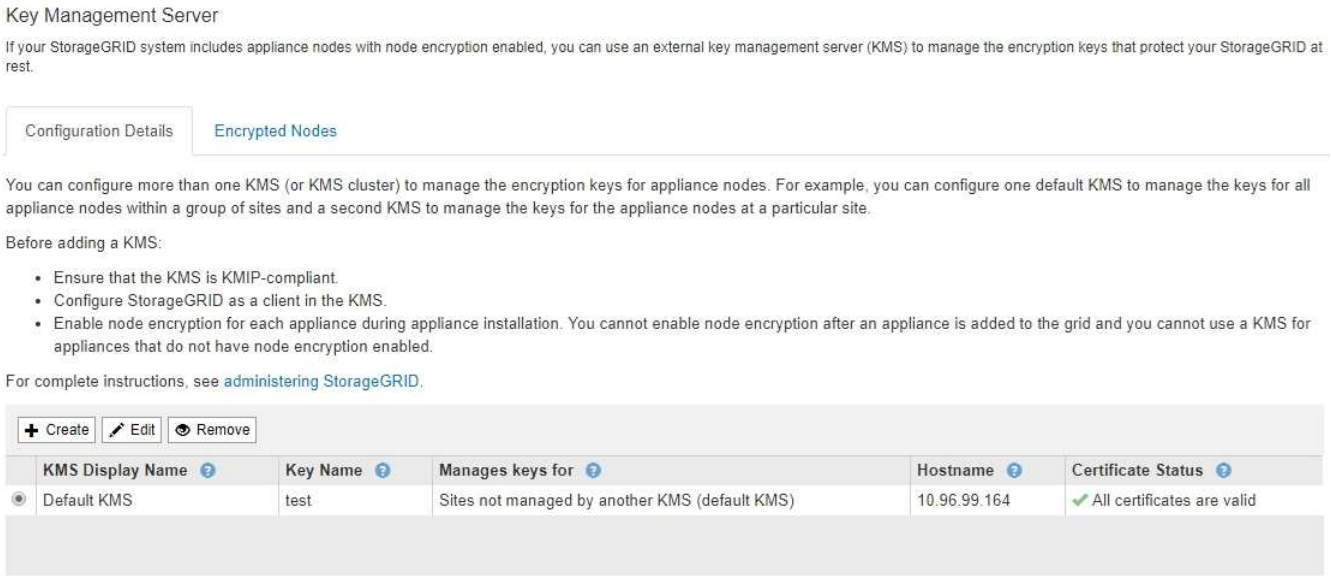
Vea los nodos cifrados

Puede ver información acerca de los nodos del dispositivo en el sistema StorageGRID que tienen activada la configuración * cifrado de nodos*.

Pasos

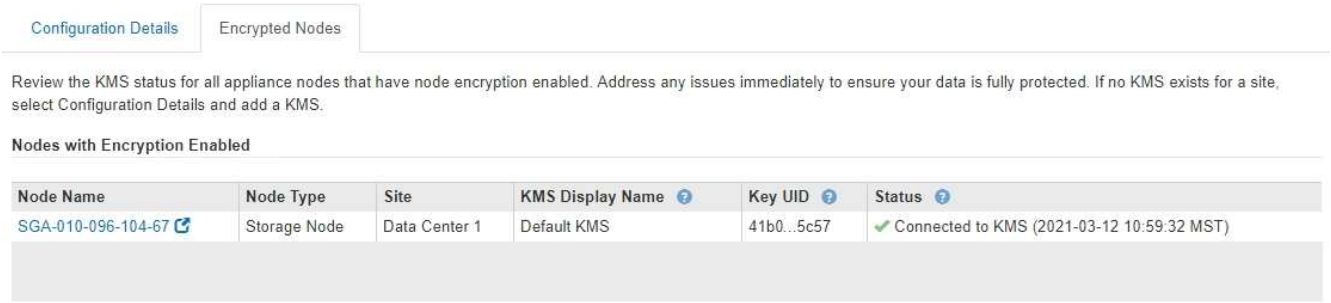
1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   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 ficha **nodos cifrados**.

   La ficha nodos cifrados muestra los nodos del dispositivo en el sistema StorageGRID que tienen activada la configuración * cifrado 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 visualización DE KMS	Nombre descriptivo del KMS utilizado para el nodo. Si no aparece ningún KMS, seleccione la ficha 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, pase el cursor por la celda. 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:** debe actualizar el explorador 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

Consulte las acciones recomendadas para estas alertas en las instrucciones de Supervisión y solución de problemas de StorageGRID.

> Debe solucionar cualquier problema inmediatamente para garantizar que los datos están totalmente protegidos.

Editar un servidor de gestión de claves (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.

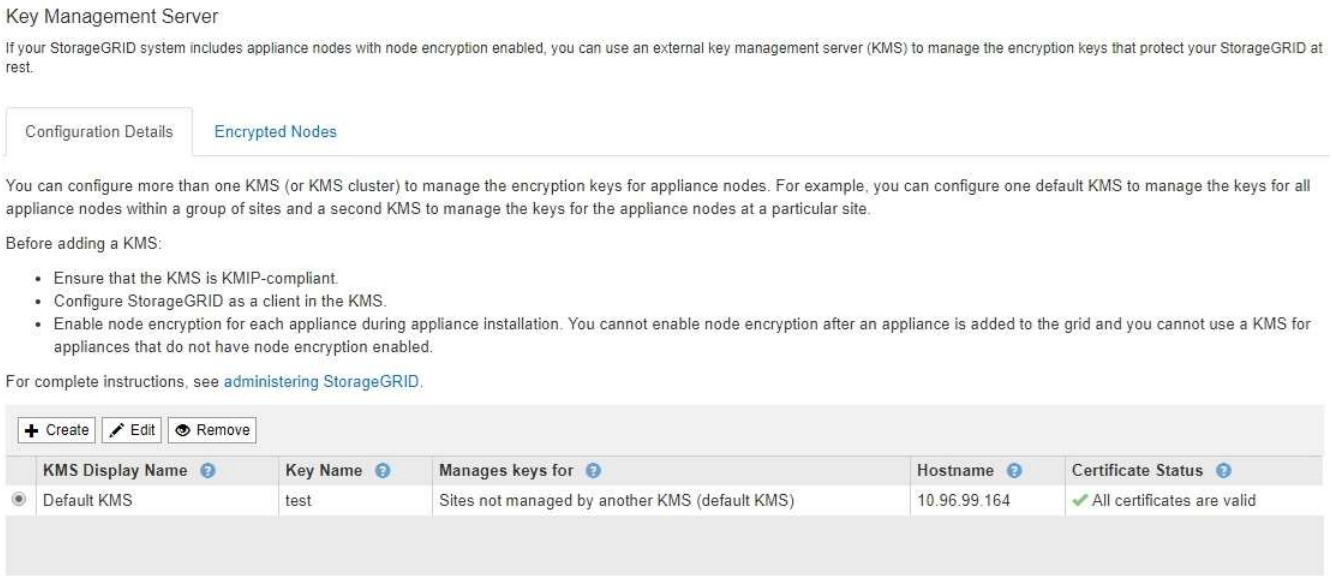
Lo que necesitará

- Ha revisado el consideraciones y requisitos para usar un servidor de gestión de claves.
- 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.
- Tiene el permiso acceso raíz.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Aparece la página servidor de gestión de claves para mostrar todos los servidores de gestión de claves configurados.



2. Seleccione el KMS que desea editar y seleccione **Editar**.

3. Opcionalmente, actualice los detalles en **Paso 1 (introducir detalles de KMS)** del asistente Editar un servidor de administración de claves.

Campo	Descripción
Nombre de visualización DE KMS	Un nombre descriptivo que le ayudará a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de la 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. Nunca intente girar una clave cambiando el nombre de clave (alias) del KMS. En su lugar, gire la clave actualizando la versión de la clave en el software 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. Consideraciones y requisitos para usar un servidor de gestión de claves
Administra claves para	Si va a editar un KMS específico del sitio y aún no tiene un KMS predeterminado, seleccione **Sitios no administrados 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 va a editar 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.
Nombre del hostl	El nombre de dominio completo o la dirección IP del KMS. **Nota:** el campo SAN del certificado de 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 va a configurar un clúster KMS, seleccione el signo más ➕ para agregar un nombre de host para cada servidor del clúster.
5. Seleccione **Siguiente**.

Aparece el paso 2 (cargar certificado de servidor) del asistente Editar un servidor de administración de claves.

6. Si necesita sustituir el certificado del servidor, seleccione **examinar** y cargue el nuevo archivo.
7. Seleccione **Siguiente**.

   Aparece el paso 3 (cargar certificados de cliente) del asistente Editar un servidor de gestión de claves.

8. Si necesita sustituir el certificado de cliente y la clave privada del certificado de cliente, seleccione **examinar** y cargue los nuevos archivos.
9. Seleccione **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**.

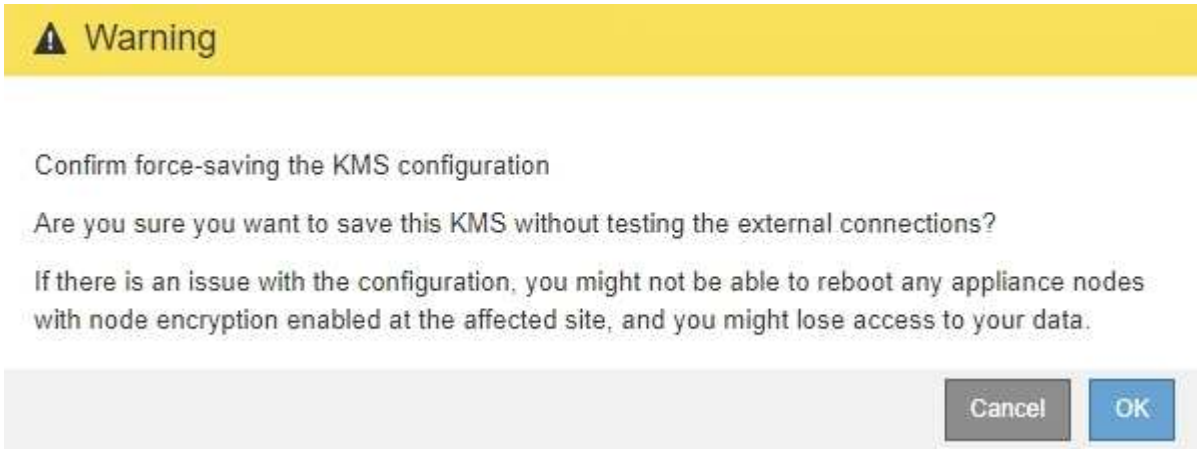
    Por ejemplo, puede recibir un error 422: Entidad no procesable si el sitio seleccionado para este KMS ya está administrado por otro KMS o si se produjo un error en una prueba de conexión.

11. Si necesita guardar la configuración actual antes de resolver los errores de conexión, seleccione **Forzar ahorro**.

    > 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 de KMS se guarda pero la conexión con el 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.

Lo que necesitará

- 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.
- Tiene el permiso acceso raíz.

Acerca de esta tarea

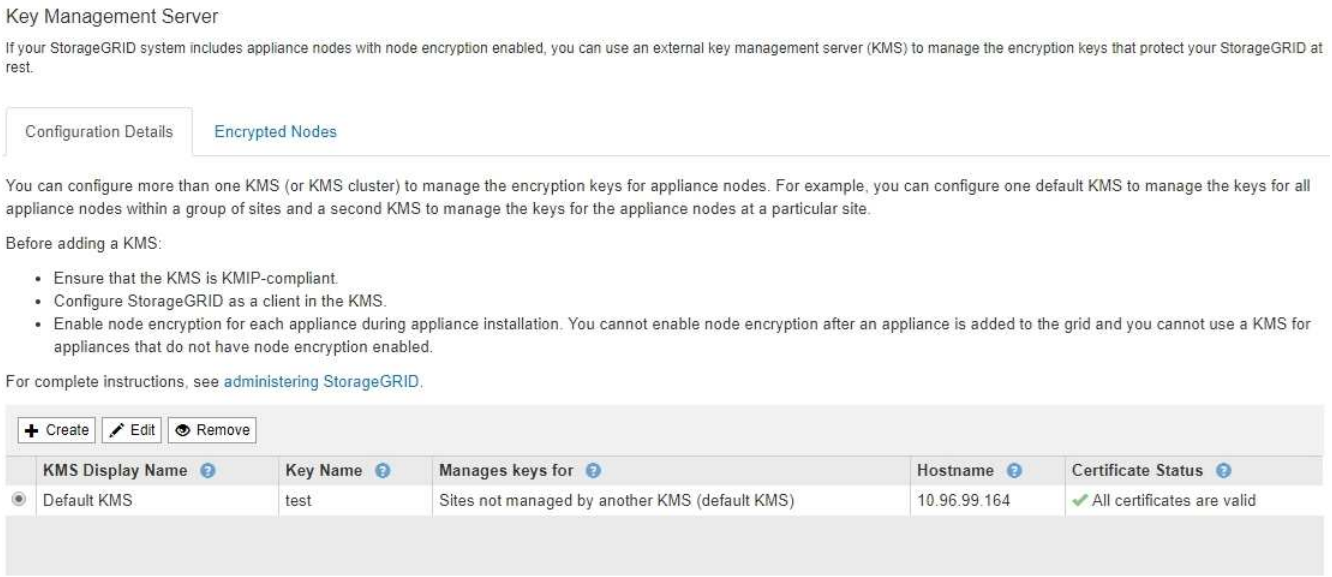
Puede eliminar un KMS en los siguientes casos:

- 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.

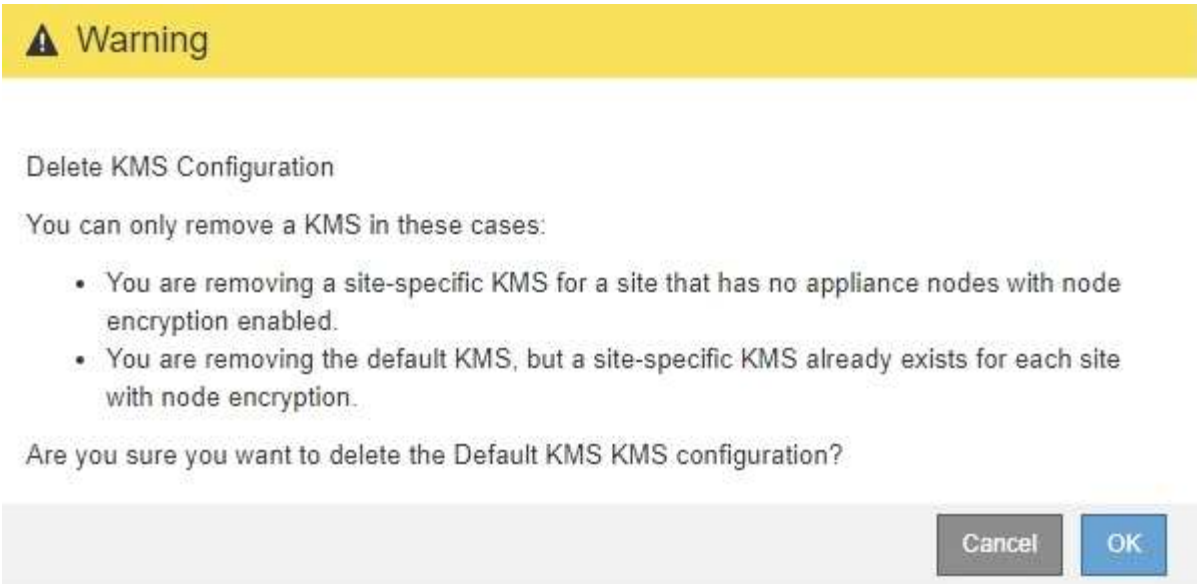
Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**.

   Aparece la página servidor de gestión de claves para mostrar todos los servidores de gestión de claves configurados.



2. Seleccione el botón de opción del KMS que desea quitar y seleccione **Quitar**.
3. Revise las consideraciones en el cuadro de diálogo de advertencia.



4. Seleccione **OK**.

   La configuración de KMS se elimina.

Administrar la configuración de proxy

Configure las opciones de 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.

Lo que necesitará

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

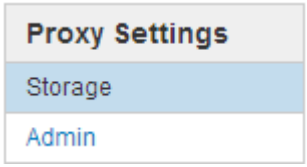
Acerca de esta tarea

Puede configurar los ajustes de un único proxy de almacenamiento.

Pasos

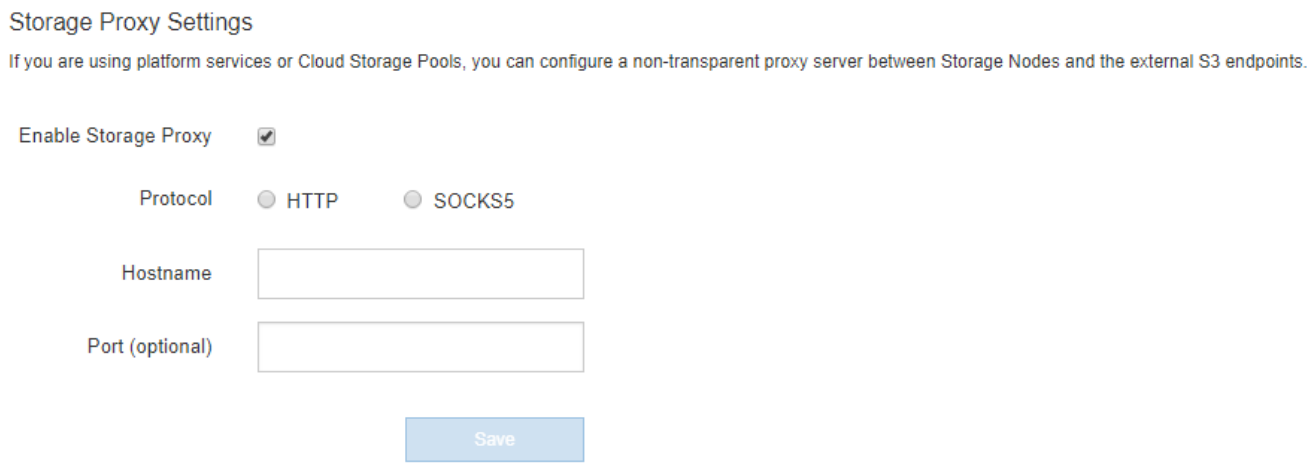
1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Ajustes de proxy**.

   Se muestra la página Storage Proxy Settings. De forma predeterminada, **almacenamiento** está seleccionado en el menú de la barra lateral.



2. Active la casilla de verificación **Activar proxy de almacenamiento**.

Aparecen los campos para configurar un proxy de almacenamiento.



3. Seleccione el protocolo del proxy de almacenamiento no transparente.
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.

   Puede dejar este campo en blanco si utiliza el puerto predeterminado para el protocolo: 80 para HTTP o 1080 para SOCKS5.

6. Seleccione **Guardar**.

   Una vez guardado el proxy de almacenamiento, se pueden configurar y probar nuevos extremos para los servicios de plataforma o Cloud Storage Pools.

   > 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.

Después de terminar

Si necesita desactivar un proxy de almacenamiento, anule la selección de la casilla de verificación **Activar proxy de almacenamiento** y seleccione **Guardar**.

Información relacionada

- Red y puertos para servicios de plataforma
- Gestión de objetos con ILM

Configure los ajustes del proxy de administración

Si envía mensajes de AutoSupport con HTTP o HTTPS (consulte Configure AutoSupport), puede configurar un servidor proxy no transparente entre los nodos de administración y el soporte técnico (AutoSupport).

Lo que necesitará

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

Acerca de esta tarea

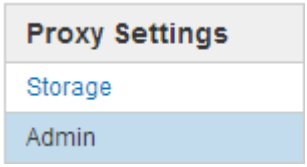
Puede configurar los ajustes de un único proxy de administración.

Pasos

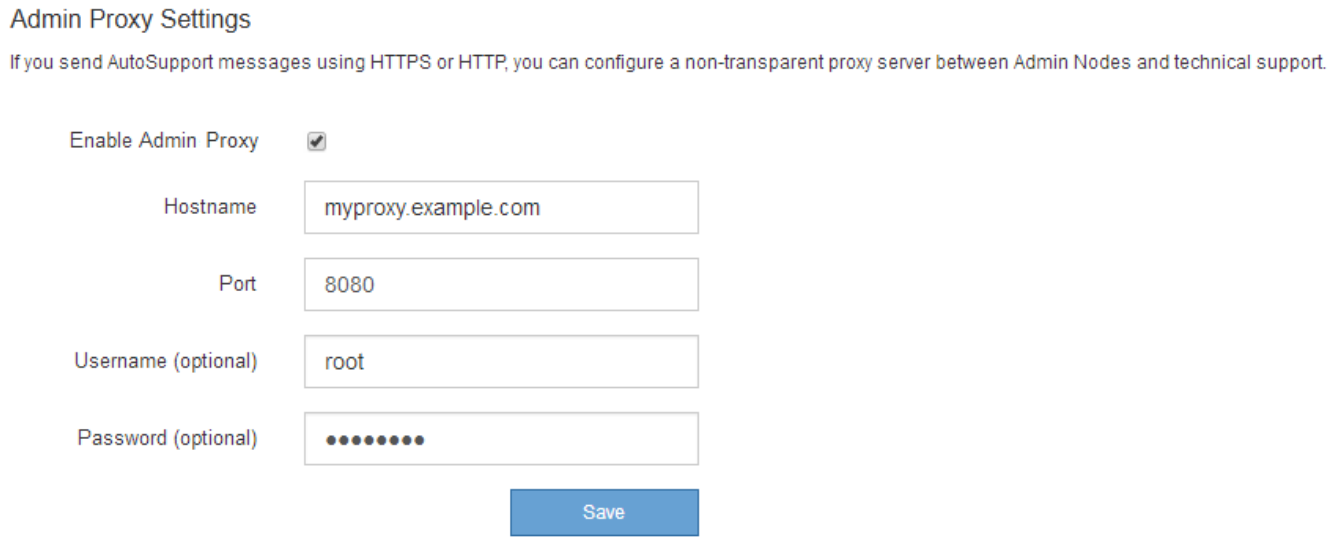
1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **Ajustes de proxy**.

   Aparece la página Admin Proxy Settings (Configuración del proxy de administración). De forma predeterminada, **almacenamiento** está seleccionado en el menú de la barra lateral.

2. En el menú de la barra lateral, seleccione **Admin**.



3. Active la casilla de verificación **Activar proxy de administración**.



4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. Introduzca el puerto utilizado para conectarse al servidor proxy.
6. Si lo desea, introduzca el nombre de usuario del proxy.

   Deje este campo en blanco si el servidor proxy no requiere un nombre de usuario.

7. De forma opcional, introduzca la contraseña del proxy.

   Deje este campo en blanco si el servidor proxy no requiere una contraseña.

8. Seleccione **Guardar**.

   Una vez guardado 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 desactivar el proxy, anule la selección de la casilla de verificación **Activar proxy de administración** y seleccione **Guardar**.

Administrar redes de clientes que no son de confianza

Administrar redes de clientes que no son de confianza: Descripción general

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 cuadrícula en todos los puertos externos disponibles (consulte la información acerca de las comunicaciones externas en Directrices sobre redes).

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.

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. En la página Load Balancer Endpoints, configure un extremo de equilibrador de carga para S3 a través de HTTPS en el puerto 443.
2. En la página redes de cliente no fiables, especifique que la red de 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

Supongamos que desea habilitar el tráfico saliente del servicio de la plataforma S3 desde un nodo de almacenamiento, pero desea impedir las conexiones entrantes a ese nodo de almacenamiento en la red cliente. Debe realizar este paso general:

- En la página redes de cliente no fiables, indique que la red de clientes del 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 solicitudes salientes a Amazon Web Services.

Especifique que la red de cliente del nodo no es de confianza

Si utiliza una red de cliente, puede especificar si la red de cliente de cada nodo es de confianza o no es de confianza. También puede especificar la configuración predeterminada para los nuevos nodos agregados en una ampliación.

Lo que necesitará

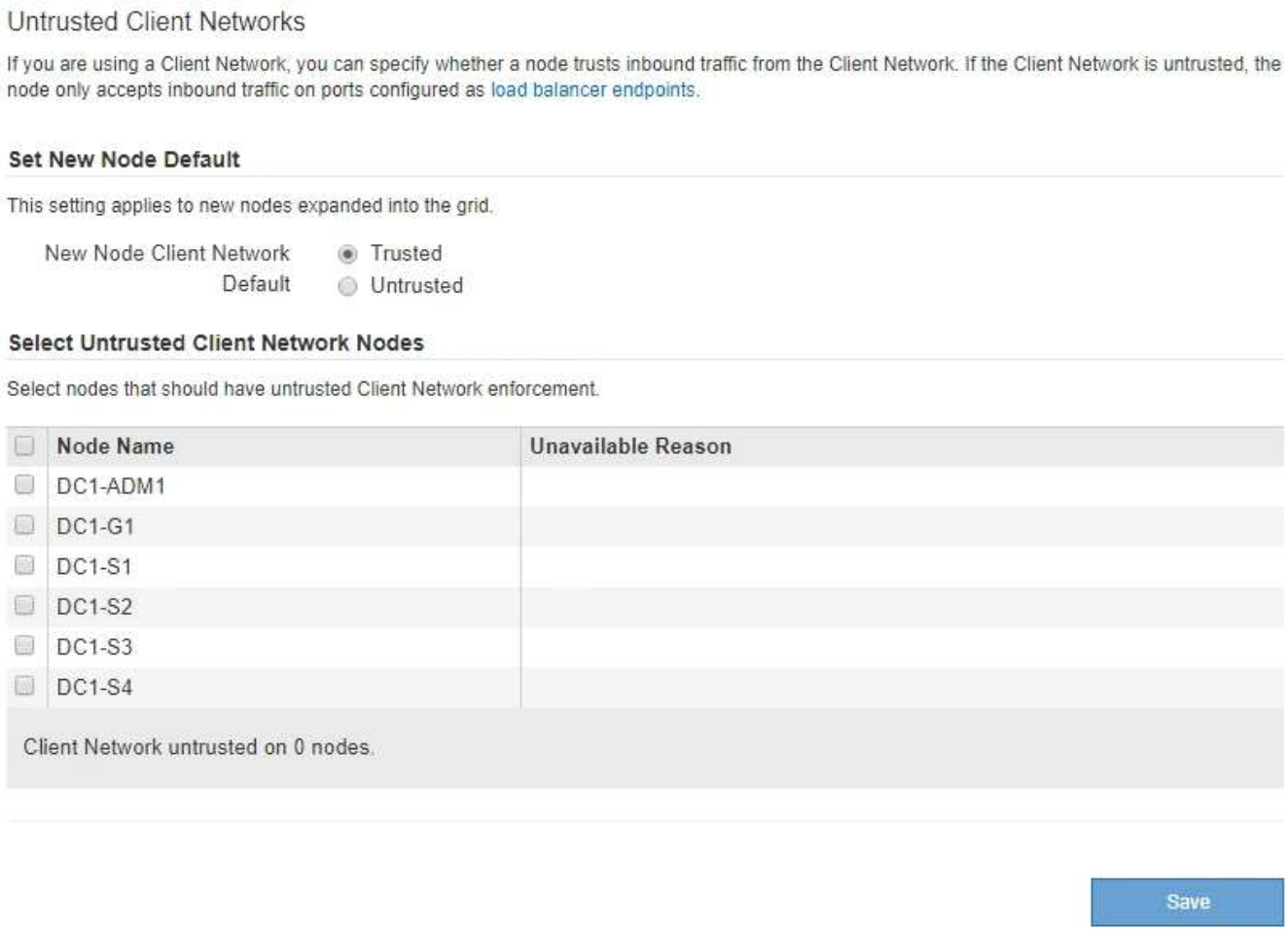
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.
- Si desea que un nodo de administración o un nodo de puerta de enlace acepte tráfico entrante sólo en puntos finales configurados explícitamente, ha definido los puntos finales del equilibrador de carga.

> Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **redes de cliente no fiables**.

   En la página redes de cliente no fiables se enumeran todos los nodos del sistema StorageGRID. La columna motivo no disponible incluye una entrada si la red de cliente del nodo debe ser de confianza.



2. En la sección **establecer nuevo nodo predeterminado** , especifique cuál debe ser la configuración predeterminada cuando se agregan nuevos nodos a la cuadrícula en un procedimiento de expansión.

   - **Trusted**: Cuando se agrega un nodo en una expansión, su red de 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 página para cambiar la configuración de un nuevo nodo concreto.

   > Esta configuración no afecta a los nodos existentes del sistema StorageGRID.

3. En la sección **Seleccionar nodos de red de cliente no confiable**, seleccione los nodos que deben permitir conexiones de cliente sólo en puntos finales de equilibrador de carga configurados explícitamente.

   Puede seleccionar o anular la selección de la casilla de comprobación en el título para seleccionar o anular la selección de todos los nodos.

4. Seleccione **Guardar**.

   Las nuevas reglas de firewall se agregan y aplican inmediatamente. Las conexiones de cliente existentes podrían fallar si no se han configurado extremos de equilibrador de carga.

Gestione inquilinos

Gestione inquilinos

Como administrador de grid, puede crear y gestionar las cuentas de inquilino que utilizan los clientes de S3 y Swift para almacenar y recuperar objetos, supervisar el uso del almacenamiento y gestionar las acciones que pueden realizar los clientes mediante el sistema StorageGRID.

¿Qué son las cuentas de inquilinos?

Las cuentas de inquilino permiten a las aplicaciones cliente que usan la API DE REST de simple Storage Service (S3) o la API DE REST de Swift para almacenar y recuperar objetos en StorageGRID.

Cada cuenta de inquilino admite el uso de un único protocolo, que se especifica al crear la cuenta. Para almacenar y recuperar objetos en un sistema StorageGRID con ambos protocolos, debe crear dos cuentas de inquilino: Una para los bloques y objetos de S3, y otra para los contenedores y objetos de Swift. Cada cuenta de inquilino tiene su propio ID de cuenta, grupos y usuarios autorizados, bloques o contenedores, y objetos.

Opcionalmente, puede crear cuentas de arrendatario adicionales si desea segregar los objetos almacenados en su sistema por entidades diferentes. Por ejemplo, puede configurar 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 cliente S3, puede utilizar bloques S3 y políticas de bucket para separar objetos entre los departamentos de una empresa. No es necesario utilizar cuentas de inquilino. Consulte las instrucciones para implementar aplicaciones cliente S3 para obtener 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.

Cree y configure cuentas de inquilino

Al crear una cuenta de inquilino, especifique la siguiente información:

- Nombre para mostrar de la cuenta de inquilino.
- Qué protocolo de cliente utilizará la cuenta de inquilino (S3 o Swift).
- Para las cuentas de inquilino de S3: Si la cuenta de inquilino tiene permiso para usar servicios de plataforma con bloques de S3. Si permite que las cuentas de arrendatario utilicen servicios de plataforma, debe asegurarse de que la cuadrícula está configurada para respaldar su uso. Consulte «gestionar servicios de plataforma».
- Opcionalmente, una cuota de almacenamiento para la cuenta de inquilino: El número máximo de gigabytes, terabytes o petabytes disponibles para los objetos del inquilino. Si se supera la cuota, el arrendatario no puede crear nuevos objetos.

  > La cuota de almacenamiento de un inquilino representa una cantidad lógica (tamaño de objeto), no una cantidad física (tamaño en disco).

- Si está habilitada la federación de identidades para el sistema StorageGRID, el grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.
- Si el sistema StorageGRID no utiliza el inicio de sesión único (SSO), tanto si la cuenta de inquilino usará su propio origen de identidad como si comparte el origen de identidad de la cuadrícula, así como la contraseña inicial del usuario raíz local del inquilino.

Después de crear una cuenta de inquilino, puede realizar las siguientes tareas:

- **Administrar servicios de plataforma para la red**: Si habilita servicios de plataforma para cuentas de inquilino, asegúrese de comprender cómo se entregan los mensajes de servicios de plataforma y los requisitos de red que el uso de servicios de plataforma tiene lugar en la implementación de StorageGRID.
- **Supervisar el uso del almacenamiento de una cuenta de inquilino**: Después de que los inquilinos comiencen a usar sus cuentas, puede utilizar Grid Manager para supervisar cuánto almacenamiento consume cada inquilino.

  > Los valores de uso de almacenamiento de un inquilino pueden dejar de estar obsoletos si se aíslan nodos de otros nodos del grid. Los totales se actualizarán cuando se restaure la conectividad de red.

  Si ha establecido cuotas para inquilinos, puede habilitar la alerta * uso de cuota de inquilino alto* para determinar si los inquilinos están consumiendo sus cuotas. Si está habilitada, esta alerta se activa cuando un inquilino ha utilizado el 90% de su cuota. Para obtener más información, consulte la referencia de alertas en las instrucciones para supervisar y solucionar problemas de StorageGRID.

- **Configurar operaciones de cliente**: Puede configurar si algunos tipos de operaciones de cliente están prohibidas.

Configure los inquilinos S3

Una vez creada una cuenta de inquilino de S3, los usuarios de inquilinos pueden acceder al administrador de inquilinos para realizar tareas como las siguientes:

- Configuración de la federación de identidades (a menos que el origen de identidades se comparta con la cuadrícula) y creación de grupos y usuarios locales
- Gestión de claves de acceso de S3
- Crear y gestionar bloques de S3
- Supervisión del uso de almacenamiento

- Uso de servicios de plataforma (si está activado)

> Los usuarios de inquilinos S3 pueden crear y gestionar bloques de clave de acceso S3 con el administrador de inquilinos, pero deben usar una aplicación cliente S3 para procesar y gestionar objetos.

Configure los inquilinos Swift

Después de crear una cuenta de inquilino de Swift, el usuario raíz del inquilino puede acceder al administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidades se comparta con la cuadrícula) y crear grupos y usuarios locales
- Supervisión del uso de 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 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.

Información relacionada

Usar una cuenta de inquilino

Cree una cuenta de inquilino

Debe crear al menos una cuenta de inquilino para controlar el acceso al almacenamiento en su sistema de StorageGRID.

Al crear una cuenta de inquilino, se especifica un nombre, un protocolo de cliente y, opcionalmente, una cuota de almacenamiento. Si se habilitó el inicio de sesión único (SSO) para StorageGRID, también se especifica qué grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino. Si StorageGRID no utiliza el inicio de sesión único, también debe especificar si la cuenta de inquilino utilizará su propio origen de identidad y configurar la contraseña inicial para el usuario raíz local del inquilino.

Grid Manager proporciona un asistente que le guía por los pasos para crear una cuenta de arrendatario. Los pasos 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- 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 instrucciones para administrar grupos de administración.

Pasos

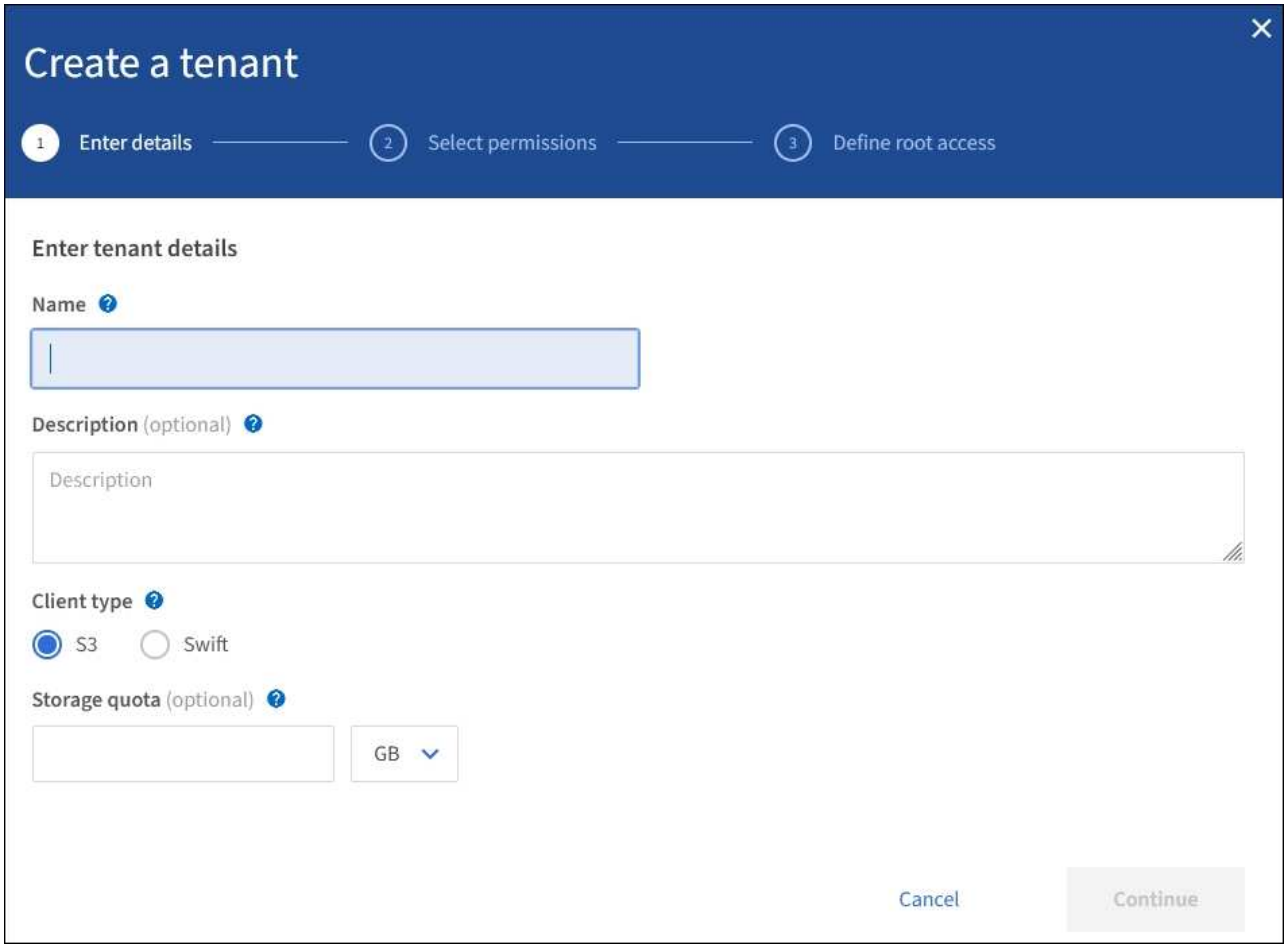
1. Seleccione **ARRENDATARIOS**.
2. Seleccione **Crear** e introduzca la siguiente información para el arrendatario:

a. **Nombre**: Introduzca un nombre para la cuenta de arrendatario. Los nombres de inquilinos no tienen que ser únicos. Cuando se crea la cuenta de arrendatario, recibe un ID de cuenta numérico único.

b. **Descripción** (opcional): Introduzca una descripción que le ayude a identificar al inquilino.

c. **Tipo de cliente**: Seleccione el tipo de cliente de **S3** o **Swift**.

d. **Cuota de almacenamiento** (opcional): Si desea que este arrendatario tenga una cuota de almacenamiento, introduzca un valor numérico para la cuota y seleccione las unidades correctas (GB, TB o PB).



3. Seleccione **continuar** y configure el inquilino S3 o Swift.

Inquilino de S3

Seleccione los permisos apropiados para el arrendatario. Algunos de estos permisos tienen requisitos adicionales. Para obtener más detalles, consulte la ayuda en línea de cada permiso.

- Permitir los servicios de plataforma
- Utilizar su propio origen de identidad (seleccionable solo si no se utiliza SSO)
- Permitir selección de S3 (consulte Gestione S3 Select para cuentas de inquilinos)

Inquilino de Swift

Si el inquilino utilizará su propia fuente de identidad, seleccione **usar su propia fuente de identidad** (seleccionable sólo si no se utiliza SSO).

1. Seleccione **continuar** y defina el acceso raíz para la cuenta de arrendatario.

federación de identidades no configurada

1. Introduzca una contraseña para el usuario raíz local.
2. Seleccione **Crear arrendatario**.

SSO habilitado

Cuando SSO está habilitado para StorageGRID, el inquilino debe utilizar el origen de identidad configurado para Grid Manager. Ningún usuario local puede iniciar sesión. Especifique qué grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.

1. Seleccione un grupo federado existente en Grid Manager para tener el permiso de acceso raíz inicial para el arrendatario.

> Si dispone de los permisos adecuados, se mostrarán los grupos federados existentes del Gestor de grid al seleccionar el campo. De lo contrario, introduzca el nombre exclusivo del grupo.

2. Seleccione **Crear arrendatario**.

SSO no está habilitado

1. Complete los pasos descritos en la tabla en función de si el inquilino gestionará sus propios grupos y usuarios o utilizará el origen de identidad configurado para Grid Manager.

Si el inquilino…	Realice lo siguiente…
Administrar sus propios grupos y usuarios	a. Seleccione **usar la propia fuente de identidad**. **Nota**: Si esta casilla de verificación está seleccionada y desea utilizar la federación de identidades para grupos de arrendatarios y usuarios, el arrendatario debe configurar su propio origen de identidad. Consulte instrucciones para el uso de cuentas de inquilino. b. Especifique una contraseña para el usuario raíz local del arrendatario y, a continuación, seleccione **Crear arrendatario**. c. Seleccione **Iniciar sesión como root** para configurar el arrendatario, o seleccione **Finalizar** para configurar el arrendatario más tarde.
Utilice los grupos y usuarios configurados para Grid Manager	a. Realice una o ambas de las siguientes acciones: ◦ Seleccione un grupo federado existente en el Gestor de grid que tenga el permiso de acceso raíz inicial para el arrendatario. **Nota**: Si dispone de los permisos adecuados, los grupos federados existentes de Grid Manager aparecen cuando seleccione el campo. De lo contrario, introduzca el nombre exclusivo del grupo. ◦ Especifique una contraseña para el usuario raíz local del inquilino. b. Seleccione **Crear arrendatario**.

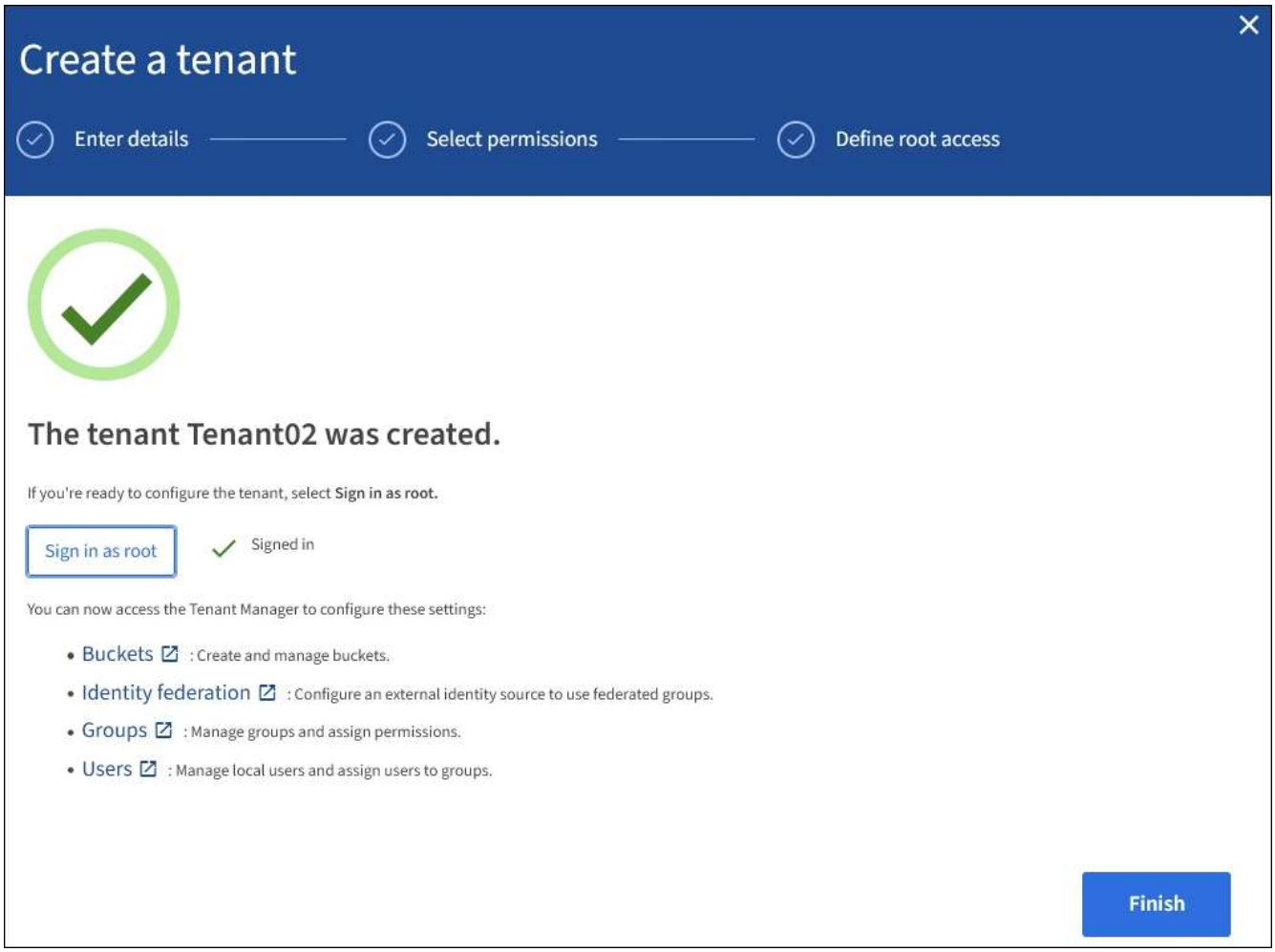
1. Para iniciar sesión en el inquilino ahora:
   - Si tiene acceso a Grid Manager en un puerto restringido, seleccione **restringido** en la tabla arrendatario para obtener más información sobre cómo acceder a esta cuenta de arrendatario.

     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
   - Si está accediendo a Grid Manager en el puerto 443 pero no ha establecido una contraseña para el usuario raíz local, en la tabla Tenants del Grid Manager, seleccione **Iniciar sesión** e introduzca las credenciales de un usuario en el grupo federado de acceso raíz.
   - Si va a acceder a Grid Manager en el puerto 443 y establece una contraseña para el usuario raíz local:
     i. Seleccione **Iniciar sesión como root** para configurar el arrendatario ahora.

     Al iniciar sesión, aparecen enlaces para configurar bloques o contenedores, federación de identidades, grupos y usuarios.



i. 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.

ii. De lo contrario, seleccione **Finalizar** para acceder al arrendatario más adelante.

2. Para acceder al inquilino más adelante:

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

Información relacionada

- Controlar el acceso mediante firewalls
- Gestione servicios de plataformas para cuentas de inquilinos de S3

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.

Lo que necesitará

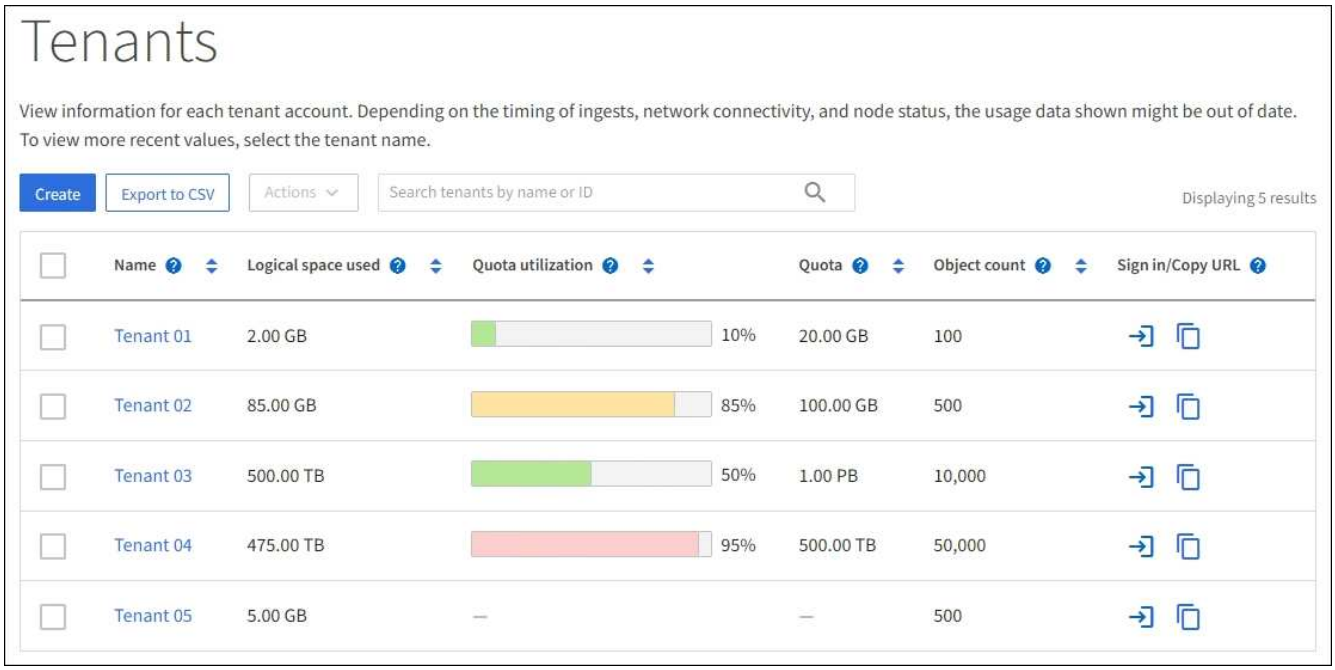
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

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 arrendatario que desee editar.

   Se habilita el botón Actions.

3. En el menú desplegable **acciones**, seleccione **Cambiar contraseña raíz**.
4. Introduzca la nueva contraseña de la cuenta de inquilino.
5. Seleccione **Guardar**.

Edite la cuenta de inquilino

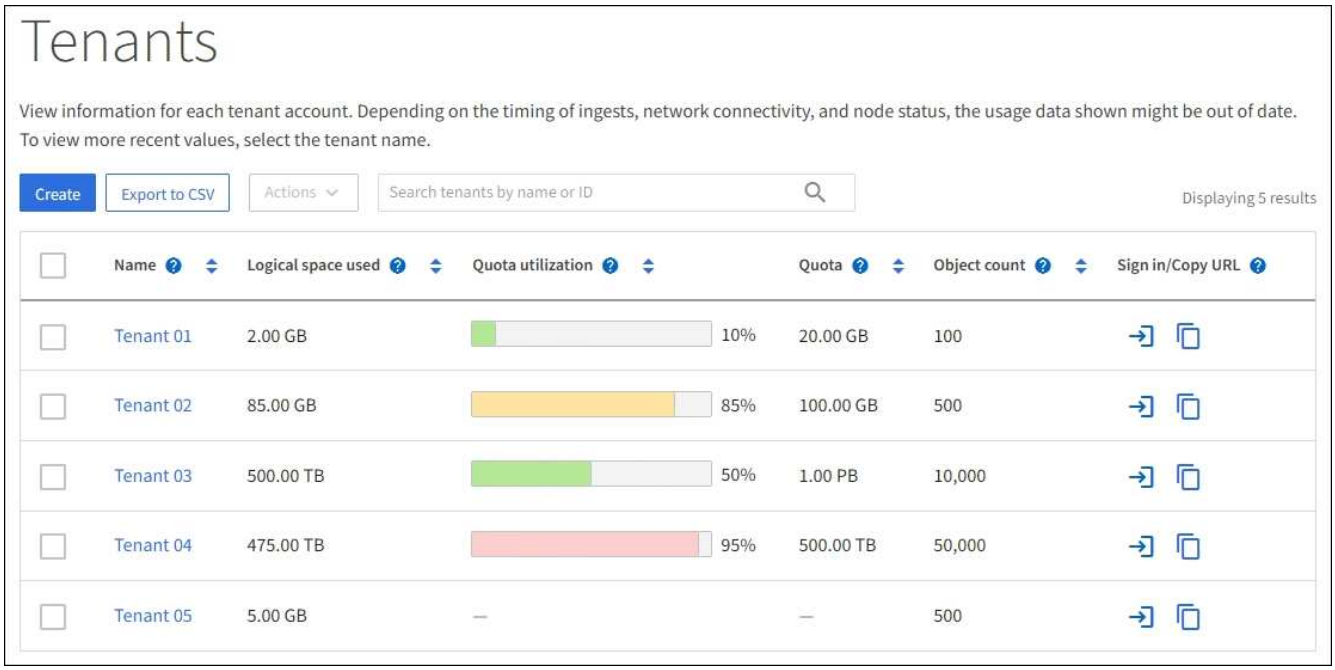
Puede editar una cuenta de arrendatario para cambiar el nombre para mostrar, cambiar la configuración del origen de identidad, permitir o desactivar servicios de plataforma o introducir una cuota de almacenamiento.

Lo que necesitará

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

Pasos

1. Seleccione **ARRENDATARIOS**.

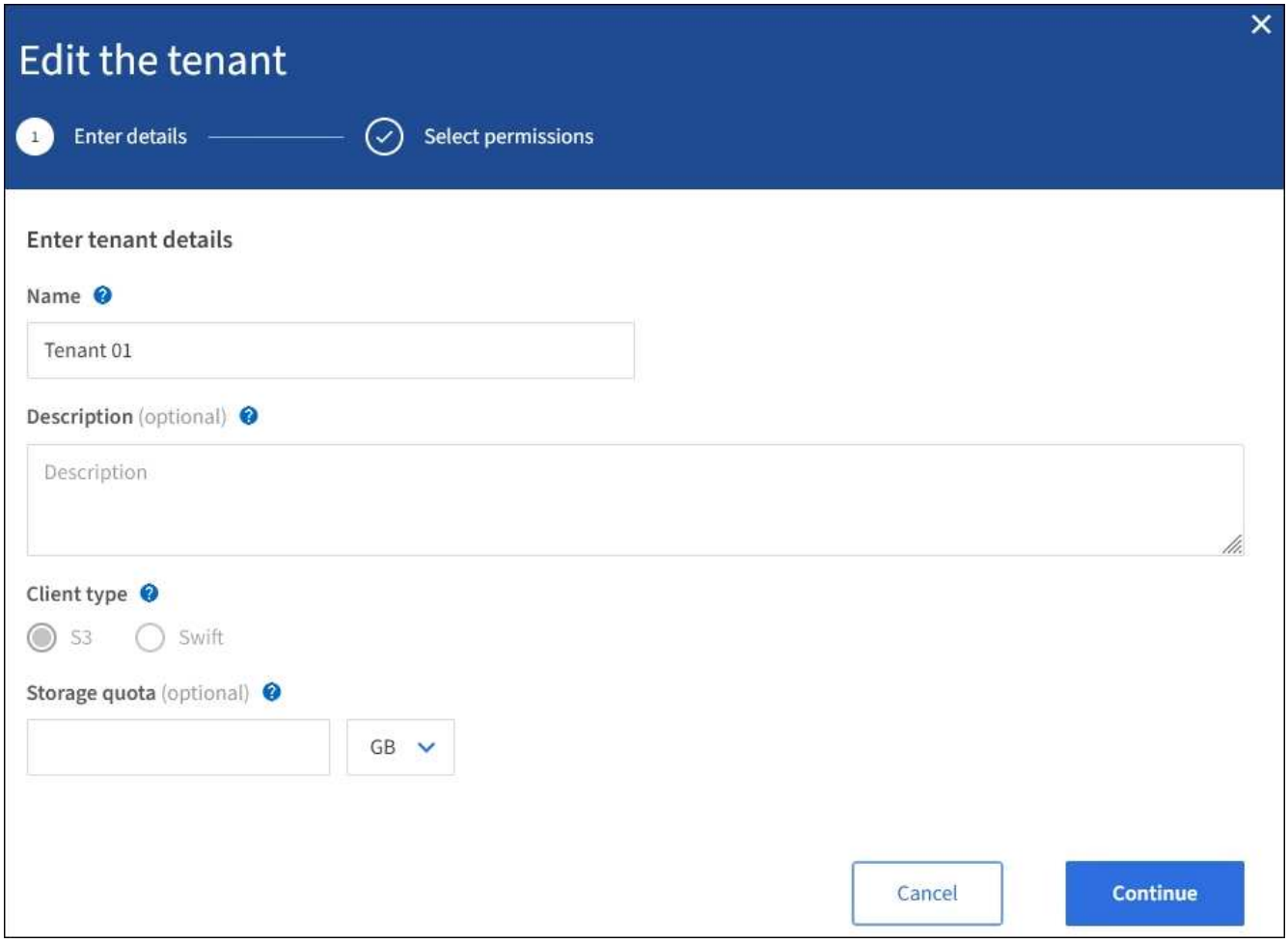


2. Seleccione la cuenta de arrendatario que desee editar.

   Utilice el cuadro de búsqueda para buscar una cuenta de inquilino por nombre o ID de inquilino.

3. En el menú desplegable acciones, seleccione **Editar**.

   Este ejemplo se utiliza para una cuadrícula que no utiliza el inicio de sesión único (SSO). Esta cuenta de inquilino no ha configurado su propio origen de identidad.



4. Cambie los valores de estos campos según sea necesario:
   - **Nombre**
   - **Descripción**
   - **Tipo de cliente**
   - **Cuota de almacenamiento**
5. Seleccione **continuar**.
6. Seleccione o anule la selección de 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.
   - Cambie la configuración de la casilla de verificación **usa el origen de identidad propio** para determinar si la cuenta de arrendatario utilizará su propio origen de identidad o el origen de identidad configurado para el administrador de cuadrícula.

     Si la casilla de verificación **usa el origen de identidad propio** 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.

        - Deshabilitado e ilimitado, SSO se encuentra habilitado para el sistema StorageGRID. El inquilino debe utilizar el origen de identidad configurado para el administrador de grid.
    - Activa o desactiva **S3 Select** según sea necesario. Consulte Gestione S3 Select para cuentas de inquilinos.
7. Seleccione **Guardar**.

Información relacionada

- Gestione servicios de plataformas para cuentas de inquilinos de S3
- Usar una cuenta de inquilino

Eliminar cuenta de inquilino

Puede eliminar una cuenta de inquilino si desea eliminar de forma permanente el acceso del inquilino al sistema.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener permisos de acceso específicos.
- Debe haber quitado todos los bloques (S3), los contenedores (Swift) y los objetos asociados con la cuenta de inquilino.

Pasos

1. Seleccione **ARRENDATARIOS**.
2. Seleccione la cuenta de arrendatario que desea eliminar.

   Utilice el cuadro de búsqueda para buscar una cuenta de inquilino por nombre o ID de inquilino.
3. En el menú desplegable **acciones**, seleccione **Eliminar**.
4. Seleccione **OK**.

Gestione los servicios de la plataforma

Gestione servicios de plataformas para cuentas de inquilinos de S3

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.

Estos servicios permiten a los inquilinos utilizar la siguiente funcionalidad con sus bloques S3:

- **Duplicación de CloudMirror**: El servicio de replicación de CloudMirror de StorageGRID se utiliza 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**: Las notificaciones de eventos por bloque se usan para enviar notificaciones sobre acciones específicas realizadas en objetos a un Amazon simple Notification Service™ (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**: El servicio de integración de búsqueda se usa para enviar metadatos de objetos S3 a un índice de Elasticsearch especificado donde se pueden buscar o analizar los metadatos utilizando 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 extremo que no se puedan completar se pondrán en cola para un máximo de 500,000 solicitudes. Este límite se comparte por igual entre los inquilinos activos. Los nuevos inquilinos pueden superar temporalmente este límite de 500,000 para que los nuevos inquilinos no se vean penalizados de forma injusta.

Información relacionada

- Usar una cuenta de inquilino
- Configure las opciones de proxy de almacenamiento
- Supervisión y solución de problemas

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
- Aplicación local que admite la recepción de mensajes del servicio de notificación simple (SNS)
- 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 los URI de punto final que comienzan con http
- **443**: Para los URI de punto final que comienzan con https

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 de proxy de almacenamiento para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

Información relacionada

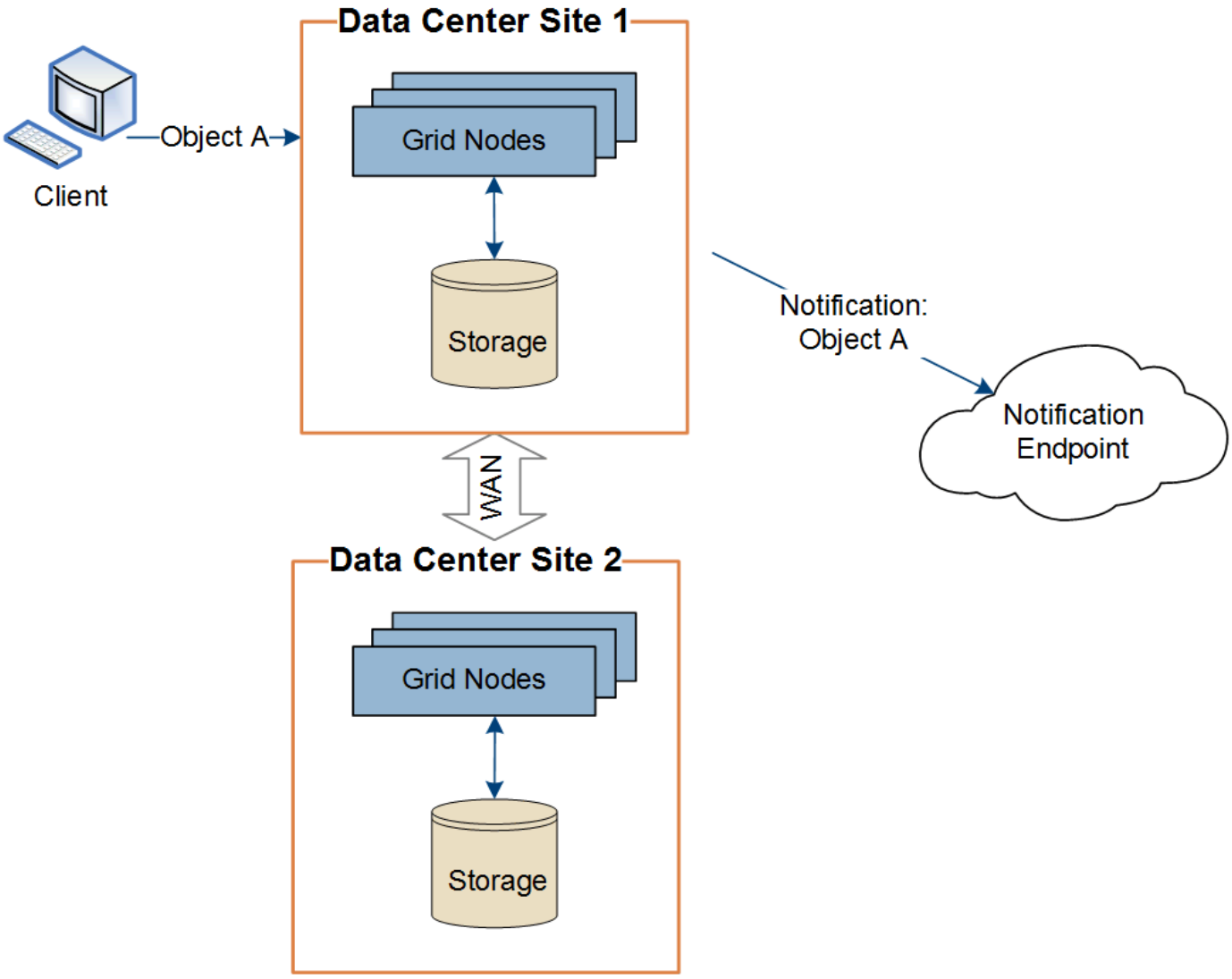
- Usar una cuenta de inquilino

Entrega de mensajes de servicios de plataforma por sitio

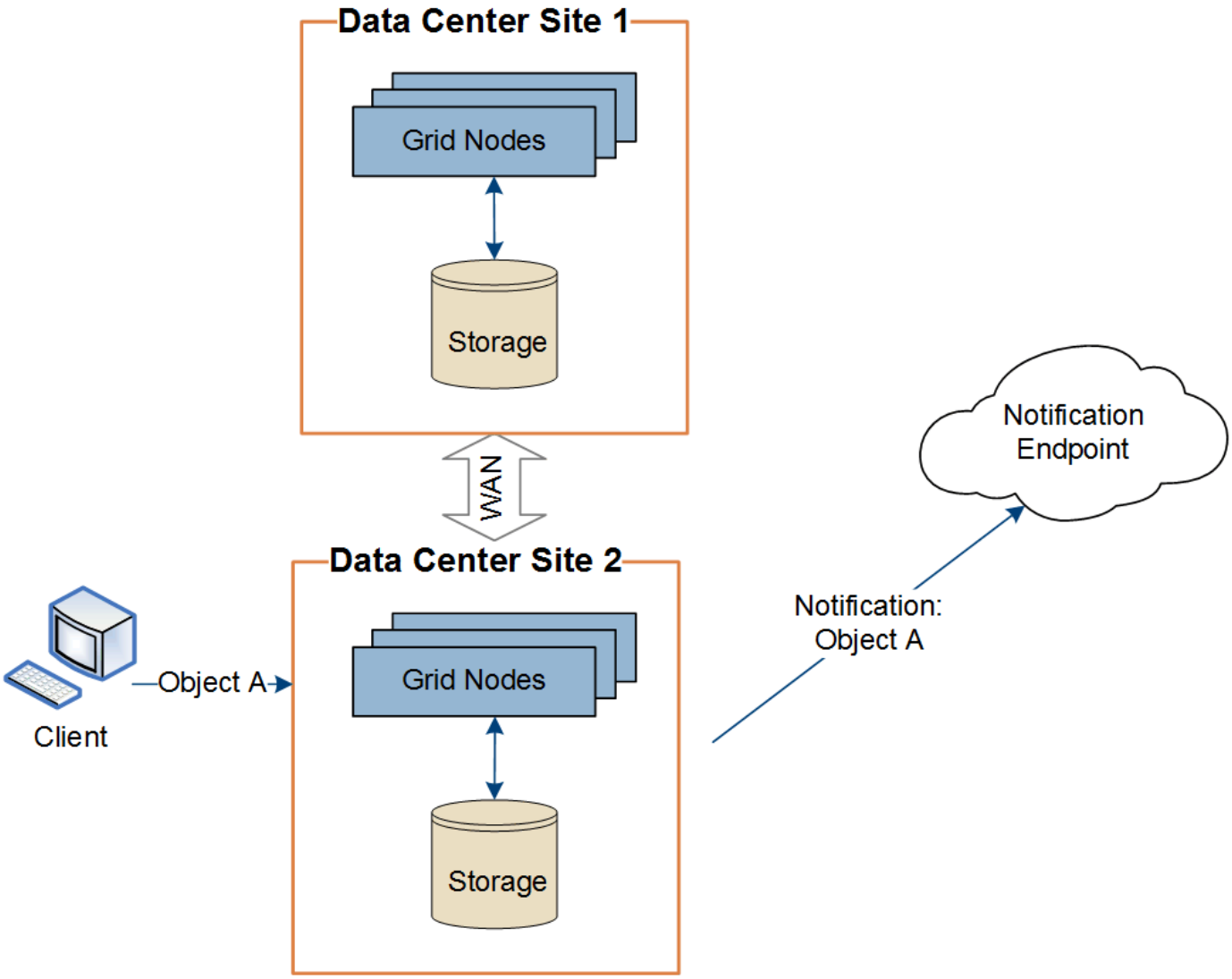
Todas las operaciones de servicios de plataforma se realizan in situ.

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 bloque de StorageGRID S3, un bloque de Amazon Web Services, un tema de servicio de notificación simple 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.

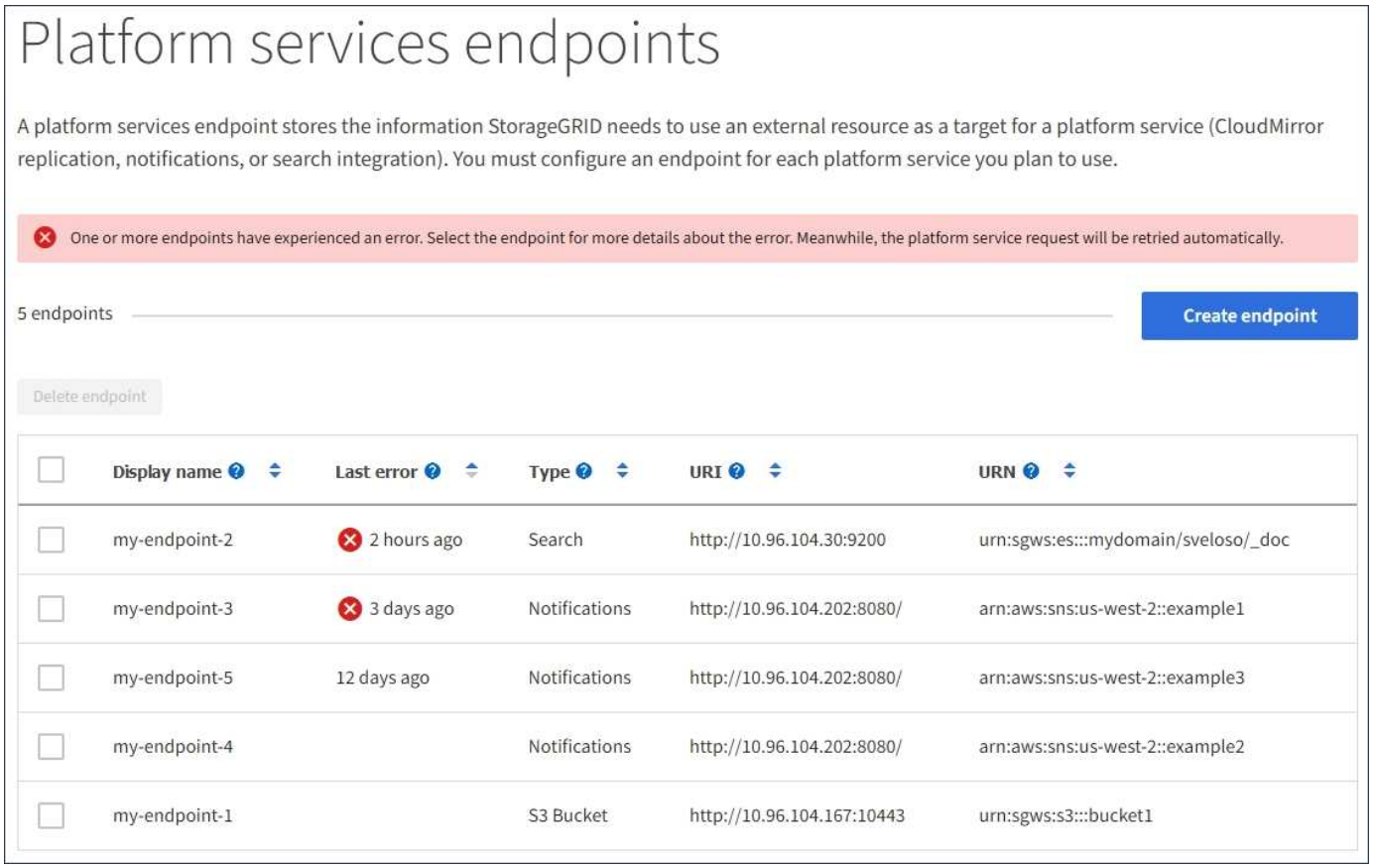
> Se producirá un error al crear el extremo si los servicios de plataforma no están habilitados para la cuenta de inquilino.

Problemas con los extremos existentes

Si se produce un error cuando StorageGRID intenta acceder a un extremo existente, se muestra un mensaje en la consola del administrador 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 configuró un proxy de almacenamiento entre nodos de almacenamiento y extremos de servicio de plataforma, se pueden producir errores si el servicio del proxy no permite los mensajes de StorageGRID. Para resolver estos problemas, compruebe la configuración del servidor proxy para asegurarse de que los mensajes relacionados con el servicio de la plataforma no están bloqueados.

Determine si se ha producido un error

Si se han producido errores de extremo en los últimos 7 días, la consola del administrador 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.
- La notificación no se puede entregar.

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 la 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 no se pueden entregar mensajes de servicios de plataforma debido a un error irrecuperable, la alarma heredada total de eventos (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.

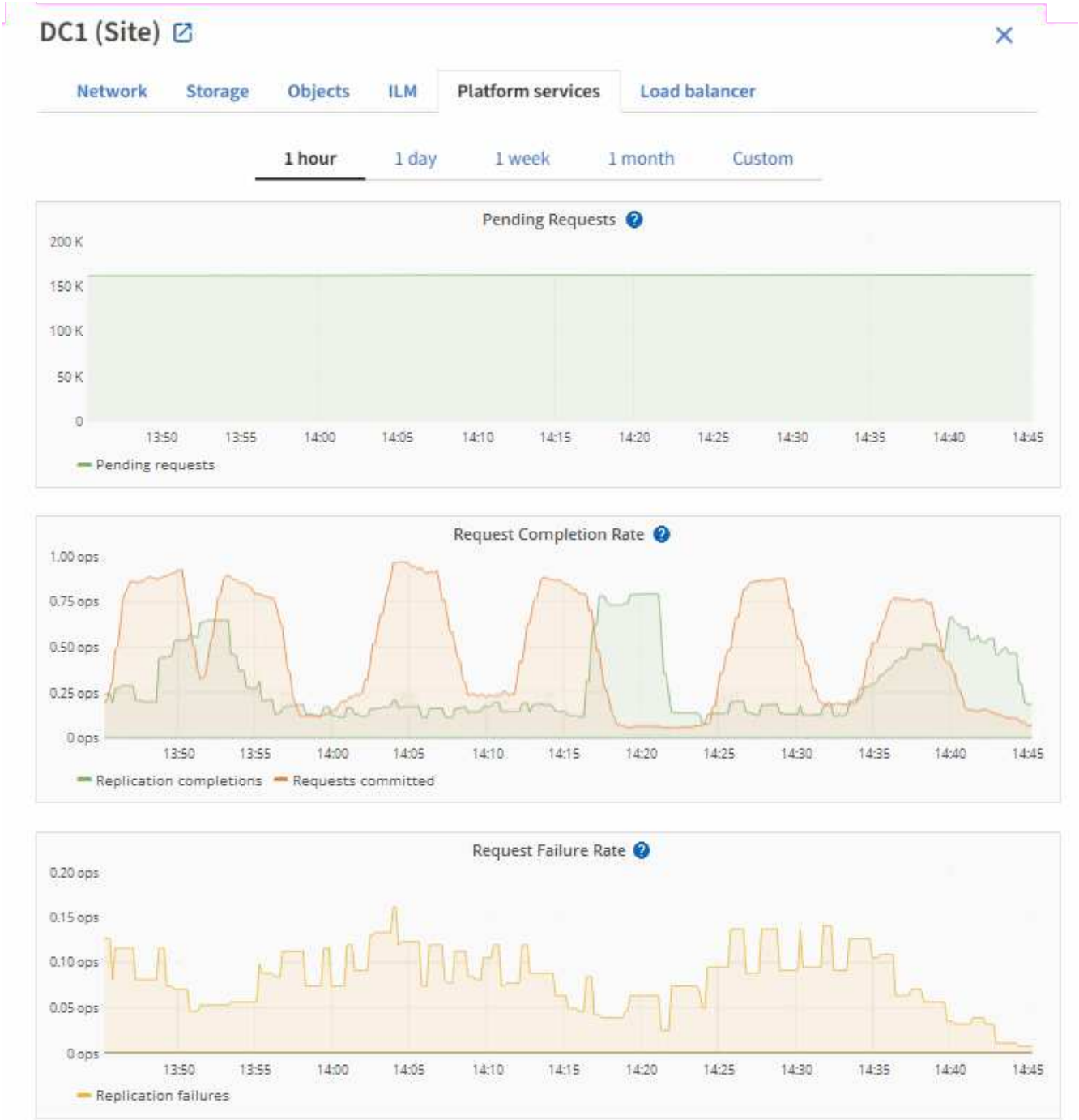
El único efecto visible es que las solicitudes entrantes de S3 tardarán más en ejecutarse. Si empieza a detectar un rendimiento significativamente más lento, debe reducir la tasa de procesamiento o utilizar un extremo con mayor capacidad. Si la acumulación de solicitudes sigue creciendo, las operaciones 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. Seleccione **NODES**.
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 sobre la solución de problemas de los extremos de servicios de la plataforma, consulte las instrucciones para usar una cuenta de inquilino.

Información relacionada

- Supervisión y solución de problemas
- Configure las opciones de proxy de almacenamiento

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

StorageGRID requiere lo siguiente para consultas S3 Select:

- El objeto que desea consultar tiene el formato CSV o es un archivo comprimido GZIP o BZIP2 que contiene un archivo con formato CSV.
- El administrador de grid debe otorgar a los inquilinos la capacidad de S3 Select. Seleccione **permitir selección de S3** cuando crear un inquilino o. edición de un arrendatario.
- La solicitud SelectObjectContent debe enviarse a un Extremo del equilibrador de carga de StorageGRID. Los nodos de administración y puerta de enlace que utiliza el extremo deben ser nodos de dispositivo SG100 o SG1000 o nodos de software basados en VMware.

Tenga en cuenta las siguientes limitaciones:

- No se admiten los nodos de equilibrador de carga de configuración básica.
- Las consultas no se pueden enviar directamente a los nodos de almacenamiento.
- Las consultas enviadas a través del servicio CLB obsoleto no son compatibles.

> 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.

Configure las conexiones de clientes S3 y Swift

Acerca de las conexiones de los clientes S3 y Swift

Como administrador de grid, gestiona las opciones de configuración que controlan cómo los inquilinos S3 y Swift pueden conectar las aplicaciones cliente con el sistema StorageGRID para almacenar y recuperar datos. Hay una serie de opciones diferentes para responder a los distintos requisitos de cliente y cliente.

Las aplicaciones cliente pueden almacenar o recuperar objetos conectándose a cualquiera de los siguientes elementos:

- El servicio Load Balancer en los nodos de administrador o de puerta de enlace, o bien, de forma opcional, la dirección IP virtual de un grupo de alta disponibilidad (ha) de nodos de administración o nodos de puerta de enlace
- El servicio CLB en los nodos de puerta de enlace o, opcionalmente, la dirección IP virtual de un grupo de nodos de puerta de enlace de alta disponibilidad

> El servicio CLB está obsoleto. Los clientes configurados antes de la versión StorageGRID 11.3 pueden seguir utilizando el servicio CLB en los nodos de puerta de enlace. El resto de aplicaciones cliente que dependen de StorageGRID para proporcionar equilibrio de carga se deben conectar mediante el servicio Load Balancer.

- Nodos de almacenamiento, con o sin un equilibrador de carga externo

Opcionalmente, puede configurar las siguientes funciones en el sistema StorageGRID:

- * Interfaces VLAN*: Puede crear interfaces LAN virtuales (VLAN) en nodos de administración y nodos de puerta de enlace para aislar y dividir el tráfico de cliente y cliente para seguridad, flexibilidad y rendimiento. Después de crear una interfaz VLAN, lo debe agregar a un grupo de alta disponibilidad.
- **Grupos de alta disponibilidad**: Puede crear un grupo ha de las interfaces para nodos de puerta de enlace o nodos de administración para crear una configuración de copia de seguridad activa, o puede utilizar DNS round-robin o un equilibrador de carga de terceros y varios grupos ha para lograr una configuración activo-activo. Las conexiones de clientes se realizan mediante las direcciones IP virtuales de los grupos de alta disponibilidad.
- **Servicio de equilibrador de carga**: Puede permitir a los clientes utilizar el servicio de equilibrador de carga mediante la creación de puntos finales de equilibrador de carga para las conexiones de cliente. Al crear un extremo de equilibrio de carga, especifica un número de puerto, si el extremo acepta conexiones HTTP o HTTPS, el tipo de cliente (S3 o Swift) que utilizará el extremo y el certificado que se utilizará para las conexiones HTTPS (si procede).
- **Red cliente no confiable**: Puede hacer que la Red cliente sea más segura configurándola como no confiable. Cuando la red de cliente no es de confianza, los clientes sólo pueden conectarse utilizando puntos finales de equilibrador de carga.

También es posible habilitar el uso de HTTP para los clientes que se conectan a StorageGRID directamente a los nodos de almacenamiento o mediante el servicio CLB (obsoleto), y es posible configurar los nombres de dominio de extremo de la API de S3 para los clientes S3.

Resumen: Direcciones IP y puertos para conexiones cliente

Las aplicaciones cliente pueden conectarse a StorageGRID utilizando la dirección IP de un nodo de grid y el número de puerto de un servicio en ese nodo. Si se configuran los grupos de alta disponibilidad, las aplicaciones cliente se pueden conectar mediante la dirección IP virtual del grupo de alta disponibilidad.

Acerca de esta tarea

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. En las instrucciones se describe cómo encontrar esta información en Grid Manager si ya se han configurado puntos finales de equilibrador de carga y grupos de alta disponibilidad (ha).

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 de punto final del equilibrador de carga
Grupo de ALTA DISPONIBILIDAD	CLB **Nota:** el servicio CLB está en desuso.	La dirección IP virtual de un grupo de alta disponibilidad	Puertos S3 predeterminados: • HTTPS: 8082 • HTTP: 8084 Puertos Swift predeterminados: • HTTPS:8083 • HTTP: 8085
Nodo de administración	Equilibrador de carga	La dirección IP del nodo de administrador	• Puerto de punto final del equilibrador de carga
Nodo de puerta de enlace	Equilibrador de carga	La dirección IP del nodo de puerta de enlace	• Puerto de punto final del equilibrador de carga

Dónde se realiza la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
Nodo de puerta de enlace	CLB **Nota:** el servicio CLB está en desuso.	La dirección IP del nodo de puerta de enlace **Nota:** de forma predeterminada, los puertos HTTP para CLB y LDR no están habilitados.	Puertos S3 predeterminados: • HTTPS: 8082 • HTTP: 8084 Puertos Swift predeterminados: • HTTPS:8083 • HTTP: 8085
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

Ejemplos

Para conectar un cliente S3 al extremo de equilibrio de carga de un grupo ha de nodos de puerta de enlace, 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 de alta disponibilidad es 192.0.2.5 y el número de puerto de un extremo de equilibrio de carga de S3 es 10443, un cliente de S3 puede usar la siguiente URL para conectarse a StorageGRID:

- `https://192.0.2.5:10443`

Para conectar un cliente Swift al extremo Load Balancer de un grupo de 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 de alta disponibilidad es 192.0.2.6 y el número de puerto de un extremo de equilibrio de carga de Swift es 10444, un cliente de Swift puede usar la siguiente URL para conectarse a StorageGRID:

- `https://192.0.2.6:10444`

Es posible configurar un nombre DNS para la dirección IP que utilizan los clientes para conectarse a

StorageGRID. Póngase en contacto con el administrador de red local.

Pasos

1. Inicie sesión en Grid Manager mediante una navegador web compatible.
2. Para encontrar la dirección IP de un nodo de grid:
   a. Seleccione **NODES**.
   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**.

      Aparece la página Load Balancer Endpoints, donde se muestra la lista de puntos finales que ya se han configurado.

   b. Seleccione un punto final y seleccione **Editar punto final**.

      Se abre la ventana Edit Endpoint y se muestran detalles adicionales sobre el extremo.

   c. Confirme que el extremo que ha seleccionado está configurado para su uso con el protocolo correcto (S3 o Swift) y, a continuación, seleccione **Cancelar**.
   d. Tenga en cuenta el número de puerto del extremo que desea utilizar para una conexión de cliente.

      > Si el número de puerto es 80 o 443, el extremo se configura únicamente en los nodos de puerta de enlace, ya que esos puertos están reservados en los nodos de administración. Todos los demás puertos están configurados tanto en los nodos de puerta de enlace como en los de administración.

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 tanto la interfaz de red de cuadrícula como la interfaz de red de cliente en el mismo nodo de puerta de enlace 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 o CentOS (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, CentOS, Ubuntu o Debian (después de instalar el nodo)**: Linux: Añada tronco o interfaces de acceso a un nodo

Cree una interfaz VLAN

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso 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

1. Seleccione **CONFIGURACIÓN** > **Red** > **interfaces VLAN**.
2. Seleccione **Crear**.

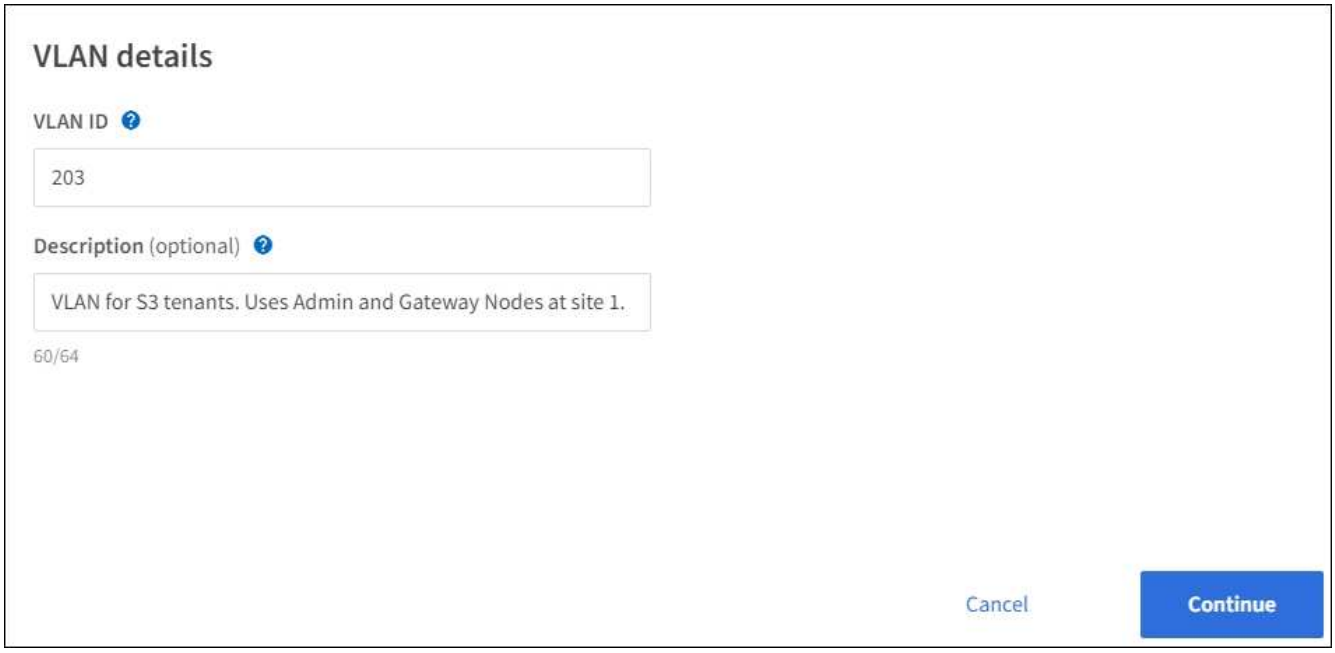
Introduzca los detalles de las interfaces de VLAN

1. Especifique el ID de la VLAN en la red. Puede introducir cualquier valor entre 1 y 4094.

   No es necesario que los ID de VLAN sean 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 VLAN con un mismo ID no pueden compartir la misma interfaz en un nodo.

   Si especifica un ID que ya se ha utilizado, aparecerá un mensaje. Puede continuar creando otra interfaz VLAN para la misma identificación de VLAN o puede seleccionar **Cancelar** y, a continuación, editar el ID existente.

2. De manera opcional, introduzca una breve descripción para la interfaz de VLAN.



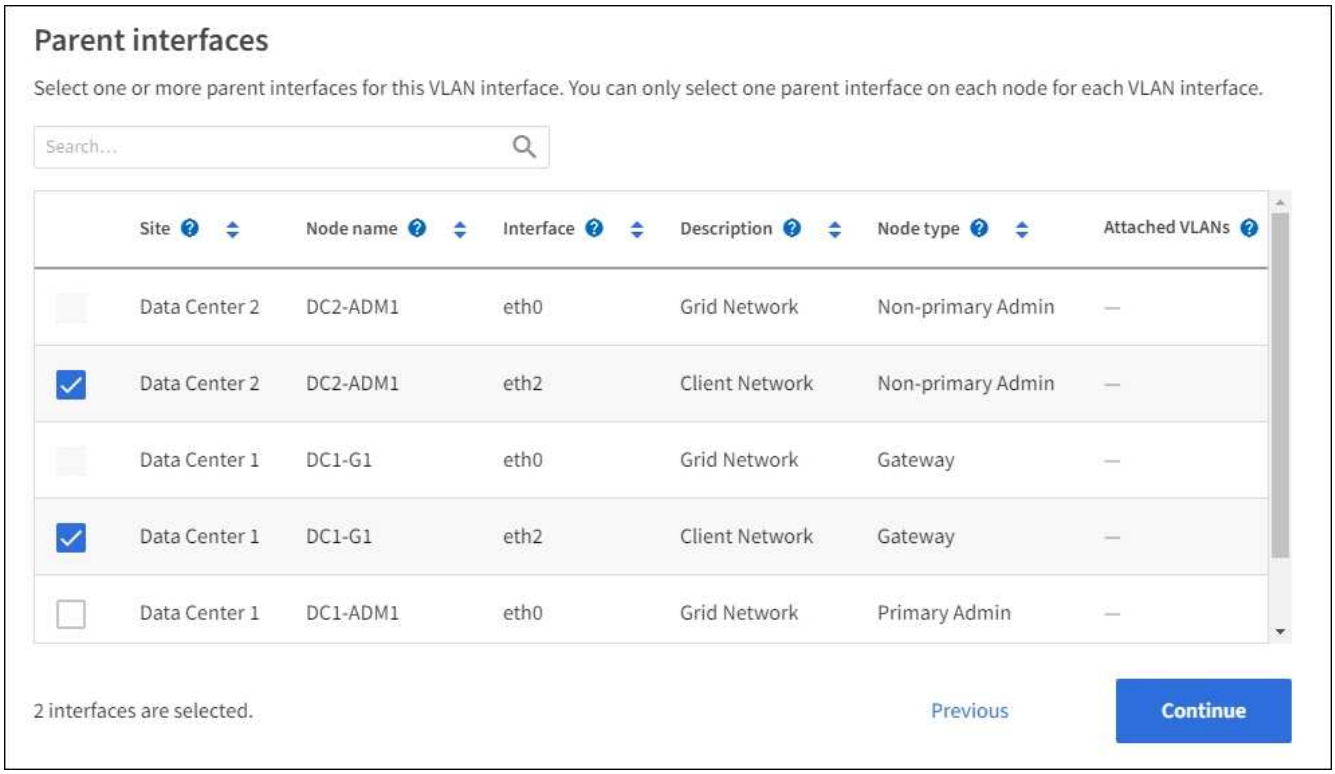
3. Seleccione **continuar**.

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 red de administración (eth1) no se pueden utilizar como interfaces principales y no se muestran.

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

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 quitar la interfaz principal sin usar para el nodo B, pero no puede quitar la interfaz principal utilizada 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 anule la selección de las casillas de verificación para agregar interfaces padre o para eliminar 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.

Gestión de 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 primaria es la interfaz "'activa'" del grupo.

Del mismo modo, durante el funcionamiento normal, cualquier interfaz con menor prioridad para el grupo ha actúa como interfaces «'backup'». Estas interfaces de backup 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

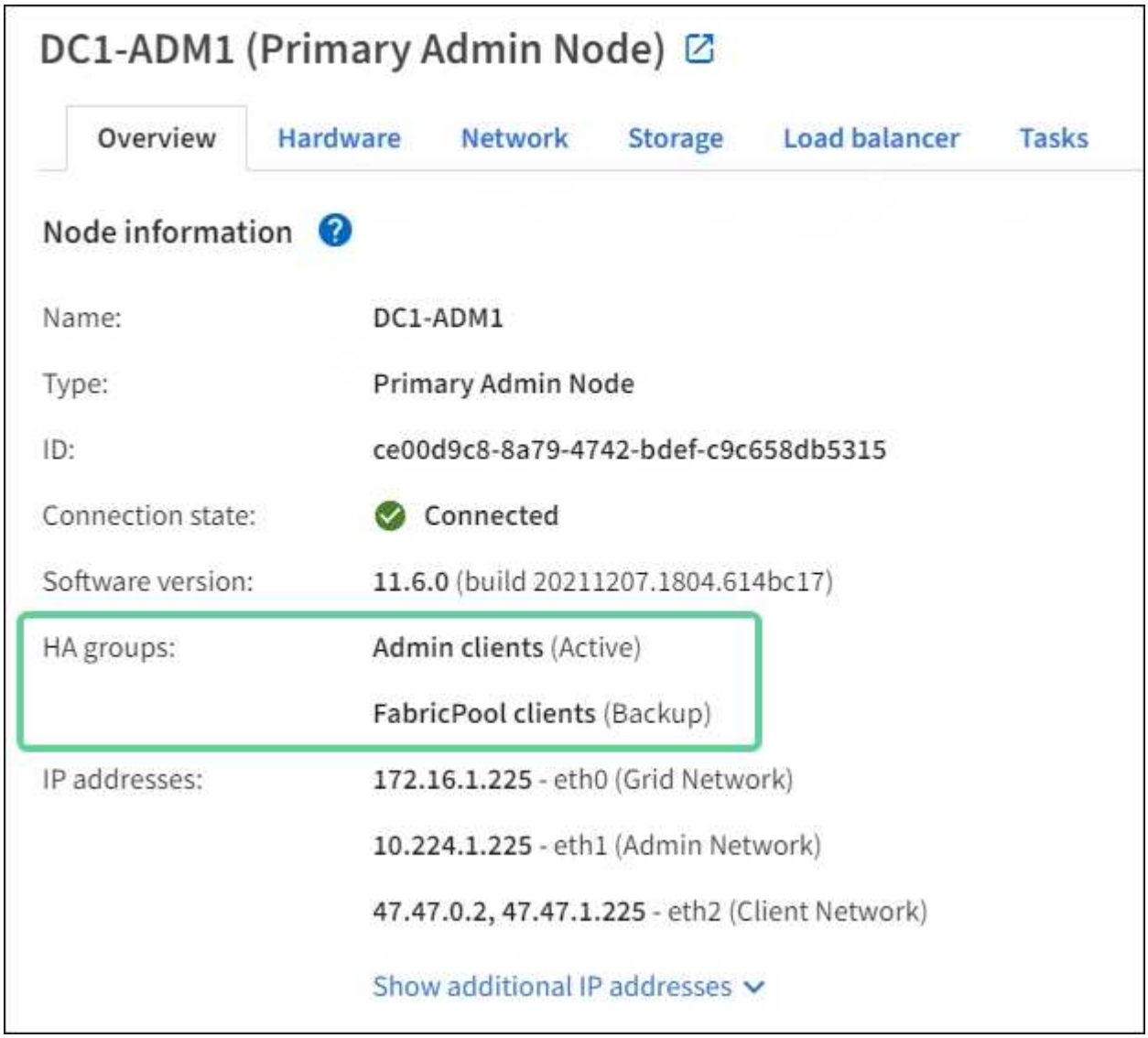
Para ver si un nodo está asignado a un grupo ha y determinar su estado actual, seleccione **NODES** > ***node***.

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 de alta disponibilidad (keepalived) se ha detenido manualmente.
- **Fallo**: El grupo ha no se puede alojar en este nodo debido a una o más de las siguientes situaciones:
  - 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, la conmutación por error no se activa con el fallo del servicio CLB (obsoleto) o los servicios para el administrador de grid o el administrador de inquilinos.

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 puerta de enlace**: Incluye el servicio Load Balancer y el servicio CLB (obsoleto).

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.
Acceso al cliente S3 o Swift: Servicio CLB **Nota:** el servicio CLB está en desuso.	• Nodos de puerta de enlace

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.

No se pueden realizar algunos procedimientos de mantenimiento cuando el nodo administrador principal no está disponible. Durante la conmutación por error, puede utilizar Grid Manager para supervisar el sistema StorageGRID.

Limitaciones del uso de grupos de alta disponibilidad con el servicio CLB

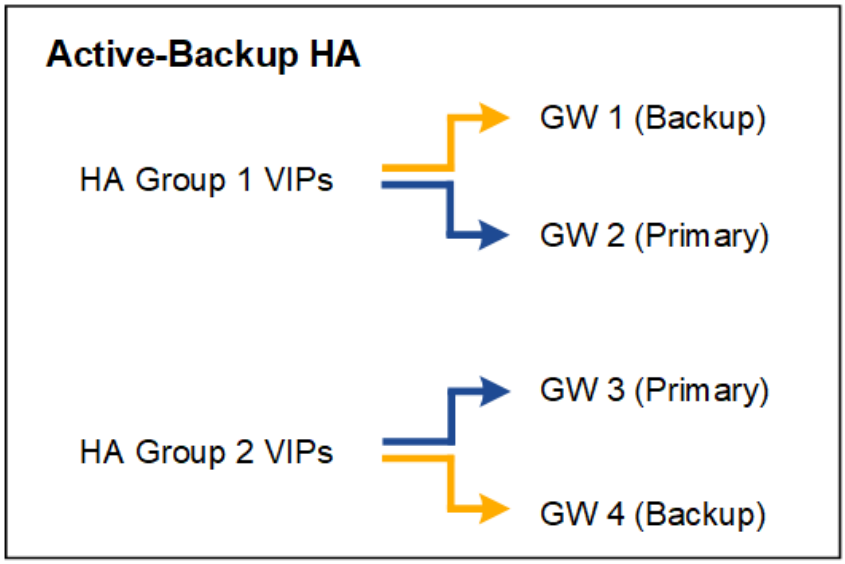
El error del servicio CLB no activa la conmutación por error dentro del grupo ha.

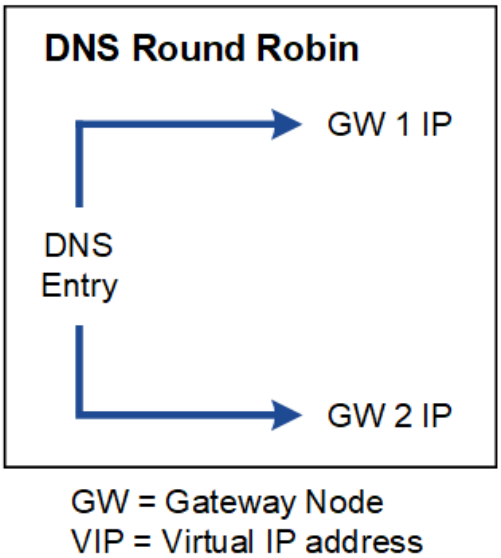
> El servicio CLB está obsoleto.

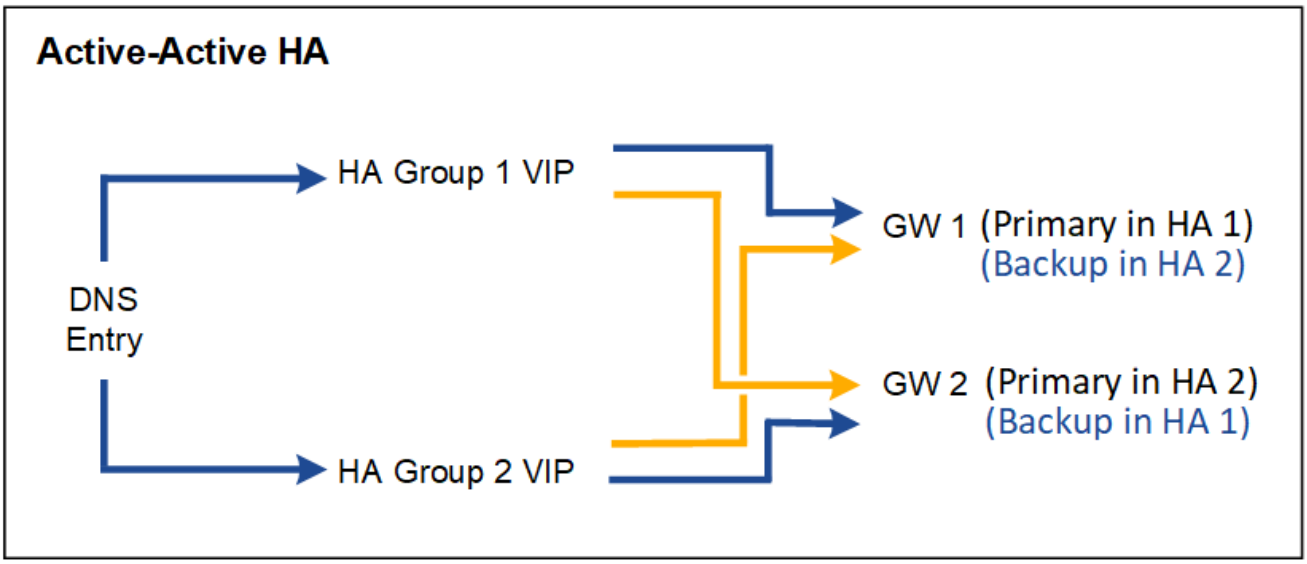
Opciones de configuración para grupos de alta disponibilidad

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.

Configuración	Ventajas	Desventajas
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.
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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso 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 o CentOS (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.

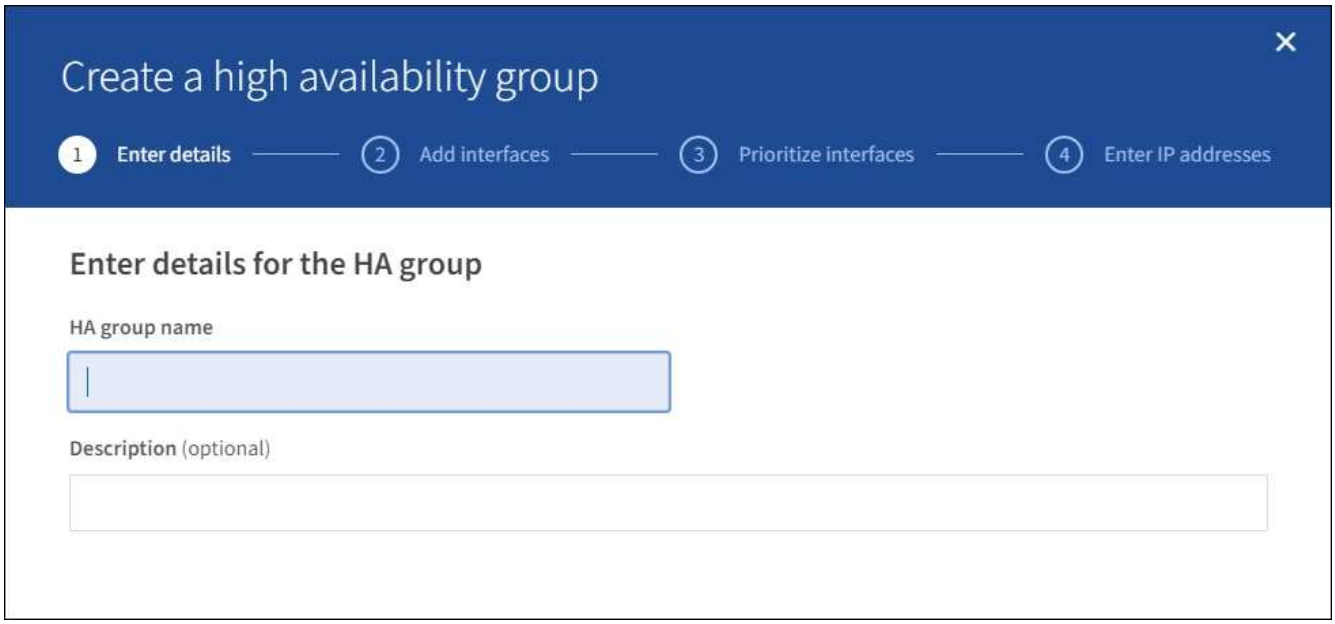
Una interfaz debe ser para que un nodo de puerta de enlace o un nodo de administrador se incluyan en un grupo de alta disponibilidad. Un grupo de alta disponibilidad solo puede usar una interfaz para cualquier nodo concreto; sin embargo, se pueden usar otras interfaces para el mismo nodo en otros grupos de alta disponibilidad.

Acceda al asistente

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
2. Seleccione **Crear**.

Introduzca los detalles del grupo de alta disponibilidad

1. Proporcione un nombre único para el grupo de alta disponibilidad.

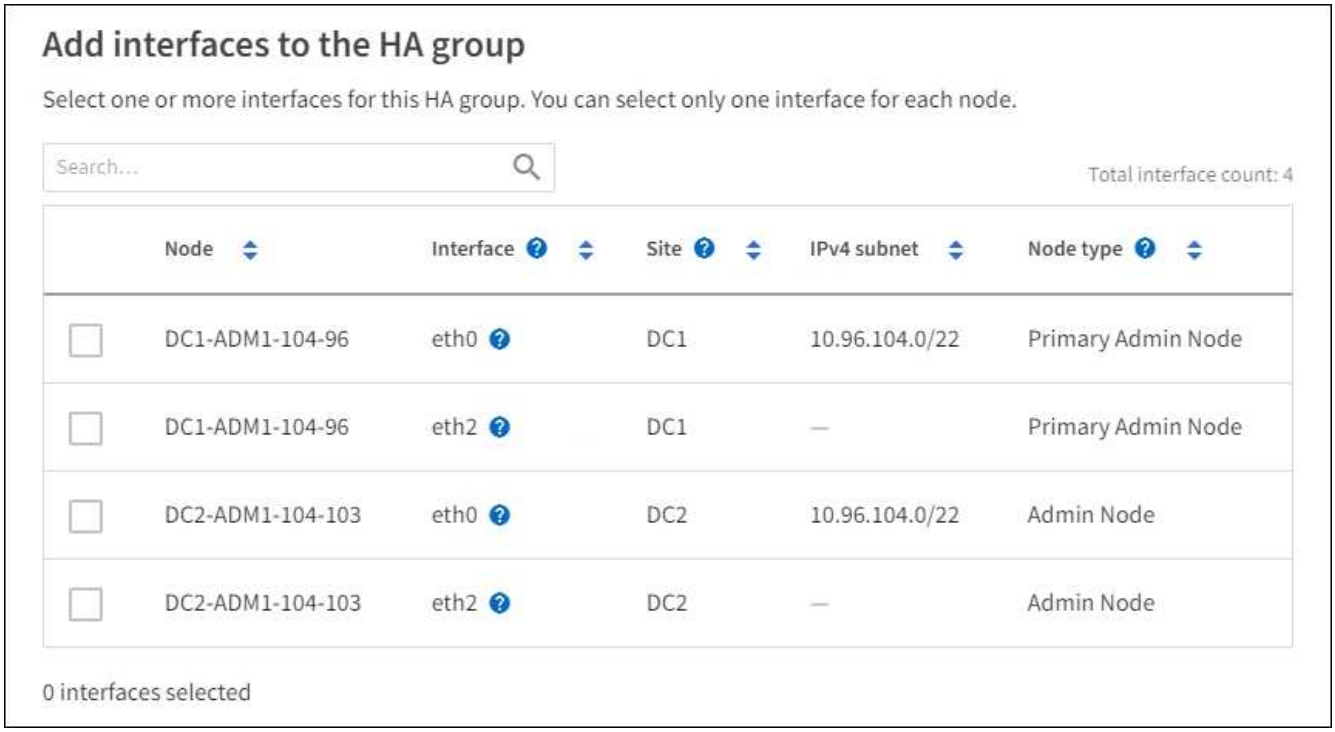


2. De forma opcional, puede introducir una descripción para el grupo de alta disponibilidad.
3. Seleccione **continuar**.

Añada interfaces al grupo de alta disponibilidad

1. Seleccione una o varias interfaces para añadirlas a este grupo de alta disponibilidad.

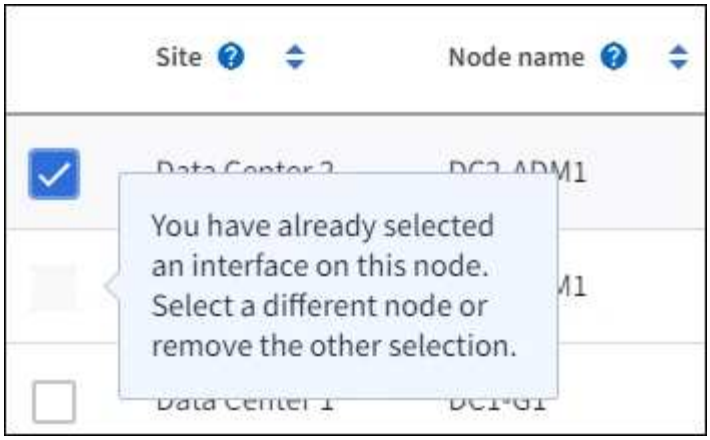
   Utilice los encabezados de columna para ordenar las filas o introduzca un término de búsqueda para localizar las interfaces más rápidamente.



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 el grupo ha es para la protección de alta disponibilidad del servicio CLB obsoleto, seleccione interfaces sólo en nodos de puerta de enlace.
- 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 respaldo no puede ofrecer protección de alta disponibilidad de los servicios de nodo de administrador. Del mismo modo, un nodo de administrador de backup no puede realizar todos los procedimientos de mantenimiento que proporciona el nodo de administración principal.
- Si no puede seleccionar una interfaz, la casilla de verificación está desactivada. La sugerencia de herramienta proporciona más información.



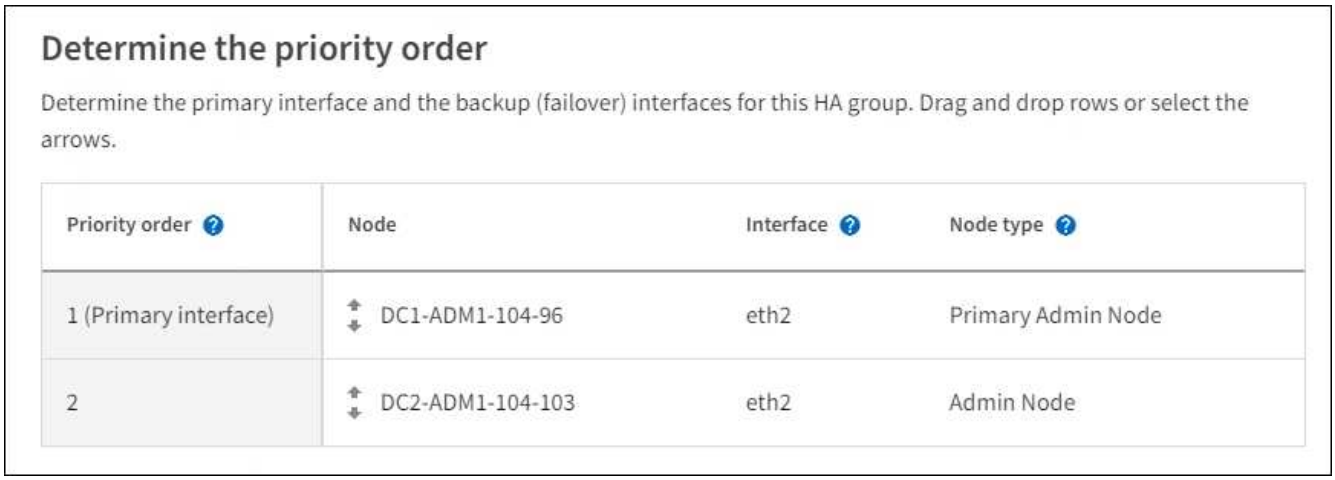
- No puede seleccionar una interfaz si su valor de subred o puerta de enlace entra en conflicto con otra interfaz seleccionada.
- No puede seleccionar una interfaz configurada si no tiene una dirección IP estática.

2. Seleccione **continuar**.

Determinar el orden de prioridad

1. Determine la interfaz principal y cualquier interfaz de backup (conmutación al nodo de respaldo) para este grupo de alta disponibilidad.

   Arrastre y suelte filas para cambiar los valores de la columna **orden de prioridad**.



> 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.

   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 incluye más de una interfaz y la interfaz principal falla, las direcciones VIP se mueven a la interfaz de mayor prioridad disponible. Si falla esa interfaz, las direcciones VIP pasan a la siguiente interfaz de mayor prioridad que esté disponible, etc.

2. Seleccione **continuar**.

Introduzca las direcciones IP

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.

   Enter details for the HA group

   Subnet CIDR

   Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

   IPv4 address followed by a slash and the subnet length (0-32)

   Gateway IP address (optional)

   Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

   Virtual IP address

   Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

   1.2.3.4

   Add another IP address

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 una o más **direcciones IP virtuales** para el grupo ha. Puede añadir hasta 10 direcciones IP. Todos los VIP deben estar dentro de la subred VIP.

   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.

> Espere hasta 15 minutos para que los cambios en un grupo de alta disponibilidad se apliquen a todos los nodos.

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

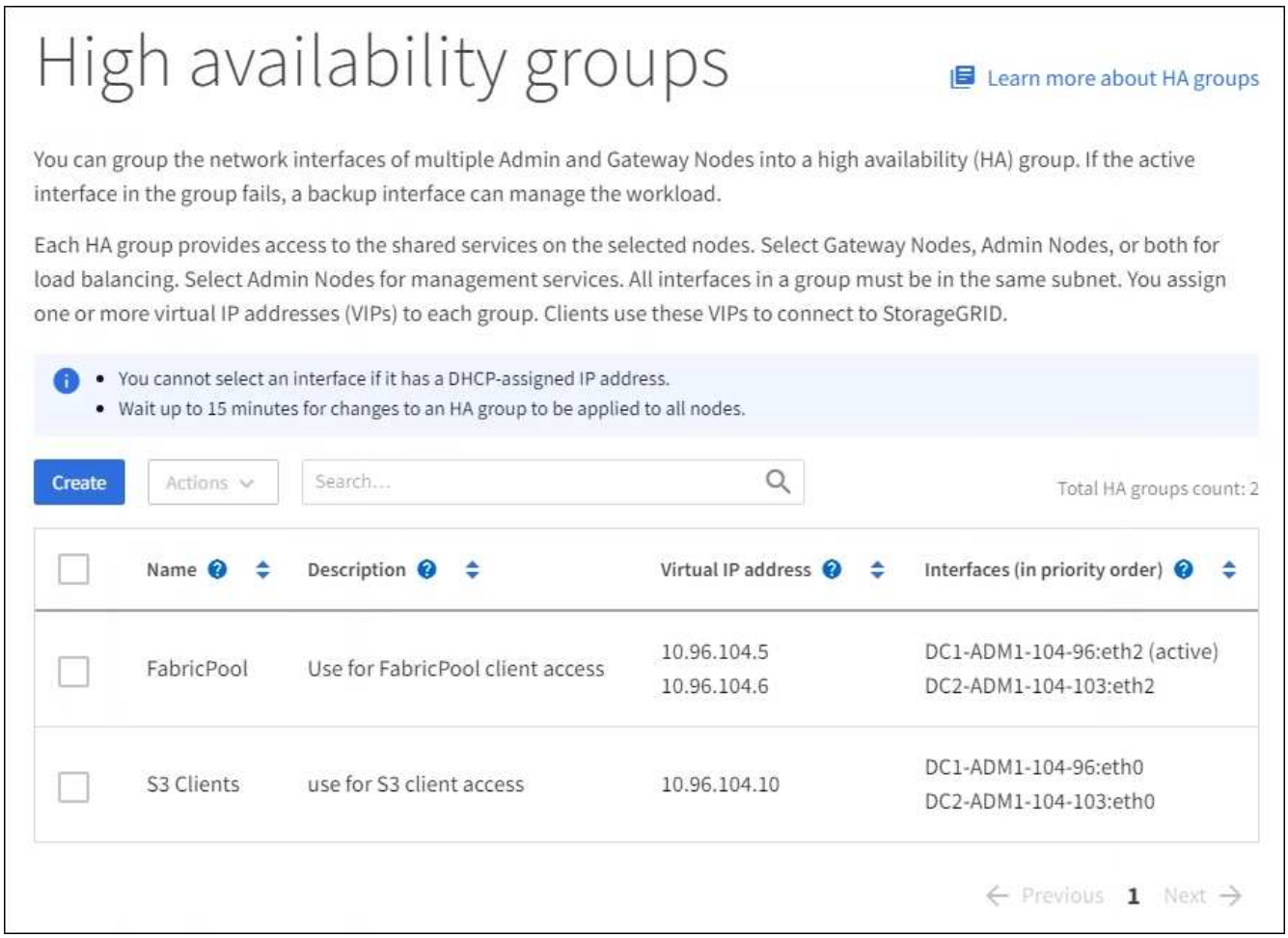
Puede editar un grupo de alta disponibilidad para cambiar su nombre y descripción, agregar o quitar interfaces, cambiar el orden de prioridad o agregar o actualizar direcciones IP virtuales.

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, active o anule la selección de las casillas de verificación para agregar o quitar 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 y suelte filas para cambiar el orden de prioridad de la interfaz primaria y cualquier interfaz de copia de seguridad de este grupo ha.
   d. De manera opcional, actualice las direcciones IP virtuales.
   e. Seleccione **Guardar** y, a continuación, seleccione **Finalizar**.

Espere hasta 15 minutos para que los cambios en un grupo de alta disponibilidad se apliquen a todos los nodos.

Eliminar un grupo de alta disponibilidad

Puede eliminar uno o varios grupos de alta disponibilidad al mismo tiempo. Sin embargo, no puede eliminar un grupo ha si está enlazado a uno o más extremos de equilibrador de carga.

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. Seleccione la casilla de comprobación de cada grupo de alta disponibilidad que desea quitar. A continuación, seleccione **acciones** > **Eliminar grupo ha**.
3. 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

Gestionar el equilibrio de carga: Descripción general

Las funciones de equilibrio de carga de StorageGRID se pueden usar para manejar cargas de trabajo de procesamiento y recuperación de los clientes S3 y Swift. El

equilibrio de carga maximiza la velocidad y la capacidad de conexión distribuyendo las cargas de trabajo y las conexiones entre varios nodos de almacenamiento.

Puede equilibrar las cargas de trabajo de clientes de las siguientes maneras:

- Use el servicio Load Balancer, que se instala en los nodos de administrador y de puerta de enlace. El servicio Load Balancer proporciona equilibrio de carga de capa 7 y realiza terminación TLS de solicitudes de cliente, inspecciona las solicitudes y establece nuevas conexiones seguras a los nodos de almacenamiento. Este es el mecanismo de equilibrio de carga recomendado.

  Consulte Cómo funciona el equilibrio de carga: Servicio de equilibrio de carga.

- Utilice el servicio de equilibrio de carga de conexión (CLB) obsoleto, que se instala sólo en nodos de puerta de enlace. El servicio CLB proporciona equilibrio de carga de capa 4 y soporta costes de enlace.

  Consulte Cómo funciona el equilibrio de carga: Servicio CLB (obsoleto).

- Integre un equilibrador de carga de terceros. Si desea obtener más información, póngase en contacto con el representante de cuenta de NetApp.

Cómo funciona el equilibrio de carga: Servicio de equilibrio de carga

El servicio Load Balancer distribuye conexiones de red entrantes desde aplicaciones cliente hasta nodos de almacenamiento. Para habilitar el equilibrio de carga, debe configurar los extremos del equilibrador de carga mediante el Administrador de grid.

Puede configurar extremos de equilibrador de carga solo para nodos de administración o nodos de puerta de enlace, ya que estos tipos de nodos contienen el servicio Load Balancer. No se pueden configurar extremos para nodos de almacenamiento ni nodos de archivado.

Cada extremo de equilibrio de carga especifica un puerto, un protocolo de red (HTTP o HTTPS), un tipo de cliente (S3 o Swift) y un modo de enlace. Los extremos HTTPS requieren un certificado de servidor. Los modos de enlace permiten restringir la accesibilidad de los puertos de extremo a:

- Las direcciones IP virtuales (VIP) de grupos específicos de alta disponibilidad (ha)
- Interfaces de red específicas de nodos Admin y Gateway específicos

Consideraciones sobre el puerto

Los clientes pueden acceder a cualquiera de los extremos que configure en cualquier nodo que ejecute el servicio Load Balancer, con dos excepciones: Los puertos 80 y 443 están reservados en nodos de administrador, de modo que los extremos configurados en estos puertos admiten operaciones de balanceo de carga solo en nodos de puerta de enlace.

Si ha reasignado algún puerto, no puede utilizar los mismos puertos para configurar los extremos de equilibrador de carga. Puede crear puntos finales mediante puertos reasignados, pero esos puntos finales se volverán a asignar a los puertos y servicios de CLB originales, no al servicio Load Balancer. Siga los pasos de Eliminar reasignaciones de puertos.

> El servicio CLB está obsoleto.

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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.
- 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. ConsulteConfigure los certificados API S3 y Swift.

    El certificado puede utilizar caracteres comodín para representar los nombres de dominio completos de todos los nodos de administración y los nodos de puerta de enlace que ejecutan el servicio Load Balancer. Por ejemplo: `*.storagegrid.`*`example`*`.com` utiliza el comodín * que se va a representar `adm1.storagegrid.`*`example`*`.com` y.. `gn1.storagegrid.`*`example`*`.com`. Consulte Configure los

nombres de dominio de extremo API de S3.

Cree un extremo de equilibrador de carga

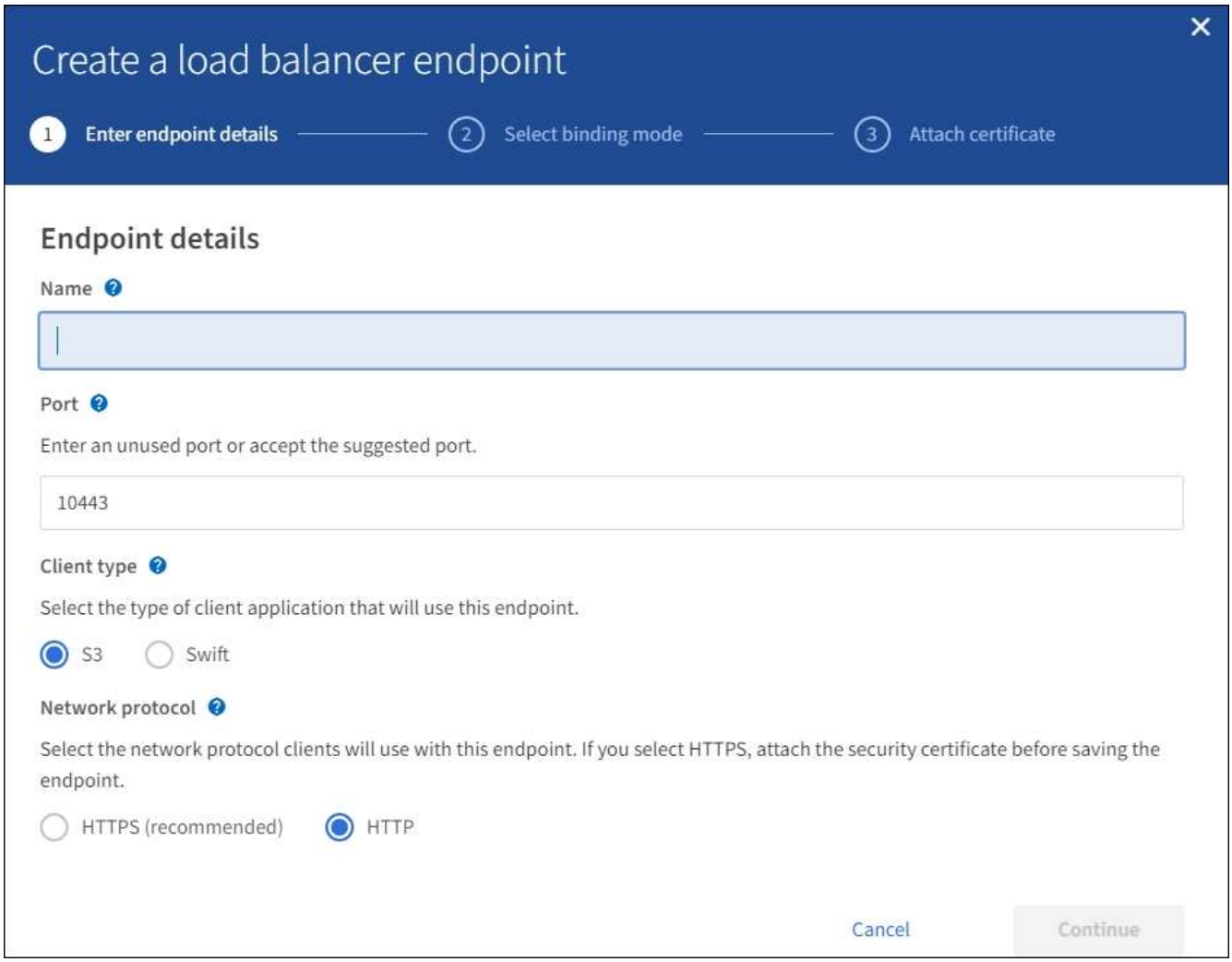
Cada extremo de equilibrio de carga especifica un puerto, un tipo de cliente (S3 o Swift) y un protocolo de red (HTTP o HTTPS).

Acceda al asistente

1. Seleccione **CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**.
2. Seleccione **Crear**.

Introduzca los detalles de los extremos

1. Introduzca los detalles del extremo.



Campo	Descripción
Nombre	Nombre descriptivo para el punto final, que aparecerá en la tabla de la página Load equilibrer Endpoints.

Campo	Descripción
Puerto	Los clientes de puertos utilizarán para conectarse al servicio Load Balancer en los nodos de administración y de puerta de enlace. Acepte el número de puerto sugerido o introduzca cualquier puerto externo que no utilice otro servicio de cuadrícula. Introduzca un valor entre 1 y 65535. Si introduce **80** o **443**, el punto final sólo se configura en los nodos de puerta de enlace. Estos puertos están reservados en los nodos de administrador. Consulte Directrices sobre redes para obtener información acerca de los puertos externos.
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.

2. Seleccione **continuar**.

Seleccione el modo de encuadernación

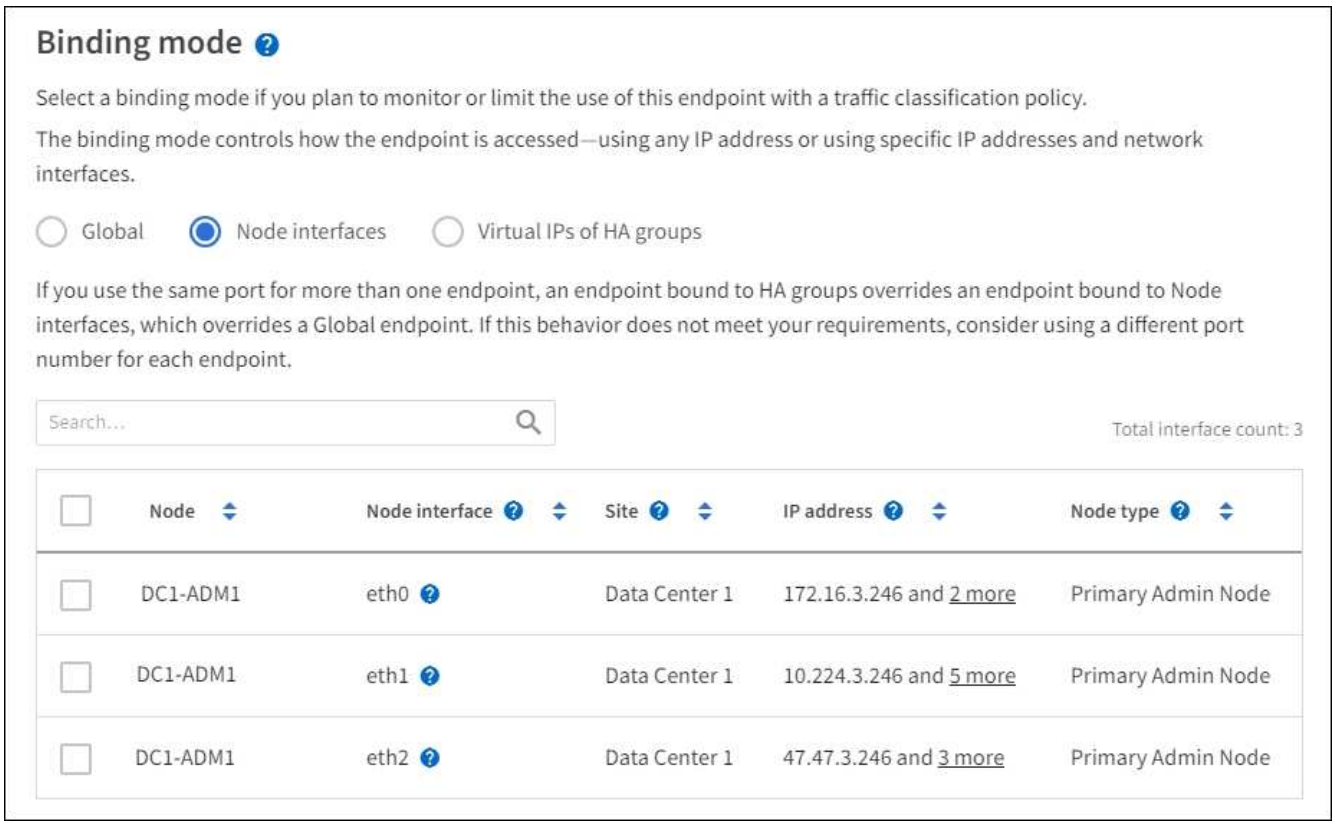
1. Seleccione un modo de enlace para que el extremo controle cómo se accede al extremo.

Opción	Descripción
Global (predeterminado)	Los clientes pueden acceder al extremo utilizando un nombre de dominio completo (FQDN), la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, o la dirección IP virtual de cualquier grupo de alta disponibilidad de cualquier red. Utilice el ajuste **Global** (predeterminado) a menos que necesite restringir la accesibilidad de este extremo.
Interfaces de nodos	Los clientes deben usar la dirección IP de un nodo e interfaz de red seleccionados para acceder a este extremo.

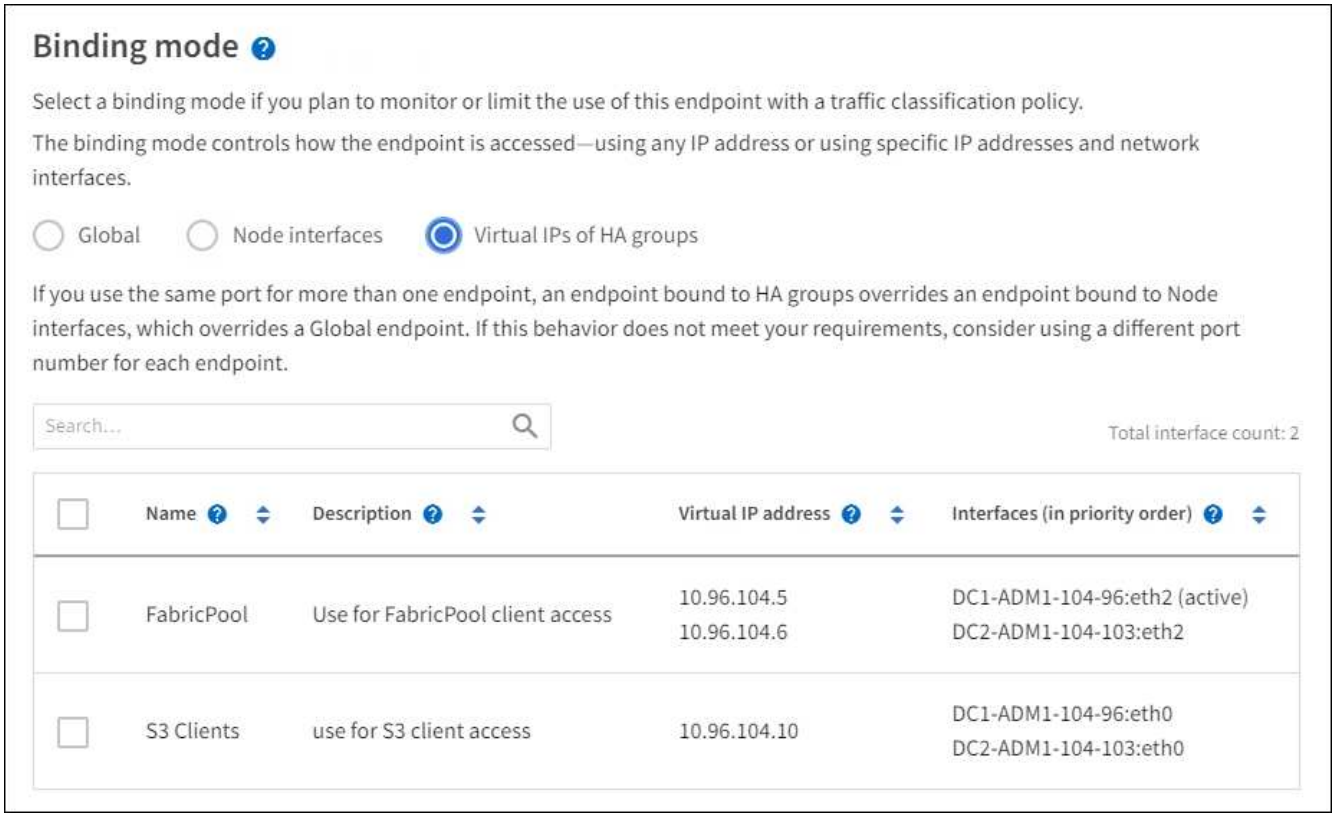
Opción	Descripción
IP virtuales de grupos de alta disponibilidad	Los clientes deben utilizar una dirección IP virtual de un grupo de alta disponibilidad para acceder a este extremo. Los extremos con este modo de enlace pueden usar el mismo número de puerto, siempre que los grupos de alta disponibilidad que seleccione para los extremos no se superpongan. Los extremos con este modo pueden usar el mismo número de puerto siempre que las interfaces que seleccione para los extremos no se superpongan.

Si utiliza el mismo puerto para más de un extremo, un punto final que utiliza el modo **IP virtuales de grupos de alta disponibilidad** anula un punto final utilizando el modo **interfaces de nodo**, que anula un punto final utilizando el modo **Global**.

2. 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.



3. Si ha seleccionado **IP virtuales de grupos ha**, seleccione uno o más grupos ha.



4. Si está creando un extremo **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

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 API predeterminado S3 y Swift, que está firmado por la CA de grid, con un certificado personalizado firmado por una entidad de certificación externa. ConsulteConfigure los certificados API S3 y Swift.

2. Si no utiliza el certificado 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 usa en todas las conexiones nuevas posteriores entre los clientes de S3 y Swift y el extremo.

Generar certificado

a. Seleccione **generar certificado**.

b. Especifique la información del certificado:

- **Nombre de dominio**: Uno o más nombres de dominio completamente cualificados que se incluirán en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
- **IP**: Una o varias direcciones IP que se incluirán en el certificado.
- **Asunto**: X.509 asunto o nombre distinguido (DN) del propietario del certificado.
- **Días válidos**: Número de días después de la creación que expira el certificado.

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 usa para todas las conexiones nuevas posteriores entre los clientes de S3 y Swift y este extremo.

[[después de terminar]]después de terminar

1. Si utiliza un sistema de nombres de dominio (DNS), asegúrese de que el DNS incluye un registro para asociar el nombre de dominio completo 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 de alta disponibilidad, los clientes se conectarán al servicio de equilibrador de carga de StorageGRID mediante la dirección IP de cualquier 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.

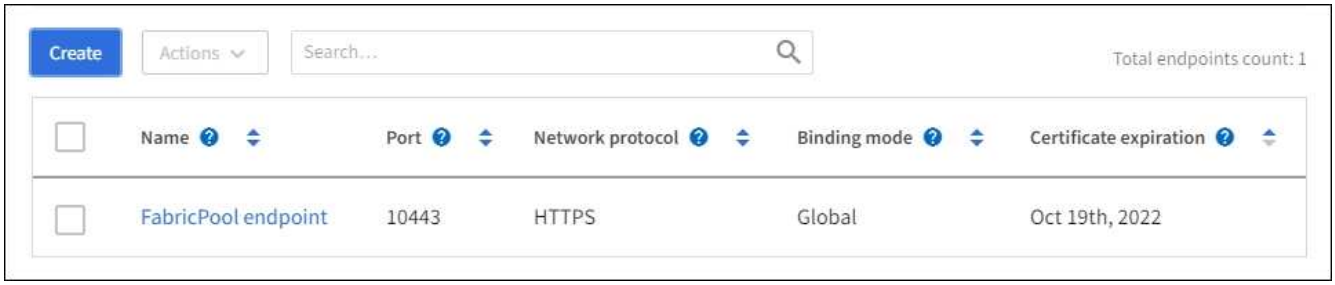
2. Proporcione a los clientes S3 y Swift la información necesaria para conectarse al extremo:
   - Número de puerto
   - Nombre de dominio o dirección IP completos
   - Los detalles de certificado necesarios

Ver y editar puntos finales del equilibrador de carga

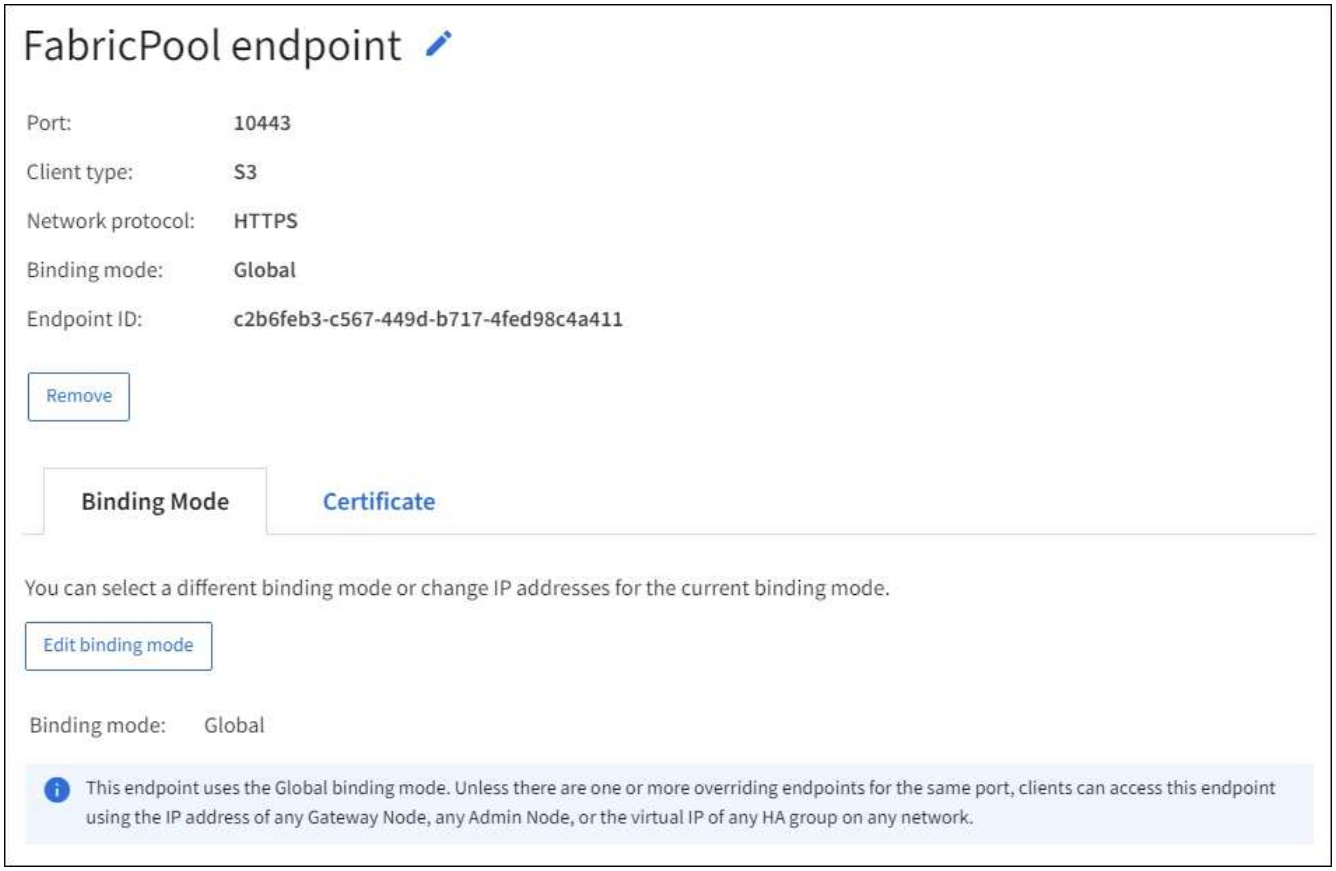
Puede ver detalles de los extremos de equilibrador de carga existentes, incluidos los metadatos de certificado para un extremo protegido. También puede cambiar el nombre de un extremo o el modo de enlace y actualizar los certificados asociados.

No puede cambiar el tipo de servicio (S3 o Swift), el puerto o el protocolo (HTTP o HTTPS).

- Para ver información básica de todos los puntos finales del equilibrador de carga, revise la tabla de la página puntos finales del 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.



- Para editar un punto final, utilice el menú **acciones** de la página puntos finales del equilibrador de carga o la página de detalles de un punto final específico.

> 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 del extremo. 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**.

Tarea	Menú Actions	Detalles
Edite el modo de enlace de punto final	a. Seleccione la casilla de verificación del extremo. 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 del extremo. 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**.

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.

- Para eliminar uno o varios puntos finales:
  a. En la página Load Balancing, seleccione la casilla de verificación de cada extremo que desee quitar.
  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**.

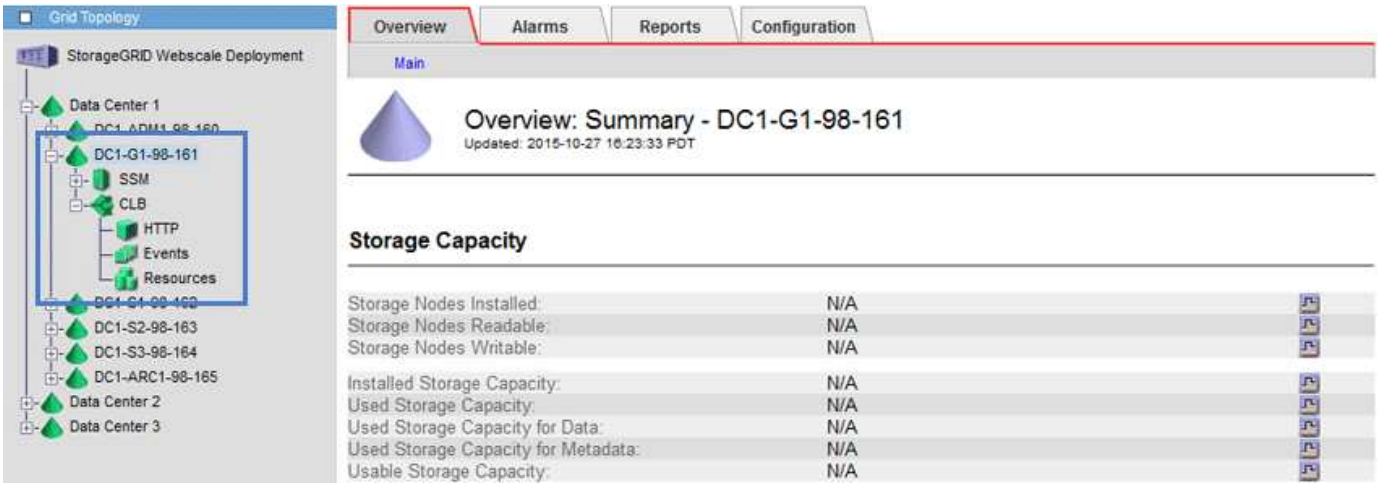
Cómo funciona el equilibrio de carga: Servicio CLB (obsoleto)

El servicio Connection Load Balancer (CLB) en los nodos de Gateway queda obsoleto. El servicio Load Balancer es ahora el mecanismo de equilibrio de carga recomendado.

El servicio CLB utiliza el equilibrio de carga de capa 4 para distribuir las conexiones de red TCP entrantes de

las aplicaciones cliente al nodo de almacenamiento óptimo en función de la disponibilidad, la carga del sistema y el coste de enlace configurado por el administrador. Cuando se elige el nodo de almacenamiento óptimo, el servicio CLB establece una conexión de red bidireccional y reenvía el tráfico hacia y desde el nodo elegido. El CLB no considera la configuración de red de red de cuadrícula al dirigir las conexiones de red entrantes.

Para ver información sobre el servicio CLB, seleccione **SUPPORT** > **Tools** > **Grid topolog** y, a continuación, expanda un nodo Gateway hasta que pueda seleccionar **CLB** y las opciones que aparecen a continuación.



Si decide utilizar el servicio CLB, debe considerar la configuración de los costes de enlace para su sistema StorageGRID.

- ¿Cuáles son los costes de enlace
- Actualizar costes de enlace

Configure los nombres de dominio de extremo API de S3

Para admitir solicitudes de estilo alojado virtuales S3, debe usar Grid Manager para configurar la lista de nombres de dominio de extremo a los que se conectan los clientes S3.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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 se esté realizando una actualización de la cuadrícula.

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 utiliza el cliente para las conexiones HTTPS a StorageGRID esté firmado para todos los nombres de dominio que el cliente necesita.

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 utilizan los clientes para realizar conexiones y asegúrese de que los registros hagan referencia a todos los nombres de dominio de extremo requeridos, incluidos los nombres de 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.

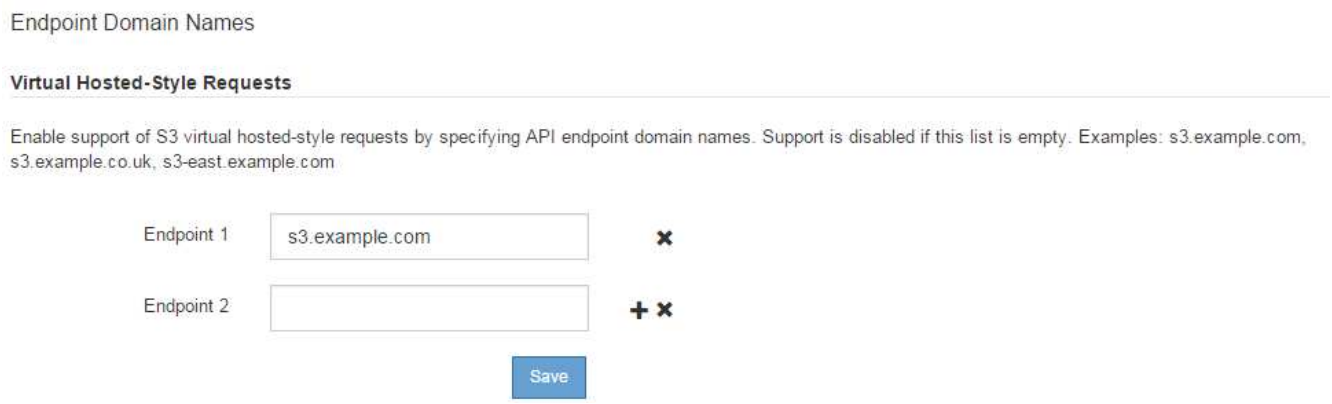
Los clientes que usan conexiones HTTPS (recomendadas) a la cuadrícula pueden usar cualquiera de los siguientes certificados:

- Los clientes que se conectan a un extremo de equilibrador de carga pueden utilizar un certificado personalizado para ese extremo. Cada punto final de equilibrador de carga se puede configurar para reconocer diferentes nombres de dominio de punto final.
- Los clientes que se conectan a un extremo de equilibrio de carga, directamente a un nodo de almacenamiento o directamente al servicio CLB obsoleto en un nodo de puerta de enlace pueden personalizar el certificado de API S3 y Swift global para incluir todos los nombres de dominio de extremo necesarios.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **nombres de dominio**.

   Aparece la página Endpoint Domain Names.



2. Introduzca la lista de nombres de dominio de extremo de API de S3 en los campos **Endpoint**. Utilice la ➕ con el icono para añadir campos adicionales.

   Si esta lista está vacía, se deshabilita la compatibilidad con las solicitudes de estilo alojado virtuales de S3.

3. Seleccione **Guardar**.
4. Asegúrese de que los certificados de servidor que utilizan los clientes coinciden con los nombres de dominio de extremo requeridos.
   - Si los clientes se conectan a un extremo de equilibrador de carga que utiliza su propio certificado,

actualice el certificado asociado al extremo.

- Si los clientes se conectan a un extremo de equilibrio de carga que usa el certificado de API global S3 y Swift, directamente en los nodos de almacenamiento o al servicio CLB en los nodos de puerta de enlace, actualice el certificado de la 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.

Información relacionada

- Use S3
- Ver direcciones IP
- Configuración de grupos de alta disponibilidad
- Configure los certificados API S3 y Swift
- Configurar puntos finales del equilibrador de carga

Habilite HTTP para las comunicaciones del cliente

De forma predeterminada, las aplicaciones cliente utilizan el protocolo de red HTTPS para todas las conexiones a nodos de almacenamiento o al servicio CLB obsoleto en nodos de puerta de enlace. Puede habilitar HTTP opcionalmente para estas conexiones, por ejemplo, al probar una cuadrícula que no sea de producción.

Lo que necesitará

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

Acerca de esta tarea

Complete esta tarea solo si los clientes S3 y Swift necesitan realizar conexiones HTTP directamente a los nodos de almacenamiento o al servicio CLB obsoleto en los nodos de puerta de enlace.

No es necesario completar esta tarea para clientes que solo utilizan conexiones HTTPS o para clientes que se conectan al servicio Load Balancer (ya que puede configurar cada extremo de Load Balancer para usar HTTP o HTTPS). Consulte la información sobre la configuración de puntos finales del equilibrador de carga para obtener más información.

Consulte Resumen: Direcciones IP y puertos para conexiones cliente Para conocer los puertos que utilizan los clientes S3 y Swift al conectarse a los nodos de almacenamiento o al servicio CLB obsoleto a través de HTTP o HTTPS

> Tenga cuidado al habilitar HTTP para una cuadrícula de producción porque las solicitudes se enviarán sin cifrar.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de red , active la casilla de verificación **Activar conexión HTTP** .

3. Seleccione **Guardar**.

Información relacionada

- Configurar puntos finales del equilibrador de carga
- Use S3
- Use Swift

Controlar qué operaciones de cliente están permitidas

Puede seleccionar la opción de cuadrícula evitar modificación de cliente para denegar operaciones específicas de cliente HTTP.

Lo que necesitará

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

Acerca de esta tarea

Evitar modificación de cliente es un valor para todo el sistema. Cuando se selecciona la opción impedir modificación de cliente, se deniegan las siguientes solicitudes:

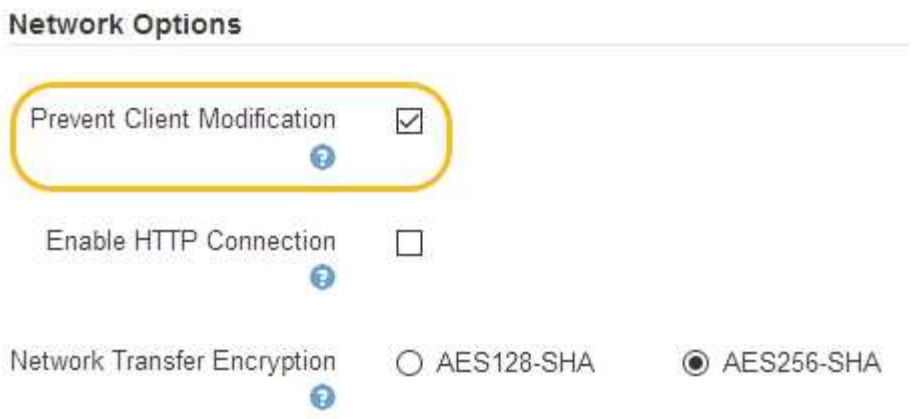
- **API REST S3**
  - Eliminar solicitudes de bloques
  - Cualquier solicitud para modificar los datos de un objeto existente, los metadatos definidos por el usuario o el etiquetado de objetos S3

> Este ajuste no se aplica a bloques con versiones habilitadas. El control de versiones ya evita modificaciones en los datos de objetos, los metadatos definidos por el usuario y el etiquetado de objetos.

- **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.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de red, active la casilla de verificación **evitar modificación de cliente**.



3. Seleccione **Guardar**.

Administrar redes y conexiones

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 de grid StorageGRID requiere una interfaz de red dedicada, una dirección IP, una máscara de

subred y una puerta de enlace para cada red a la que está asignado.

- 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 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
- **RHEL o CentOS (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, CentOS, 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. A continuación, puede usar esta dirección IP para iniciar sesión en el nodo de grid en la línea de comandos y realizar varios procedimientos de mantenimiento.

Lo que necesitará

Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

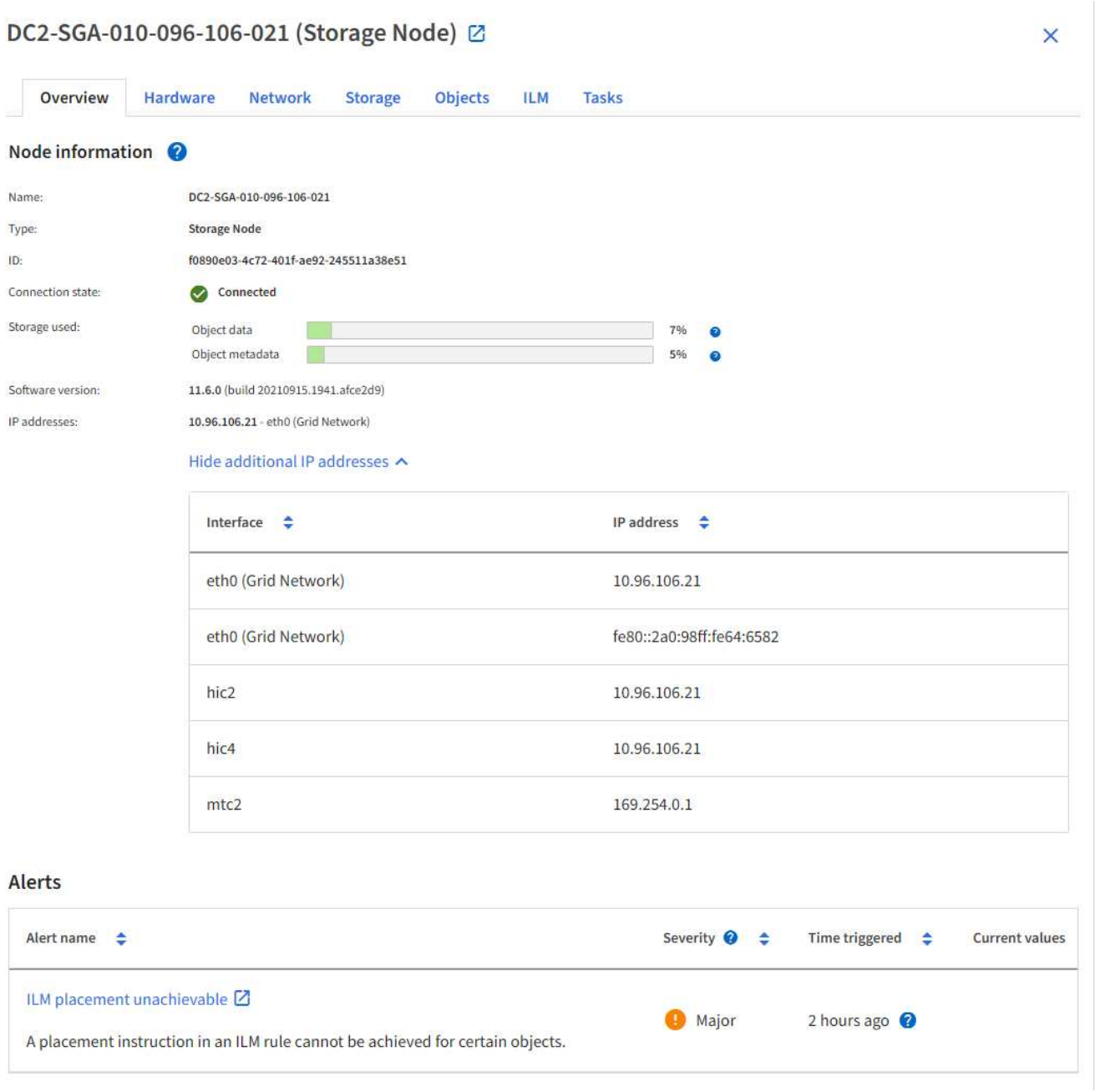
Acerca de esta tarea

Para obtener información acerca del cambio de direcciones IP, consulte Recuperación y mantenimiento.

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.



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.

> Las opciones de configuración de TLS, como las versiones del protocolo, 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.

Paquetes de cifrado TLS 1.2 admitidos

Se admiten los siguientes conjuntos de cifrado TLS 1.2:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Paquetes de cifrado TLS 1.3 admitidos

Se admiten los siguientes conjuntos de cifrado TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Cambie el cifrado de transferencia de red

El sistema StorageGRID utiliza Seguridad de la capa de transporte (TLS) para proteger el tráfico de control interno entre los nodos de la cuadrícula. La opción Network Transfer Encryption (cifrado de transferencia de red) establece el algoritmo utilizado por TLS para cifrar el tráfico de control entre los nodos de la cuadrícula. Esta configuración no afecta al cifrado de datos.

Lo que necesitará

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

Acerca de esta tarea

De forma predeterminada, el cifrado de transferencia de red utiliza el algoritmo AES256-SHA. El tráfico de control también se puede cifrar utilizando el algoritmo AES128-SHA.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de red, cambie el cifrado de transferencia de red a **AES128-SHA** o **AES256-SHA** (predeterminado).

3. Seleccione **Guardar**.

Administrar directivas de clasificación de tráfico

Administrar directivas de clasificación de tráfico

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
- Clientes
- Subredes (subredes IPv4 que contienen al cliente)
- Puntos finales (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 establecer límites para una directiva en función de los siguientes parámetros:

- Ancho de banda del agregado en

- Ancho de banda del agregado agotado
- Solicitudes de lectura simultáneas
- Solicitudes de escritura simultáneas
- Ancho de banda por solicitud en
- Ancho de banda por solicitud agotado
- Tasa de solicitud de lectura
- Tasa de solicitudes de escritura

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, 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. 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.

Los límites de clasificación del tráfico se implementan por 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.

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	Rendimiento	Coste
Oro	1 PB de almacenamiento permitido	Regla de 3 copia de ILM	25 000 solicitudes/s Ancho de banda de 5 GB/s (40 Gbps)	por mes

Nivel de servicio	Capacidad	Protección de datos	Rendimiento	Coste
Plata	Capacidad de almacenamiento de 250 TB	2 regla de copia de ILM	10 000 solicitudes/s Ancho de banda de 1.25 GB/s (10 Gbps)	$$ al mes
Bronce	Capacidad de almacenamiento de 100 TB	2 regla de copia de ILM	5 000 solicitudes/s Ancho de banda de 1 GB/s (8 Gbps)	$ al mes

Cree directivas de clasificación de tráfico

Cree políticas de clasificación de tráfico si desea supervisar y, opcionalmente, limitar el tráfico de red por bloque, inquilino, subred IP o extremo de equilibrador de carga. 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.

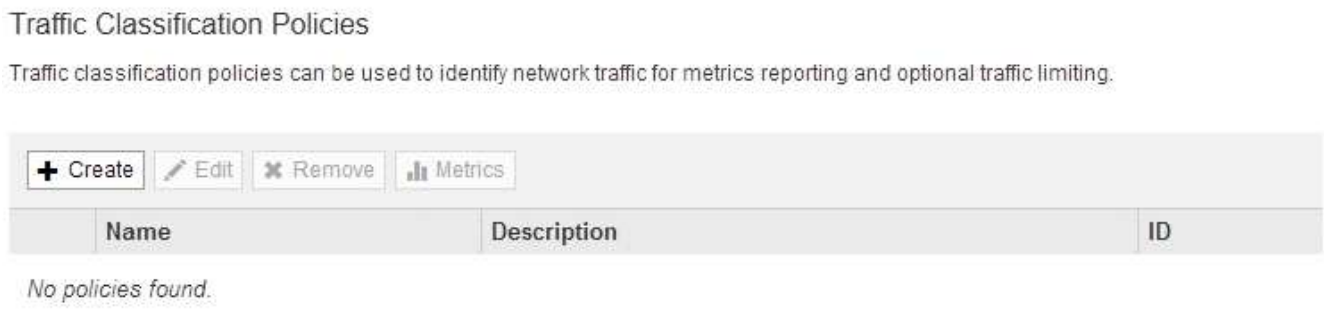
Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.
- Ha creado cualquier punto final de equilibrador de carga que desee que coincida.
- Ha creado los inquilinos que desea que coincidan.

Pasos

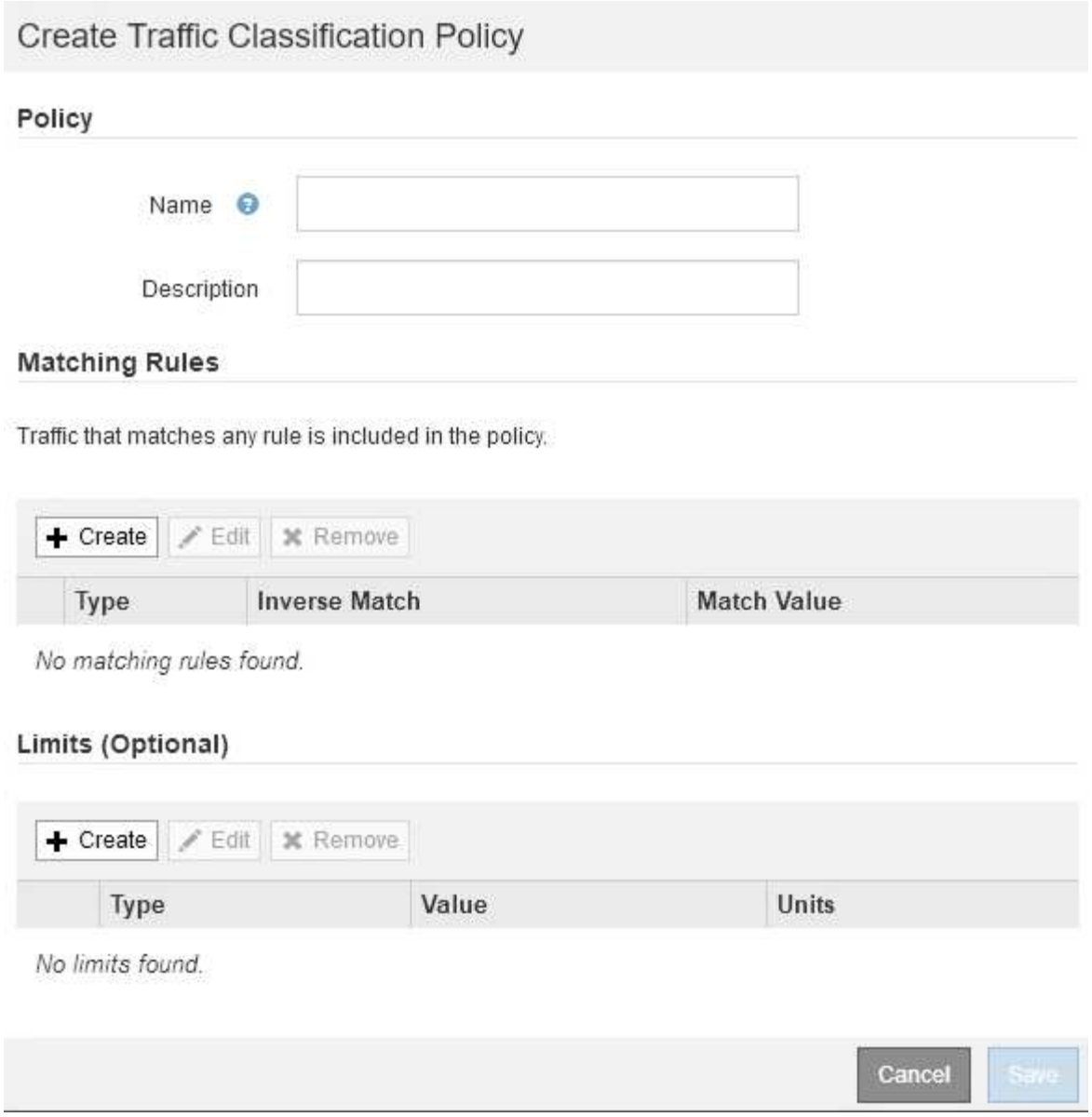
1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.

   Aparece la página Directivas de clasificación del tráfico.

2. Seleccione **Crear**.

   Aparece el cuadro de diálogo Crear directiva de clasificación de tráfico.



3. En el campo **Nombre**, escriba un nombre para la directiva.

   Introduzca un nombre descriptivo para poder reconocer la política.

4. Opcionalmente, agregue una descripción para la directiva en el campo **Descripción**.

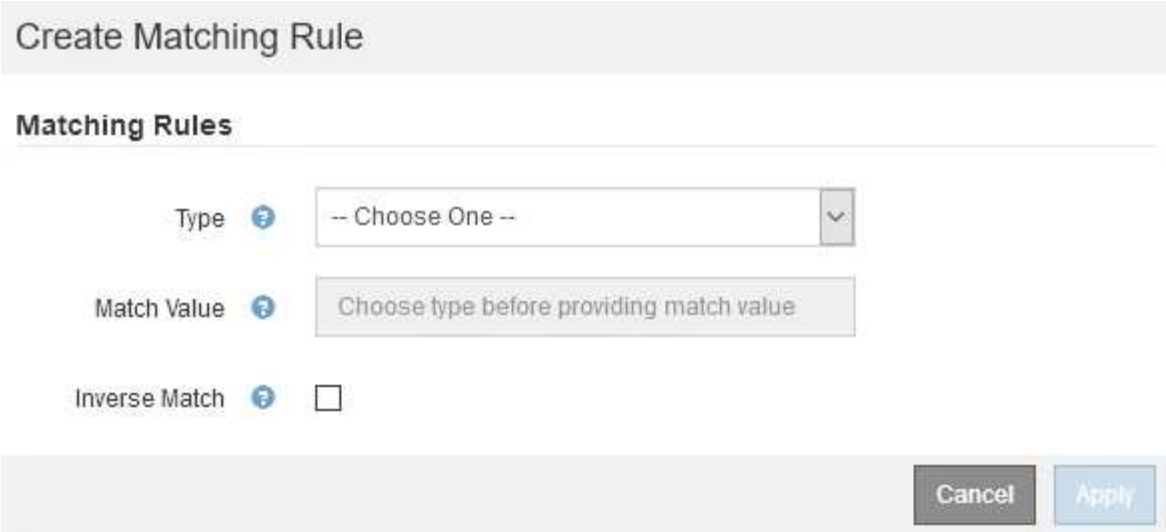
   Por ejemplo, describa a qué se aplica esta política de clasificación del tráfico y a qué se limitará.

5. Cree una o varias reglas coincidentes para la política.

   Las reglas coincidentes controlan qué entidades se verán afectadas por esta directiva de clasificación de tráfico. Por ejemplo, seleccione arrendatario si desea que esta directiva se aplique al tráfico de red de un arrendatario específico. O seleccione Endpoint si desea que esta directiva se aplique al tráfico de red en un extremo de equilibrio de carga específico.

   a. Seleccione **Crear** en la sección **Reglas coincidentes**.

      Aparece el cuadro de diálogo Crear regla de coincidencia.



b. En la lista desplegable **Tipo**, seleccione el tipo de entidad que se incluirá en la regla de coincidencia.

c. En el campo **valor de coincidencia**, escriba un valor de coincidencia basado en el tipo de entidad elegido.

   - Bucket: Introduzca un nombre de bloque.
   - Bucket Regex: Introduzca una expresión regular que se utilizará para coincidir con un conjunto de nombres de bloques.

     La expresión regular no está anclada. Utilice el delimitador ^ para que coincida al principio del nombre del bloque y utilice el delimitador $ para que coincida al final del nombre.

   - CIDR: Introduzca una subred IPv4, en notación CIDR, que coincida con la subred deseada.
   - Extremo: Seleccione un extremo de la lista de extremos existentes. Estos son los puntos finales de equilibrador de carga definidos en la página de extremos de equilibrador de carga. Consulte Configurar puntos finales del equilibrador de carga.
   - Inquilino: Seleccione un inquilino de la lista de arrendatarios existentes. La coincidencia de inquilinos se basa en la propiedad del bloque al que se va a acceder. El acceso anónimo a un bloque coincide con el inquilino al que pertenece el bloque.

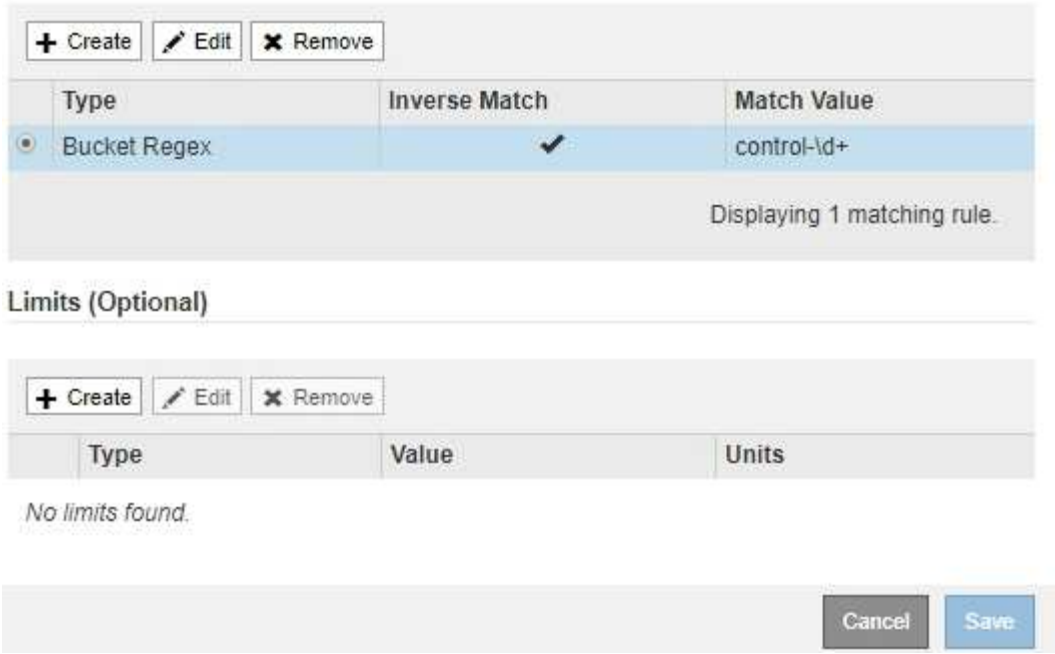
d. Si desea hacer coincidir todo el tráfico de red *excepto* que sea coherente con el valor Type and Match que acaba de definir, active la casilla de verificación **Inverse** . De lo contrario, deje la casilla de verificación sin seleccionar.

   Por ejemplo, si desea que esta directiva se aplique a todos los puntos finales del equilibrador de carga excepto uno, especifique el punto final del equilibrador de carga que se excluirá y seleccione **Inverse**.

   > 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.

e. Seleccione **aplicar**.

   La regla se crea y se muestra en la tabla Reglas coincidentes.



a. Repita estos pasos para cada regla que desee crear para la política.

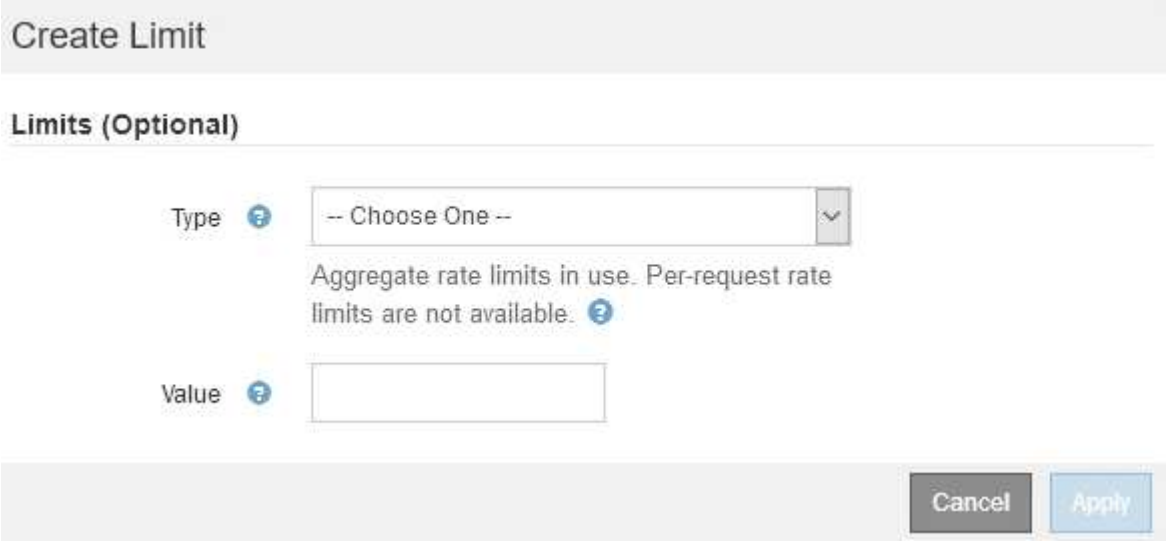
> El tráfico que coincide con cualquier regla se gestiona mediante la directiva.

6. De manera opcional, crear límites para la política.

> Aunque no cree límites, StorageGRID recopila métricas para poder supervisar el tráfico de red que se ajuste a la directiva.

a. Seleccione **Crear** en la sección **límites**.

   Se muestra el cuadro de diálogo Crear límite.



b. En el menú desplegable **Tipo**, seleccione el tipo de límite que desea aplicar a la directiva.

   En la siguiente lista, **in** hace referencia al tráfico de clientes S3 o Swift en el equilibrador de carga StorageGRID, y **OUT** hace referencia al tráfico desde el equilibrador de carga a clientes S3 o Swift.

- Ancho de banda del agregado en
- Ancho de banda del agregado agotado
- Solicitudes de lectura simultáneas
- Solicitudes de escritura simultáneas
- Ancho de banda por solicitud en
- Ancho de banda por solicitud agotado
- Tasa de solicitud de lectura
- Tasa de solicitudes de escritura

> Puede crear políticas para limitar el ancho de banda agregado o para limitar el ancho de banda por solicitud. Sin embargo, 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 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 implementa coincidencias «mejores» para límites de ancho de banda en el siguiente orden:

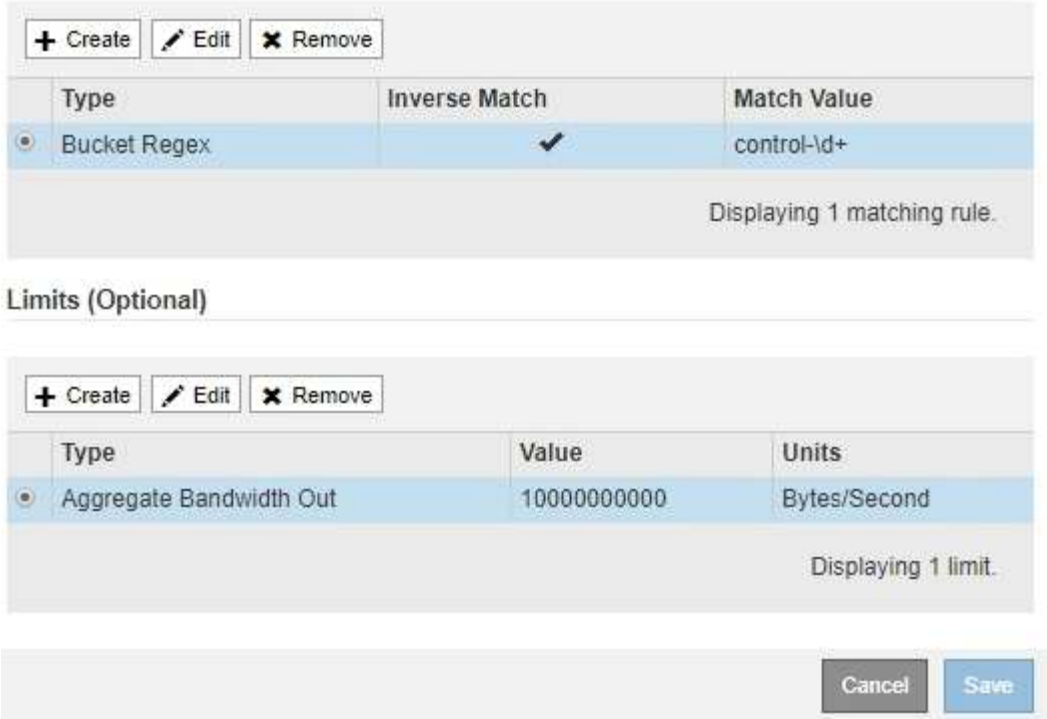
- Dirección IP exacta (/máscara 32)
- Nombre exacto del cucharón
- Regex. Cucharón
- Inquilino
- Extremo
- Coincidencias CIDR no exactas (no /32)
- Coincidencias inversas

c. En el campo **valor**, introduzca un valor numérico para el tipo de límite elegido.

   Las unidades esperadas se muestran cuando se selecciona un límite.

d. Seleccione **aplicar**.

   El límite se crea y se muestra en la tabla límites.



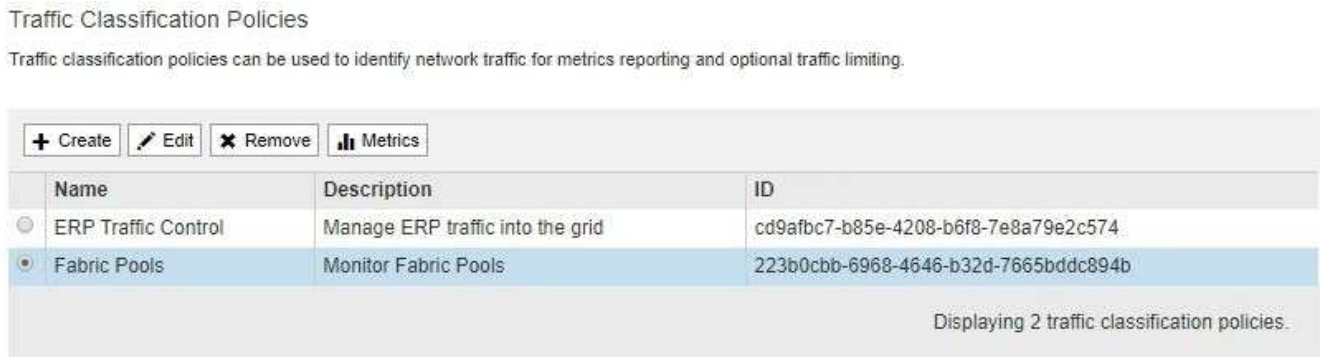
e. Repita estos pasos para cada límite que desee agregar a la directiva.

   Por ejemplo, si desea crear un límite de ancho de banda de 40 Gbps para un nivel de acuerdo de nivel de servicio, cree un límite de ancho de banda del agregado en el límite y un límite de ancho de banda de agregado en y establezca cada uno de entre 1 y 40 Gbps.

   > Para convertir megabytes por segundo a gigabits por segundo, multiplique por ocho. Por ejemplo, 125 MB/s equivale a 1,000 Mbps o 1 Gbps.

7. Cuando termine de crear reglas y límites, seleccione **Guardar**.

   La directiva se guarda y se muestra en la tabla Directivas de clasificación del tráfico.



   El tráfico del cliente S3 y Swift ahora se gestiona de acuerdo con las políticas de clasificación del tráfico. Puede ver los gráficos de tráfico y comprobar que las directivas están aplicando los límites de tráfico que espera. Consulte Ver las métricas de tráfico de red.

Edite una directiva 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.

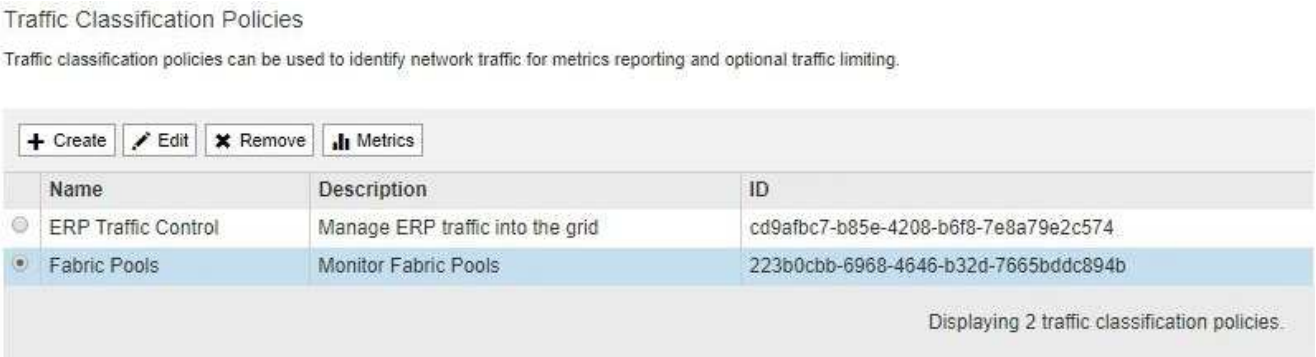
Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

Pasos

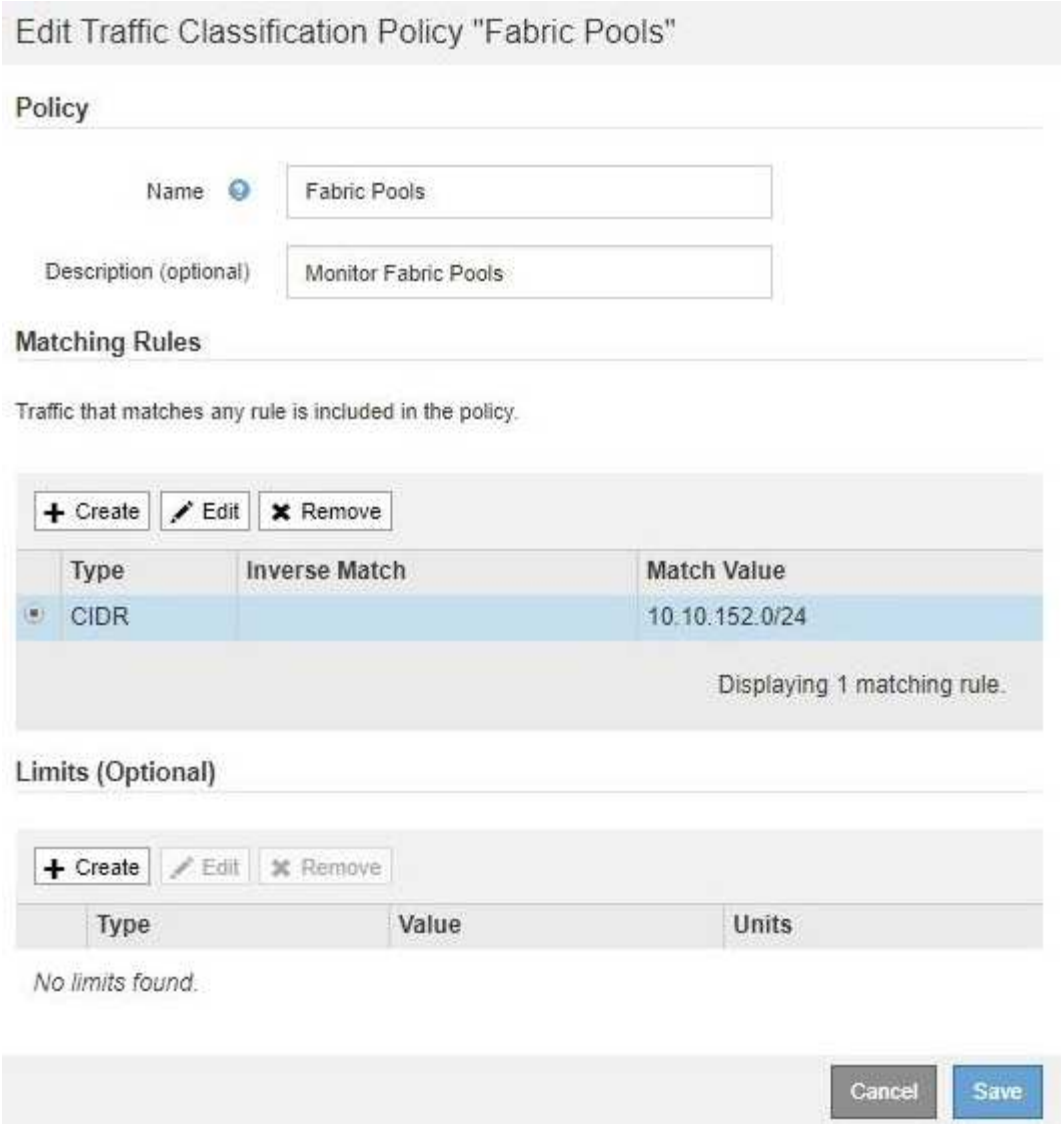
1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.

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



2. Seleccione el botón de opción situado a la izquierda de la directiva que desea editar.
3. Seleccione **Editar**.

   Aparece el cuadro de diálogo Editar directiva de clasificación del tráfico.



4. Cree, edite o elimine reglas y límites coincidentes según sea necesario.
   a. Para crear una regla o un límite coincidente, seleccione **Crear** y siga las instrucciones para crear una regla o crear un límite.
   b. Para editar una regla o un límite coincidente, seleccione el botón de opción para la regla o límite, seleccione **Editar** en la sección **Reglas coincidentes** o la sección **límites** y siga las instrucciones para crear una regla o crear un límite.
   c. Para eliminar una regla o un límite coincidente, seleccione el botón de opción de la regla o límite y seleccione **Quitar**. A continuación, seleccione **Aceptar** para confirmar que desea eliminar la regla o el límite.
5. Cuando haya terminado de crear o editar una regla o un límite, seleccione **aplicar**.
6. Cuando termine de editar la directiva, seleccione **Guardar**.

   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

Si ya no necesita una directiva de clasificación del tráfico, puede eliminarla.

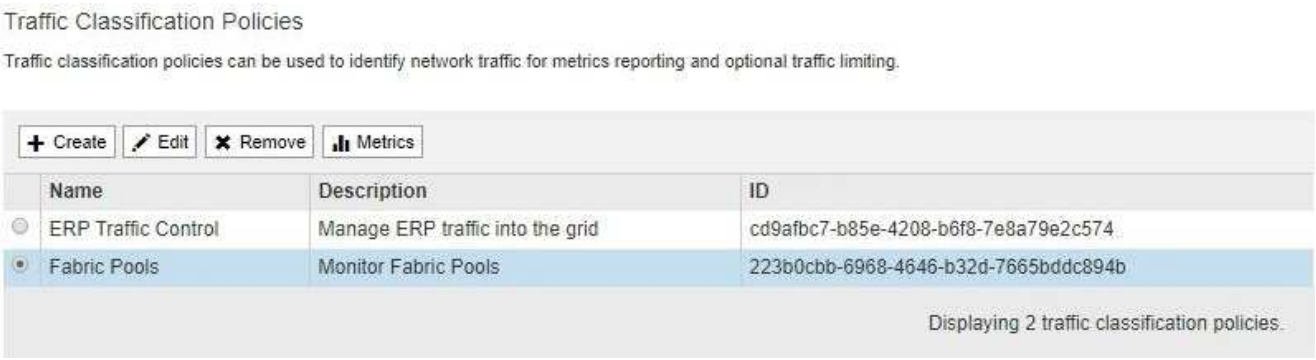
Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

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. Seleccione el botón de opción situado a la izquierda de la directiva que desea eliminar.
3. Seleccione **Quitar**.

   Aparecerá un cuadro de diálogo Advertencia.

4. Seleccione **Aceptar** para confirmar que desea eliminar la directiva.

   La directiva se elimina.

Ver las métricas de tráfico de red

Puede supervisar el tráfico de red mediante la visualización de los gráficos disponibles en la página Directivas de clasificación del tráfico.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz o Cuentas de inquilino.

Acerca de esta tarea

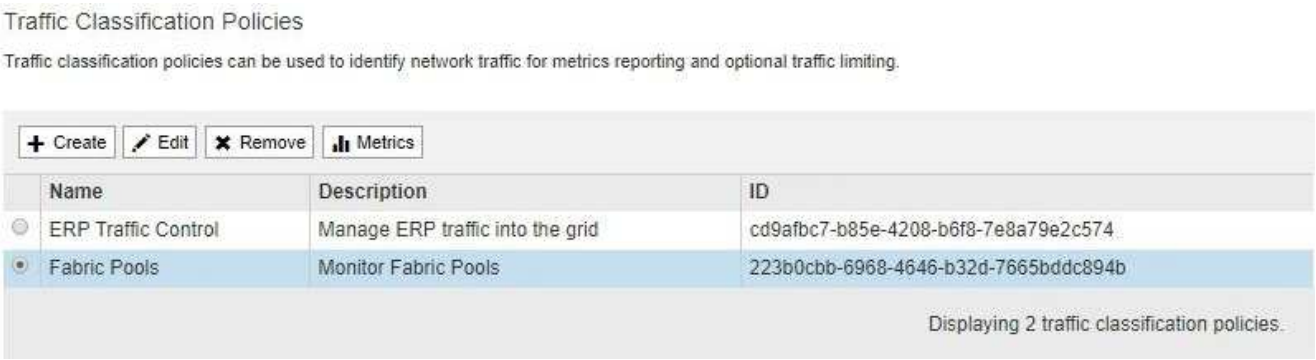
Para cualquier directiva de clasificación de tráfico existente, puede ver las métricas del servicio Load Balancer para determinar si la directiva limita correctamente el tráfico en toda la red. Los datos de los gráficos pueden ayudarle a determinar si es necesario ajustar la política.

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



   Los botones **Crear**, **Editar** y **Quitar** están desactivados si tiene el permiso Cuentas de arrendatario pero no tiene el permiso acceso raíz.

2. Seleccione el botón de opción situado a la izquierda de la política para la que desea ver las métricas.
3. Seleccione **métricas**.

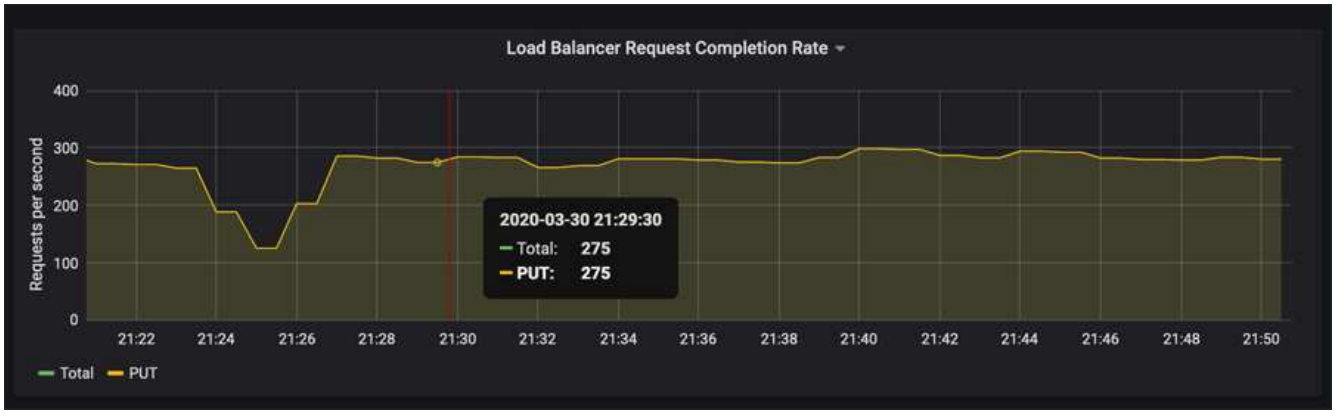
   Se abrirá una nueva ventana del explorador y aparecerán los gráficos de la directiva de clasificación del tráfico. Los gráficos muestran métricas solo para el tráfico que coincide con la directiva seleccionada.

   Puede seleccionar otras directivas para visualizarlas mediante el menú desplegable **Policy**.

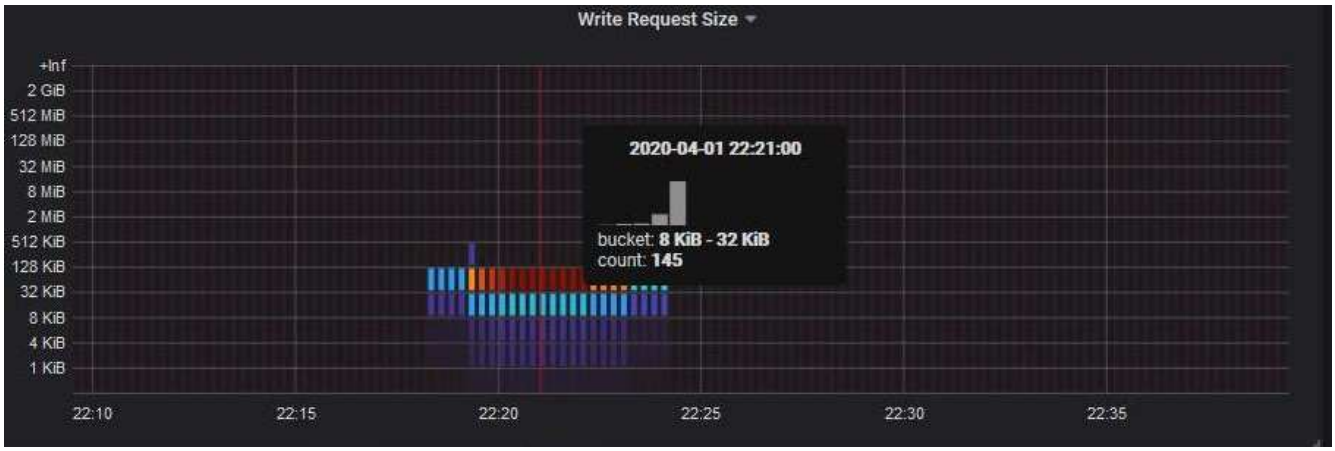
Los siguientes gráficos están incluidos en la página web.

- Tráfico de solicitud del equilibrador de carga: 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.
- Tasa de finalización de solicitudes de equilibrador de carga: Este gráfico proporciona una media de movimiento de 3 minutos del número de solicitudes completadas 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.
- 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.
- Duración media de la solicitud (sin error): Este gráfico proporciona una media móvil de 3 minutos de duración de la solicitud, 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 solicitud de escritura por tamaño de objeto: Este mapa térmico proporciona una media móvil de 3 minutos de la velocidad a la que se completan las solicitudes de escritura en función del tamaño del objeto. En este contexto, las solicitudes de escritura se refieren sólo a SOLICITUDES PUT.
- Tasa de solicitud de lectura por tamaño de objeto: Este mapa térmico proporciona una media móvil de 3 minutos de la velocidad a la que se completan las solicitudes de lectura en función del tamaño del objeto. En este contexto, las solicitudes de lectura se refieren sólo a OBTENER solicitudes. Los colores del mapa térmico indican la frecuencia relativa de un tamaño de objeto dentro de un gráfico individual. Los colores más frescos (por ejemplo, púrpura y azul) indican tasas relativas más bajas, y los colores más cálidos (por ejemplo, naranja y rojo) indican tasas relativas más altas.

4. Pase el cursor por un gráfico de líneas para ver una ventana emergente de valores en una parte específica del gráfico.



5. Pase el cursor por encima de un mapa térmico para ver una ventana emergente que muestra la fecha y hora de la muestra, los tamaños de objeto agregados al recuento y el número de solicitudes por segundo durante ese período de tiempo.



6. Utilice el menú desplegable **Política** de la parte superior izquierda para seleccionar una directiva diferente.

   Se muestran los gráficos de la política seleccionada.

7. También puede acceder a los gráficos desde el menú **SUPPORT**.
   a. Seleccione **SUPPORT** > **Tools** > **Metrics**.
   b. En la sección **Grafana** de la página, seleccione **Directiva de clasificación de tráfico**.
   c. Seleccione la política del menú desplegable que hay en la esquina superior izquierda de la página.

      Las directivas de clasificación del tráfico se identifican por su ID. Los ID de directiva se muestran en la página Directivas de clasificación de tráfico.

8. Analice los gráficos para determinar con qué frecuencia la política limita el tráfico y si necesita ajustar la política.

Información relacionada

Supervisión y solución de problemas

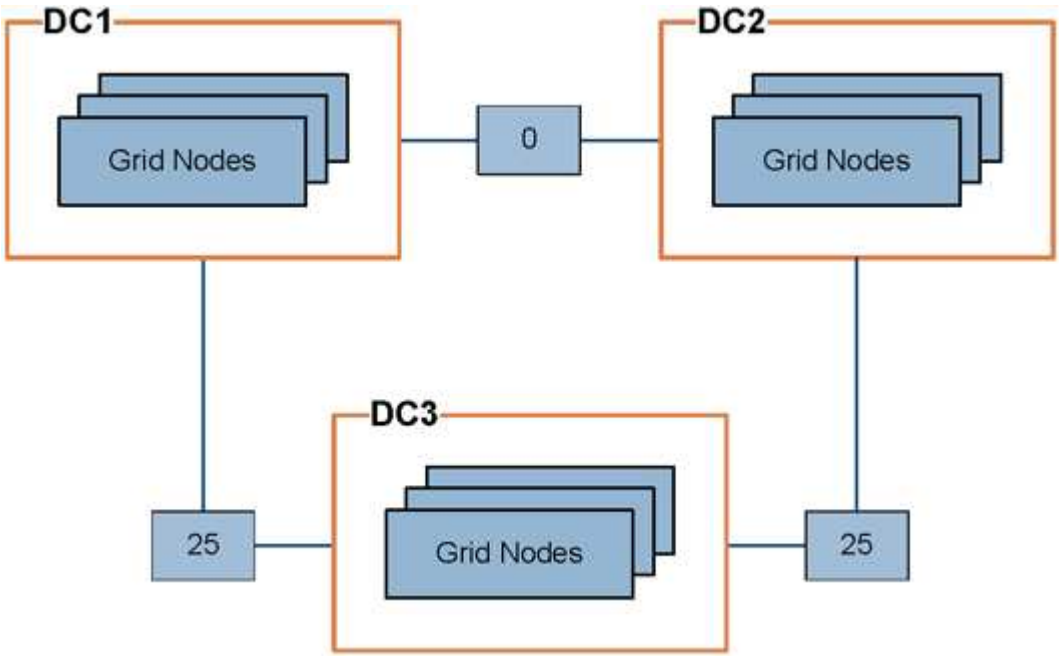
Gestionar costes de enlaces

¿Cuáles son los costes de enlace

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.

- 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 se utilizan en el servicio de equilibrador de carga de conexión (CLB) obsoleto de los nodos de puerta de enlace para dirigir las conexiones de cliente. Consulte Cómo funciona el equilibrio de carga: Servicio CLB.

El diagrama muestra una cuadrícula de tres sitios con costes de enlace configurados entre sitios:



- El servicio CLB de los nodos Gateway distribuye igualmente las conexiones de cliente a todos los nodos de almacenamiento del 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 en DC2 recupera un objeto almacenado en DC1 y DC3, el objeto se recupera de DC1, ya que el coste del vínculo de DC1 a D2 es 0, que es inferior al coste del vínculo 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

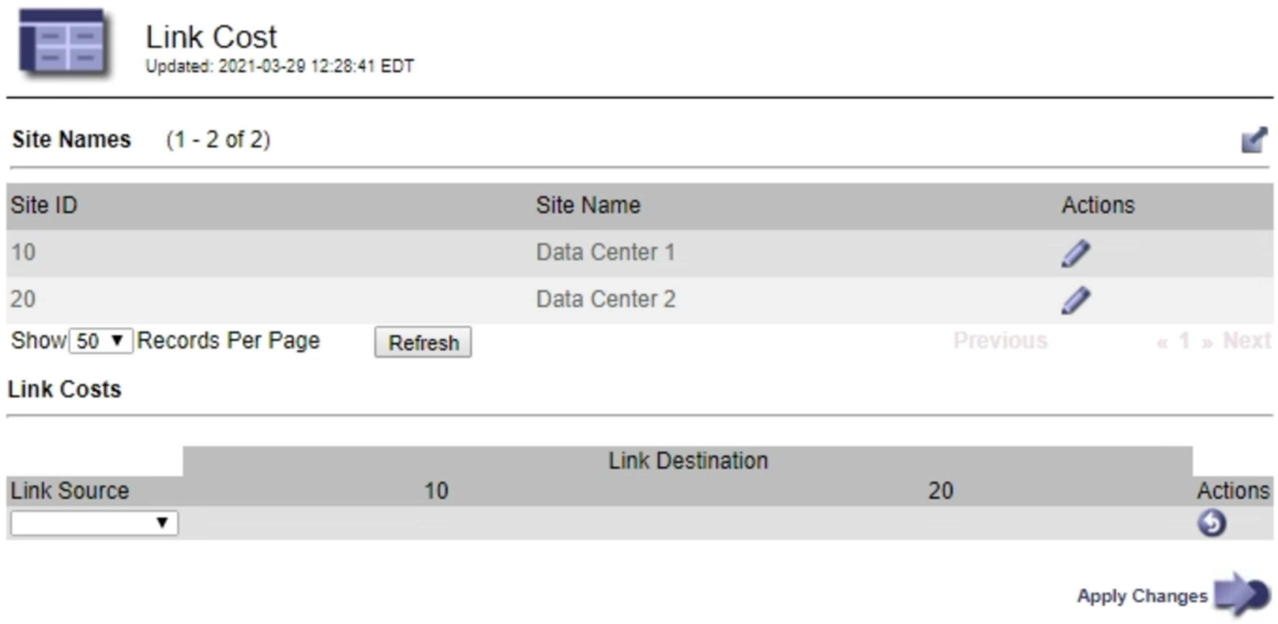
Puede actualizar los costes de enlace entre los sitios de centros de datos para reflejar la latencia entre los sitios.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso Configuración de página de topología de cuadrícula.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **coste 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 se puede cambiar el coste del vínculo si el origen es el mismo que el destino.

   Para cancelar los cambios, seleccione **Revert**.

3. Seleccione **aplicar cambios**.

Utilice AutoSupport

¿Qué es AutoSupport?

La función AutoSupport permite que el sistema StorageGRID envíe mensajes de estado y estado al soporte técnico.

El uso de AutoSupport puede acelerar significativamente la detección 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 los mensajes de AutoSupport para que se envíen a un destino adicional.

Información incluida en los mensajes de AutoSupport

Los mensajes de AutoSupport incluyen información como la siguiente:

- Versión del software StorageGRID
- Versión del sistema operativo
- Información de atributos a nivel de sistema y ubicación
- Alertas y alarmas recientes (sistema heredado)
- Estado actual de todas las tareas de cuadrícula, incluidos los datos históricos
- Uso de la base de datos del nodo de administrador
- Número de objetos perdidos o faltantes
- Ajustes de configuración de cuadrícula
- Entidades NMS
- Política de ILM activa
- Archivo de especificación de grid aprovisionado
- Métricas de diagnóstico

Puede habilitar la función AutoSupport y las opciones individuales de AutoSupport cuando instale StorageGRID por primera vez, o bien puede habilitarlas más adelante. Si AutoSupport no está habilitado, aparecerá un mensaje en el Panel 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.

¿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.

Debe habilitar AutoSupport si desea usar las consolas y la funcionalidad de Active IQ del sitio de soporte de NetApp.

"Documentación del asesor digital de Active IQ"

Protocolos para enviar mensajes AutoSupport

Puede elegir uno de los tres protocolos para enviar mensajes de AutoSupport:

- HTTPS
- HTTP
- SMTP

Si envía mensajes de AutoSupport mediante HTTPS o HTTP, puede configurar un servidor proxy no transparente entre los nodos de administrador y el soporte técnico.

Si utiliza SMTP como protocolo para mensajes de AutoSupport, debe configurar un servidor de correo SMTP.

Opciones de AutoSupport

Puede utilizar cualquier combinación de las siguientes opciones para enviar mensajes de AutoSupport al soporte técnico:

- **Semanal**: Envía automáticamente mensajes de AutoSupport una vez por semana. Valor predeterminado: Activado.
- **Desencadenada por eventos**: Envía automáticamente mensajes AutoSupport cada hora o cuando se producen eventos significativos del sistema. Valor predeterminado: Activado.
- **A petición**: Permita que el servicio de asistencia técnica solicite que el sistema StorageGRID envíe mensajes AutoSupport automáticamente, lo que resulta útil cuando está trabajando activamente en un problema (requiere el protocolo de transmisión HTTPS AutoSupport). Ajuste predeterminado: Desactivado.
- **Desencadenado por el usuario**: Envía manualmente mensajes AutoSupport en cualquier momento.

Información relacionada

"Soporte de NetApp"

Configure AutoSupport

Puede habilitar la función AutoSupport y las opciones individuales de AutoSupport cuando instale StorageGRID por primera vez, o bien puede habilitarlas más adelante.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz u otra configuración de cuadrícula.
- Si utilizará el protocolo HTTPS o HTTP para enviar mensajes AutoSupport, ha proporcionado acceso saliente a Internet al nodo de administración principal, ya sea directamente o mediante un servidor proxy (no se necesitan conexiones entrantes).
- Si usará el protocolo HTTPS o HTTP y desea utilizar un servidor proxy, ya lo tiene Se configuró un servidor proxy de administrador.

- Si utilizará SMTP como protocolo para mensajes de AutoSupport, configuró un servidor de correo SMTP. La misma configuración del servidor de correo se utiliza para las notificaciones de correo electrónico de alarma (sistema heredado).

Especifique el protocolo para los mensajes de AutoSupport

Puede utilizar cualquiera de los siguientes protocolos para enviar mensajes de AutoSupport:

- **HTTPS**: Es la configuración predeterminada y recomendada para nuevas instalaciones. El protocolo HTTPS utiliza el puerto 443. Si desea habilitar la función AutoSupport On Demand, debe usar el protocolo HTTPS.
- **HTTP**: Este protocolo no es seguro, a menos que se utilice en un entorno de confianza donde el servidor proxy se convierte a HTTPS al enviar datos a través de Internet. El protocolo HTTP utiliza el puerto 80.
- **SMTP**: Utilice esta opción si desea que se envíen mensajes de AutoSupport por correo electrónico. Si utiliza SMTP como protocolo para mensajes AutoSupport, debe configurar un servidor de correo SMTP en la página Configuración de correo electrónico heredado (**SUPPORT** > **Alarmas (heredado)** > **Configuración de correo electrónico heredado**).

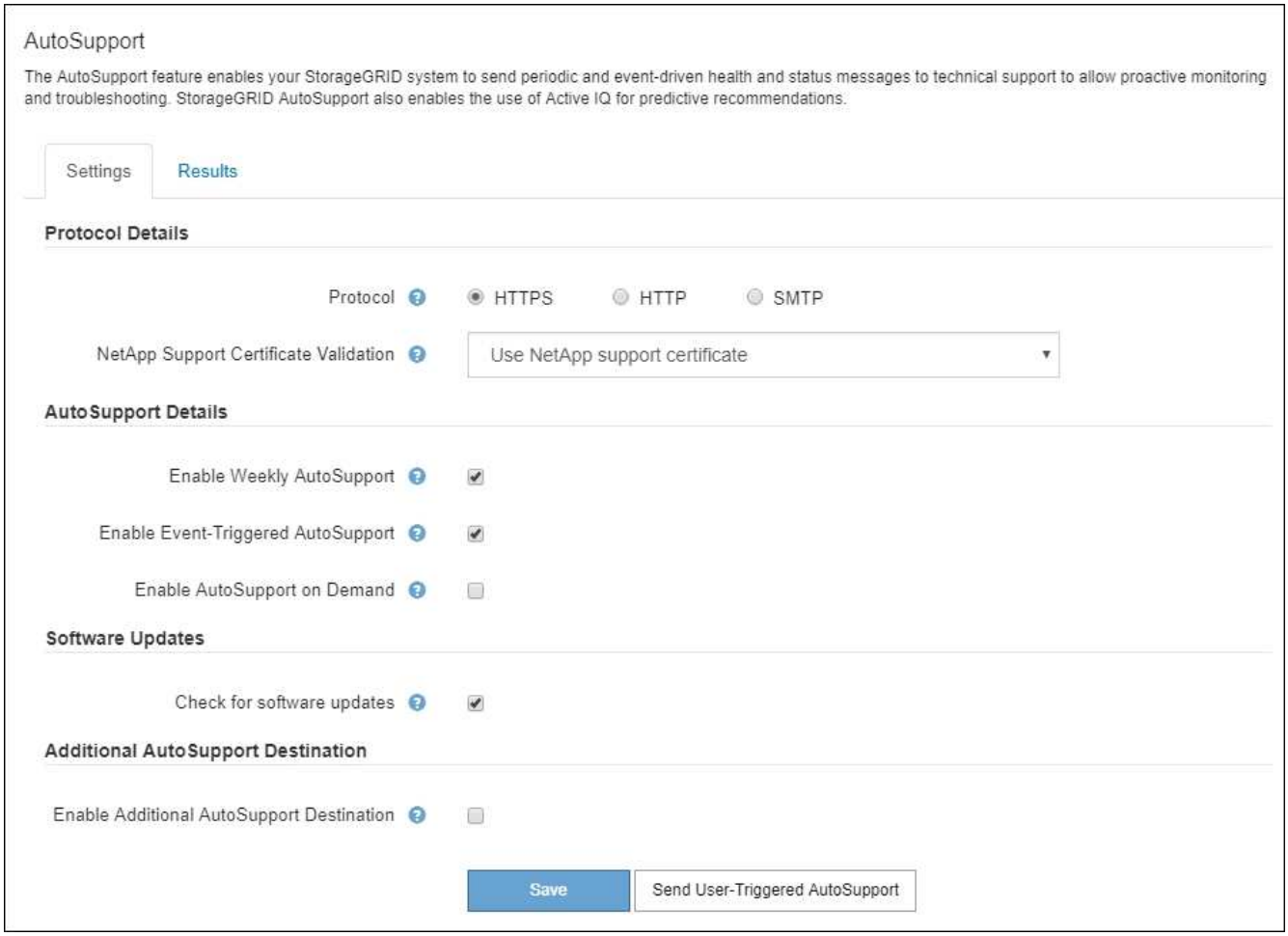
> SMTP era el único protocolo disponible para mensajes de AutoSupport antes de la versión de StorageGRID 11.2. Si instaló inicialmente una versión anterior de StorageGRID, es posible que SMTP sea el protocolo seleccionado.

El protocolo configurado se utiliza para enviar todos los tipos de mensajes de AutoSupport.

Pasos

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

   Aparece la página AutoSupport y la ficha **Configuración** está seleccionada.



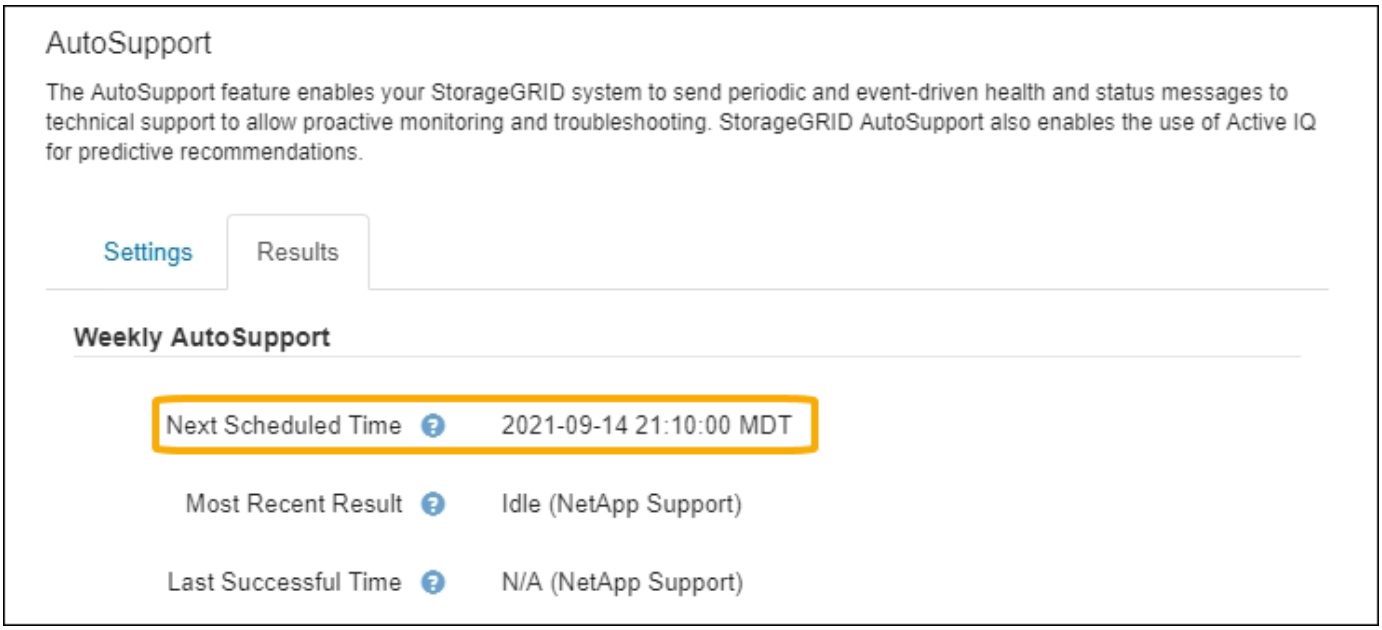
2. Seleccione el protocolo que desea utilizar para enviar mensajes de AutoSupport.
3. Si seleccionó **HTTPS**, seleccione si desea utilizar un certificado TLS para proteger la conexión con el servidor de soporte de NetApp.
   - **Utilizar el certificado de soporte de NetApp** (predeterminado): La validación del certificado garantiza la seguridad de la transmisión de mensajes AutoSupport. 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 mensajes semanales, activados por el usuario y activados por un evento se envían mediante el protocolo seleccionado.

Desactivar los mensajes semanales de AutoSupport

De manera predeterminada, el sistema StorageGRID se configura para que envíe un mensaje de AutoSupport al soporte de NetApp una vez por semana.

Para determinar cuándo se enviará el mensaje semanal de AutoSupport, vaya a la ficha **AutoSupport** > **resultados**. En la sección **AutoSupport** semanal, consulte el valor de **próxima hora programada**.



Puede deshabilitar el envío automático de mensajes semanales de AutoSupport en cualquier momento.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Anule la selección de la casilla de verificación **Activar AutoSupport semanal**.
3. Seleccione **Guardar**.

Deshabilite los mensajes de AutoSupport activados por un evento

De forma predeterminada, el sistema StorageGRID se configura para enviar un mensaje de AutoSupport al soporte de NetApp cuando se produce una alerta importante u otro evento significativo del sistema.

Puede deshabilitar los mensajes de AutoSupport activados por eventos en cualquier momento.

> Los mensajes de AutoSupport activados por los eventos también se suprimen cuando se suprimen las notificaciones de correo electrónico de todo el sistema. (Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de visualización**. A continuación, seleccione **notificación Suprimir todo**.)

Pasos

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Anule la selección de 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 mensajes de AutoSupport automáticamente. El soporte técnico también puede establecer el intervalo de sondeo para AutoSupport en consultas bajo demanda.

El soporte técnico no puede habilitar o deshabilitar AutoSupport bajo demanda.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Seleccione **HTTPS** para el protocolo.
3. Active la casilla de verificación **Activar AutoSupport semanal**.
4. Active la casilla de verificación **Activar AutoSupport a petición**.
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. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Deseleccione la casilla de verificación **Buscar actualizaciones de software**.
3. Seleccione **Guardar**.

Añada un destino de AutoSupport adicional

Cuando se habilita AutoSupport, se envían mensajes de estado y estado al soporte de NetApp. Puede especificar un destino adicional para todos los mensajes de AutoSupport.

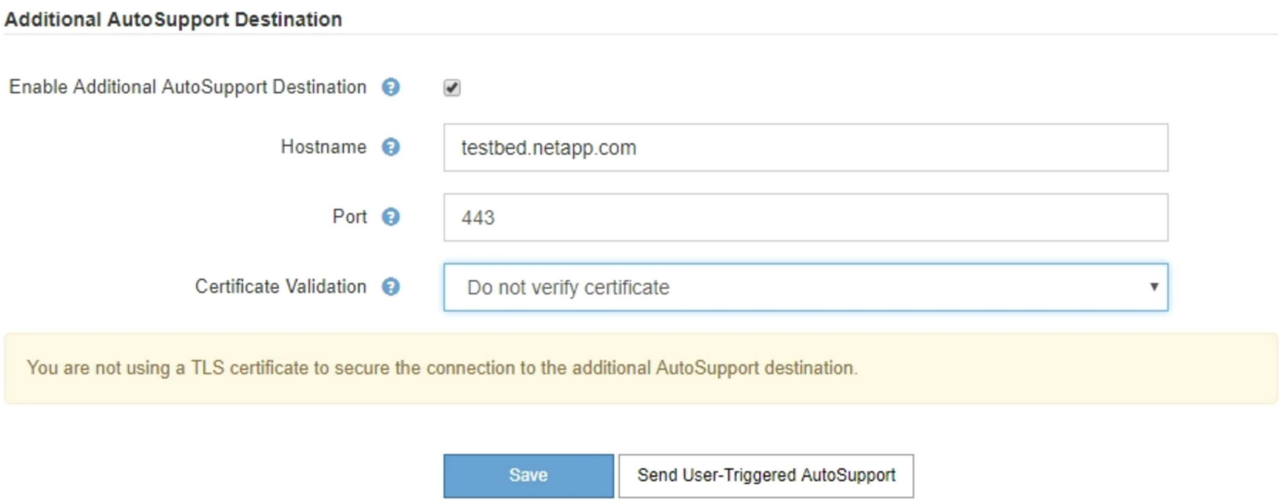
Para comprobar o cambiar el protocolo utilizado para enviar mensajes AutoSupport, consulte las instrucciones a. Especifique el protocolo para los mensajes de AutoSupport.

> No se puede utilizar el protocolo SMTP para enviar mensajes de AutoSupport a un destino adicional.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **AutoSupport**.
2. Seleccione **Activar destino AutoSupport adicional**.

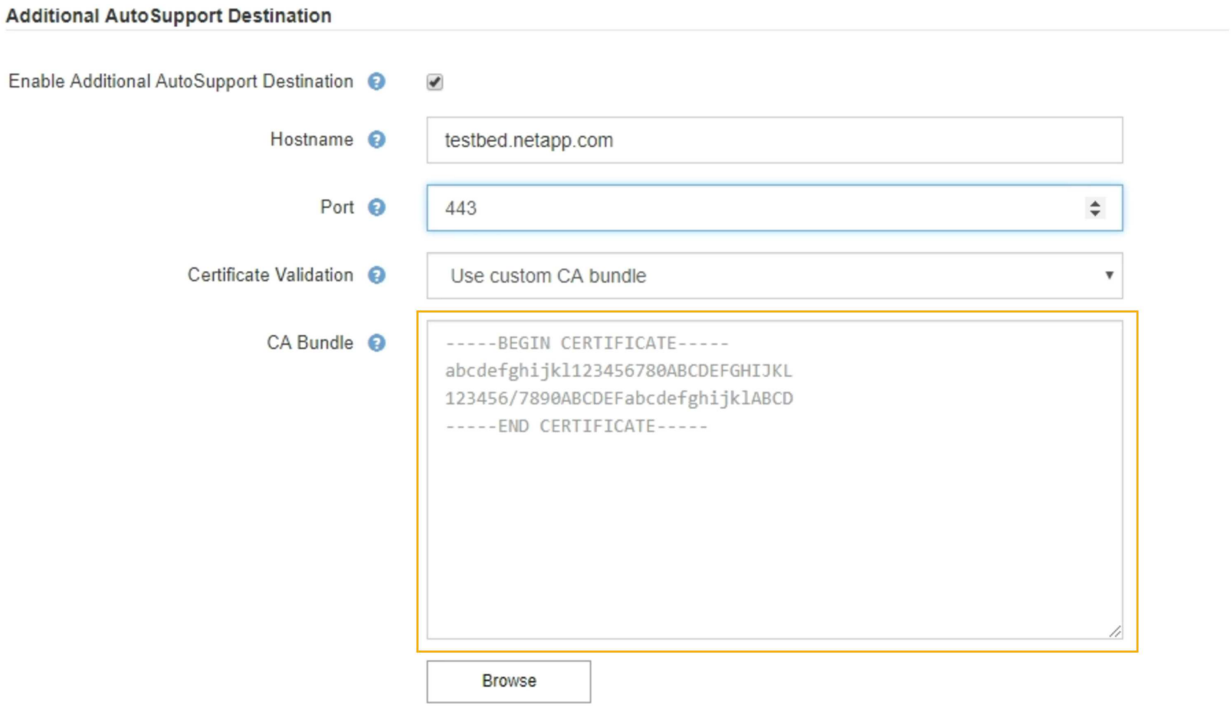
   Aparecerán los campos destino AutoSupport adicional.



3. Introduzca el nombre de host o la dirección IP del servidor de un servidor de destino AutoSupport adicional.

> Puede introducir solo un destino adicional.

4. Introduzca el puerto utilizado para conectarse a un servidor de destino AutoSupport adicional (el puerto predeterminado es el 80 para HTTP o el puerto 443 para HTTPS).
5. Para enviar los mensajes de AutoSupport con validación de certificados, seleccione **usar paquete de CA personalizado** en el menú desplegable **validación de certificados**. A continuación, realice una de las siguientes acciones:
   - Utilice una herramienta de edición para copiar y pegar todo el contenido de cada uno de los archivos de certificados de CA codificados con PEM en el campo **paquete de CA**, concatenado en el orden de la cadena de certificados. Debe incluir `----BEGIN CERTIFICATE----` y.. `----END CERTIFICATE----` en su selección.



- Seleccione **examinar**, desplácese hasta el archivo que contiene los certificados y, a continuación, seleccione **Abrir** para cargar el archivo. La validación de certificados garantiza la seguridad de la transmisión de mensajes de AutoSupport.

6. Para enviar sus mensajes AutoSupport sin validación de certificados, seleccione **no verificar certificado** en el menú desplegable **validación de certificados**.

   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.

   Aparece un mensaje de precaución: "No está utilizando un certificado TLS para garantizar la conexión al destino AutoSupport adicional".

7. Seleccione **Guardar**.

   Todos los futuros mensajes de AutoSupport semanales, activados por un evento y activados por el usuario se enviarán al destino adicional.

Active manualmente un mensaje de AutoSupport

Con el fin de ayudar al soporte técnico a solucionar problemas con su sistema StorageGRID, puede activar manualmente el envío de un mensaje de AutoSupport.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz u otra configuración de cuadrícula.

Pasos

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

   Aparece la página AutoSupport con la ficha **Configuración** seleccionada.

2. Seleccione **Enviar AutoSupport desencadenado por el usuario**.

   StorageGRID intenta enviar un mensaje de AutoSupport al soporte técnico. Si el intento se realiza correctamente, se actualizan los valores **resultado más reciente** y **tiempo más reciente** de la ficha **resultados**. Si hay algún problema, el valor del **resultado más reciente** se actualiza a "error" y StorageGRID no intenta volver a enviar el mensaje AutoSupport.

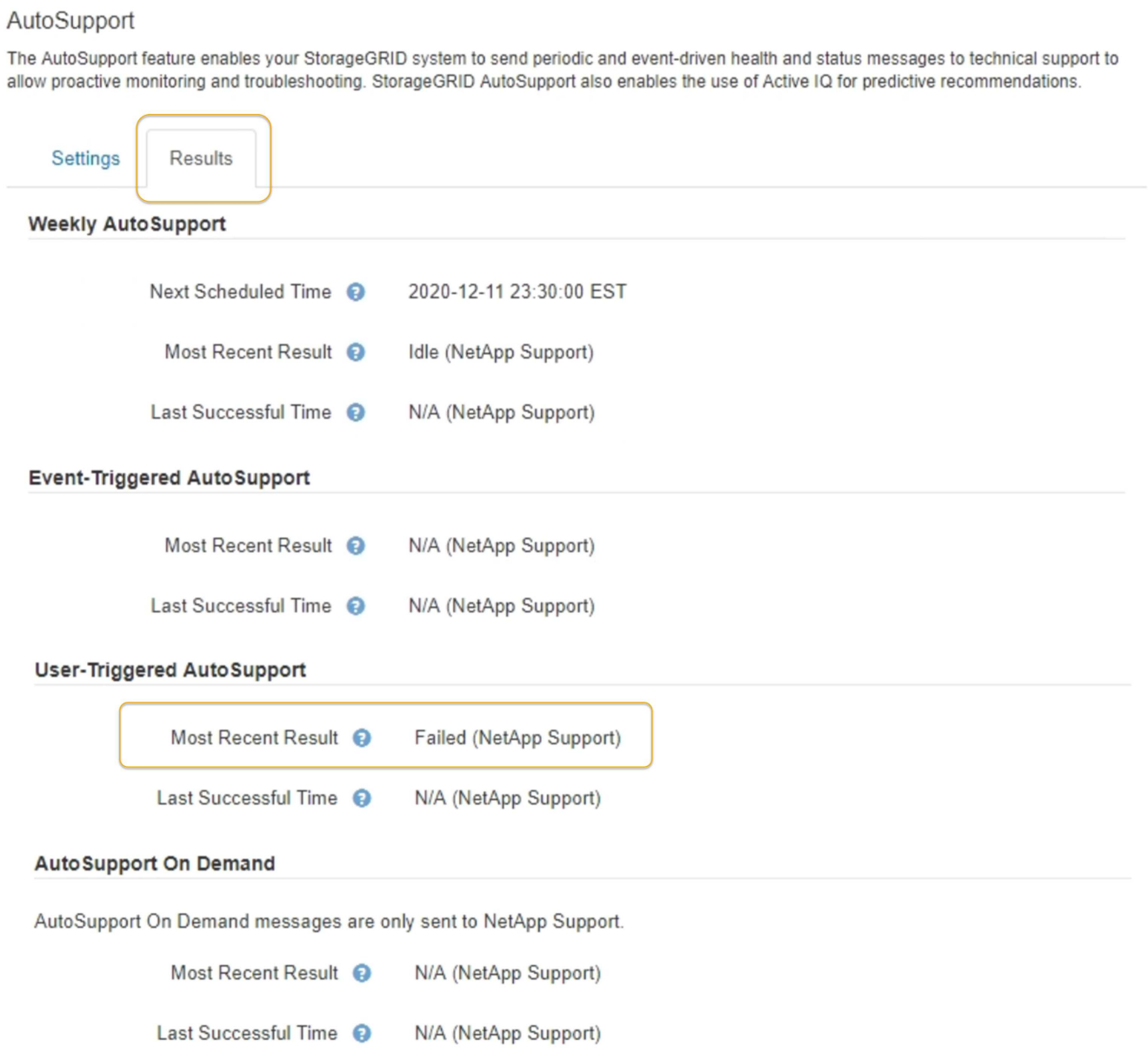
   > Después de enviar un mensaje AutoSupport activado por el usuario, actualice la página AutoSupport en el explorador después de 1 minuto para acceder a los resultados más recientes.

Solucionar los problemas de los mensajes de AutoSupport

Si se produce un error al intentar enviar un mensaje de AutoSupport, el sistema StorageGRID realiza distintas acciones según el tipo de mensaje de AutoSupport. Puede comprobar el estado de los mensajes de AutoSupport seleccionando **ASISTENCIA** > **Herramientas** > **AutoSupport** > **resultados**.

> Los mensajes de AutoSupport activados por un evento se suprimen cuando se suprimen las notificaciones de correo electrónico de todo el sistema. (Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de visualización**. A continuación, seleccione **notificación Suprimir todo**.)

Cuando el mensaje AutoSupport no se envía, aparece "'failed'" en la ficha **resultados** de la página **AutoSupport**.



Fallo de mensaje semanal de AutoSupport

Si un mensaje semanal de AutoSupport no se envía, el sistema StorageGRID realiza las siguientes acciones:

1. Actualiza el atributo de resultado más reciente a Reintentando.
2. Intenta reenviar el mensaje 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 de nuevo un mensaje de AutoSupport a la siguiente hora programada.
5. Mantiene la programación normal de AutoSupport si el mensaje falla porque el servicio NMS no está disponible y si se envía un mensaje antes de pasar siete días.
6. Cuando el servicio NMS está disponible de nuevo, envía un mensaje AutoSupport inmediatamente si no se ha enviado un mensaje durante siete días o más.

Error de mensaje AutoSupport activado por el usuario o activado por eventos

Si un mensaje AutoSupport activado por el usuario o activado por un evento no se puede enviar, el sistema StorageGRID lleva a cabo 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 messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. No intenta volver a enviar el mensaje.
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 messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Obtenga información acerca de cómo configurar los ajustes del servidor de correo electrónico en supervisar y solucionar problemas de instrucciones.

Corrija un error en un mensaje de 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 messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envíe mensajes de AutoSupport de E-Series a través de StorageGRID

Puede enviar mensajes de AutoSupport de E-Series SANtricity System Manager al soporte técnico a través de un nodo de administrador de StorageGRID en lugar de hacerlo con el puerto de gestión del dispositivo de almacenamiento.

Lo que necesitará

- Se ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso de administrador de dispositivo de almacenamiento o acceso raíz.

> Debe tener el firmware 8.70 (11.7) de SANtricity o superior para acceder a SANtricity System Manager mediante Grid Manager.

Acerca de esta tarea

Los mensajes de AutoSupport de E-Series contienen detalles del hardware de almacenamiento y son más

específicos que otros mensajes de AutoSupport que envía el sistema StorageGRID.

Configurar una dirección de servidor proxy especial en System Manager de SANtricity para que los mensajes de AutoSupport se transmitan a través de un nodo de administración de StorageGRID sin usar el puerto de gestión del dispositivo. Los mensajes AutoSupport transmitidos de esta manera respetan la configuración de proxy de administrador y remitente preferido que se puede haber configurado en el Administrador de grid.

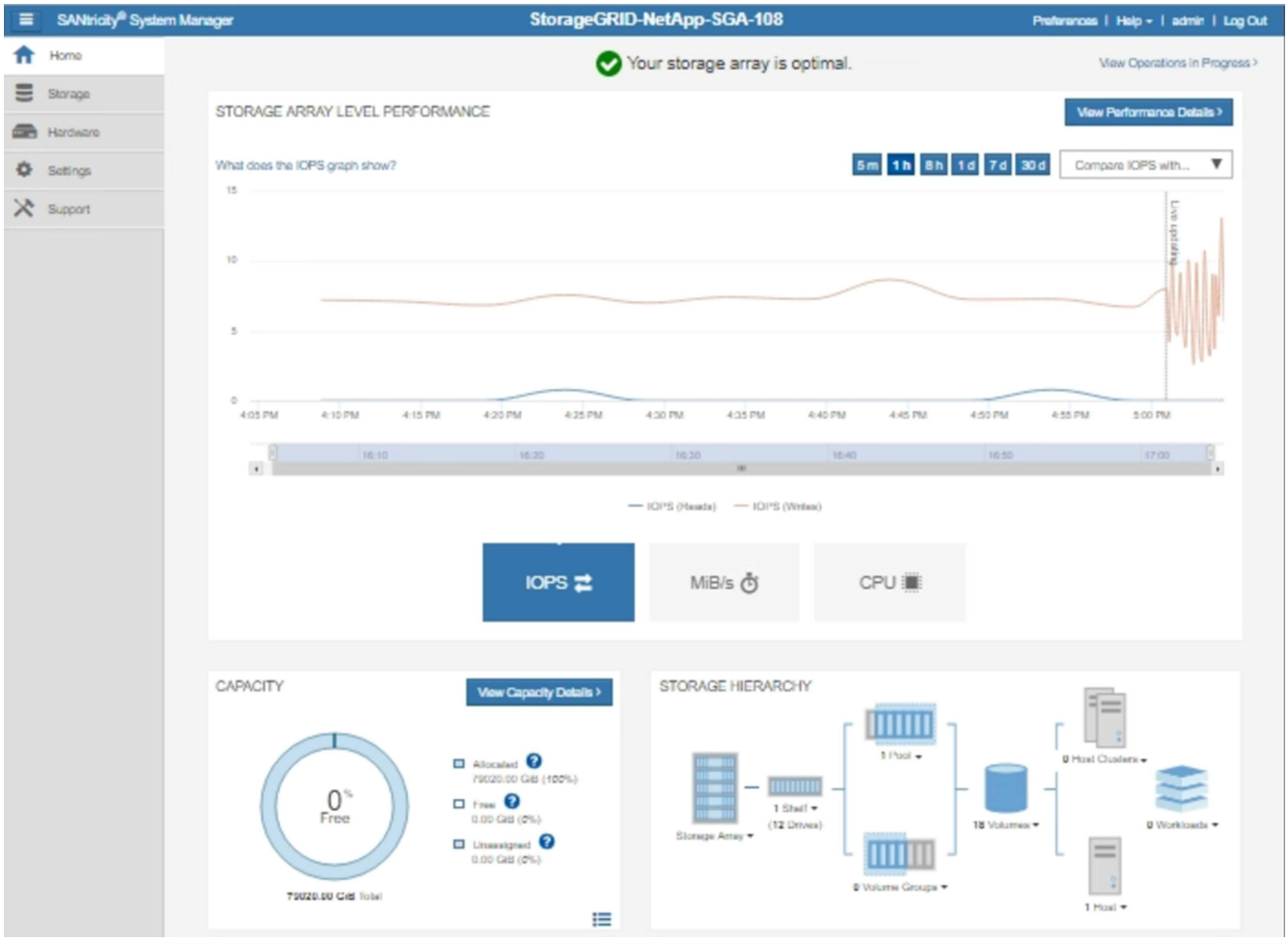
Si desea configurar el servidor proxy de administración en Grid Manager, consulte Configure los ajustes del proxy de administración.

> Este procedimiento solo se utiliza para configurar un servidor proxy StorageGRID para los mensajes de 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

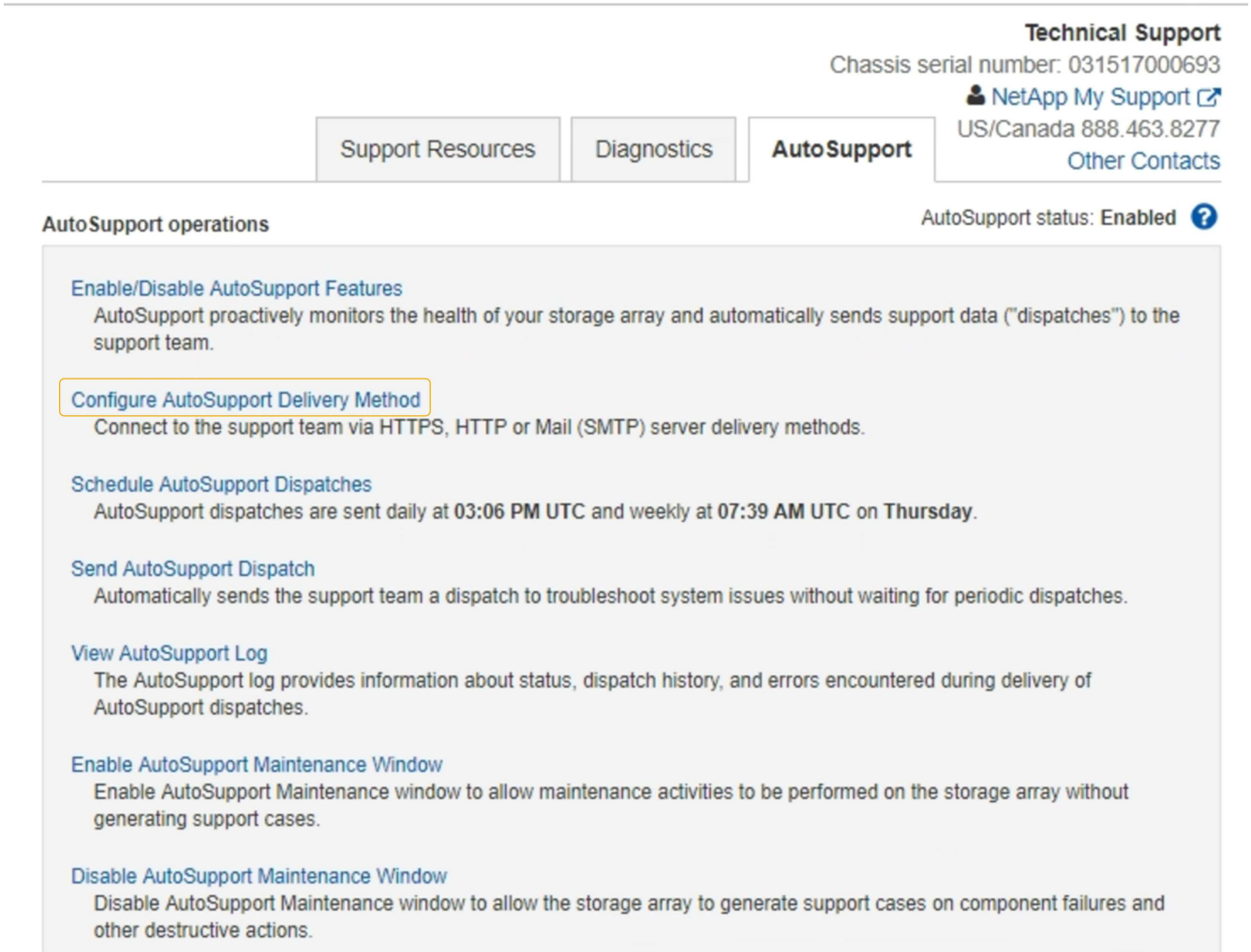
1. En Grid Manager, seleccione **NODES**.
2. En la lista de nodos que aparece a la izquierda, seleccione el nodo del dispositivo de almacenamiento que desea configurar.
3. Seleccione **Administrador del sistema SANtricity**.

   Se mostrará la página de inicio de SANtricity System Manager.



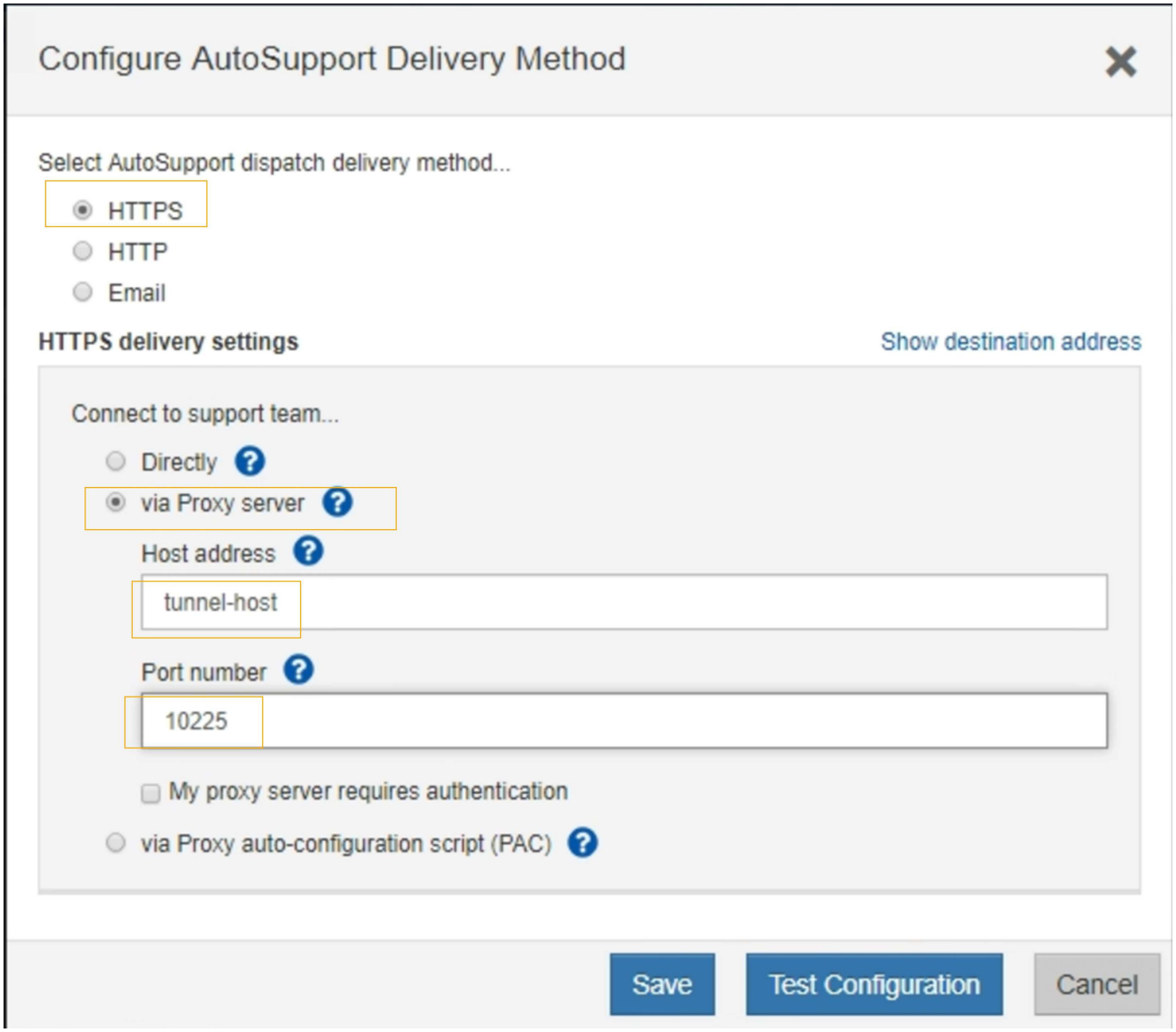
4. Seleccione **SUPPORT** > **Support Center** > **AutoSupport**.

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 permite el protocolo 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 que usa un nodo de administrador para enviar mensajes de AutoSupport E-Series.

9. Introduzca `10225` Para el **número de puerto**.

   `10225` Es el número de puerto del servidor del proxy StorageGRID que recibe mensajes de 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, aparecerá un mensaje en un banner verde: "'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 y las redes de StorageGRID, asegúrese de que el nodo de administrador del remitente preferido se pueda conectar al sitio de soporte de NetApp y vuelva a intentar la prueba.

11. Seleccione **Guardar**.

    Se guardará la configuración y aparecerá un mensaje de confirmación: "'se ha configurado el método de entrega de AutoSupport'".

Gestione nodos de almacenamiento

Acerca de la gestión de nodos de almacenamiento

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

¿Qué es un nodo de almacenamiento?

Los nodos de almacenamiento gestionan y almacenan metadatos y datos de objetos. Cada sistema StorageGRID debe tener al menos tres nodos de almacenamiento. Si tiene varios sitios, cada sitio dentro del sistema StorageGRID también debe tener tres nodos de almacenamiento.

Un nodo de almacenamiento incluye los servicios y procesos necesarios para almacenar, mover, verificar y recuperar metadatos y datos de objetos en el disco. Puede ver información detallada sobre los nodos de almacenamiento en la página **NODES**.

¿Qué es el servicio ADC?

El servicio de controlador de dominio administrativo (ADC) autentica los nodos de grid y sus conexiones entre sí. El servicio ADC está alojado en cada uno de los tres primeros nodos de almacenamiento de 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 StorageGRID, lo que permite que cualquier nodo de la cuadrícula recupere la información de configuración actual.puede ver la información de ADC de un nodo de almacenamiento en la página Topología de la cuadrícula (**SUPPORT** > **topología de la cuadrícula**).

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 a los sistemas seguir funcionando con nodos de grid conocidos incluso cuando un servicio de 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.

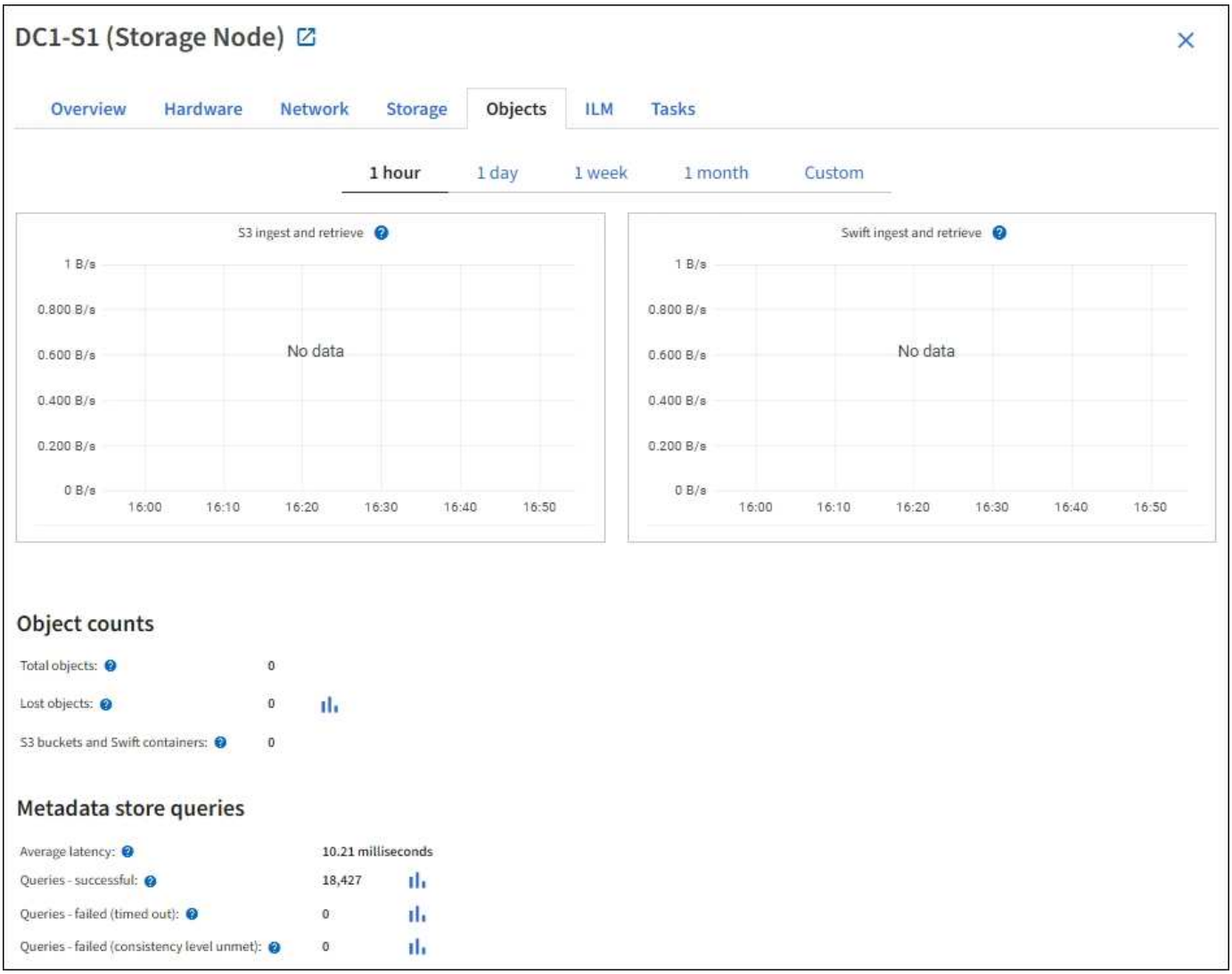
¿Qué es el servicio DDS?

Alojado por un nodo de almacenamiento, el servicio almacén de datos distribuidos (DDS) interactúa con la base de datos de Cassandra para realizar tareas en segundo plano en los metadatos de objeto almacenados en el sistema StorageGRID.

El número de objetos

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).

Puede ver el número total de objetos en la página Nodes > la pestaña Objects de cualquier nodo de almacenamiento.



Consultas

Puede identificar el tiempo medio que tarda en ejecutar una consulta en el almacén de metadatos a través del servicio DDS específico, el número total de consultas correctas y el número total de consultas que han fallado debido a un problema de tiempo de espera.

Se recomienda revisar la información de consulta para supervisar el estado del almacén de metadatos, Cassandra, lo que afecta al rendimiento de procesamiento y recuperación del sistema. Por ejemplo, si la latencia de una consulta media es lenta y el número de consultas con errores debido a tiempos de espera es elevado, es posible que el almacén de metadatos encuentre una carga mayor o realice otra operación.

También puede ver el número total de consultas que han fallado debido a los fallos de consistencia. Los fallos de nivel de coherencia se deben a un número insuficiente de almacenes de metadatos disponibles en el momento en que se realiza una consulta a través del servicio DDS específico.

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

Garantías y controles de coherencia

StorageGRID garantiza la coherencia de lectura tras escritura para los objetos recién creados. Cualquier OPERACIÓN DE OBTENER después de una operación DE PUT completada correctamente podrá leer los

datos recién escritos. Las sobrescrituras de objetos existentes, actualizaciones de metadatos y eliminaciones siguen siendo coherentes en la actualidad.

¿Qué es el servicio LDR?

Alojado por cada nodo de almacenamiento, el servicio de router de distribución local (LDR) gestiona el transporte de contenido para el sistema StorageGRID. El transporte de contenido abarca numerosas tareas, como el almacenamiento de datos, el enrutamiento y la gestión de solicitudes. El servicio LDR realiza la mayor parte del trabajo duro del sistema StorageGRID al manejar cargas de transferencia de datos y 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 gestiona la asignación de objetos S3 y Swift a los "'Content Hands' (UUID) únicos que el sistema StorageGRID asigna a cada objeto ingerido.

Consultas

Las consultas de LDR incluyen consultas de ubicación de objetos durante las operaciones de recuperación y archivado. Puede identificar el tiempo medio que tarda en ejecutar una consulta, el número total de consultas correctas y el número total de consultas que han fallado debido a un problema de tiempo de espera.

Puede revisar la información de consulta para supervisar el estado del almacén de metadatos, lo que afecta al rendimiento de procesamiento y recuperación del sistema. Por ejemplo, si la latencia de una consulta media es lenta y el número de consultas con errores debido a tiempos de espera es elevado, es posible que el almacén de metadatos encuentre una carga mayor o realice otra operación.

También puede ver el número total de consultas que han fallado debido a los fallos de consistencia. Los fallos de nivel de consistencia se deben a un número insuficiente de almacenes de metadatos disponibles en el momento en que se realiza una consulta a través del servicio LDR específico.

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

Actividad de ILM

Las métricas de gestión de ciclo de vida de la información (ILM) permiten supervisar la velocidad a la que se evalúan los objetos para la implementación de ILM. Puede ver estas métricas en el Panel o en **NODES** > ***Storage Node*** > **ILM**.

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.

Puede ver los almacenes de objetos de un nodo de almacenamiento en la página nodos > pestaña Storage.

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

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.

Para garantizar hasta el uso de espacio para las copias replicadas, los datos de objetos para un objeto determinado se almacenan en un almacén de objetos en función del espacio de almacenamiento disponible. Cuando uno o varios almacenes de objetos se llenan de capacidad, los almacenes de objetos restantes siguen almacenando objetos hasta que no hay más espacio en el nodo de almacenamiento.

Protección de metadatos

Los metadatos de objetos son información relacionada con un objeto o una descripción de él; por ejemplo, el tiempo de modificación del objeto o la ubicación de almacenamiento. StorageGRID almacena metadatos de objetos en una base de datos de Cassandra, que se conecta con el servicio LDR.

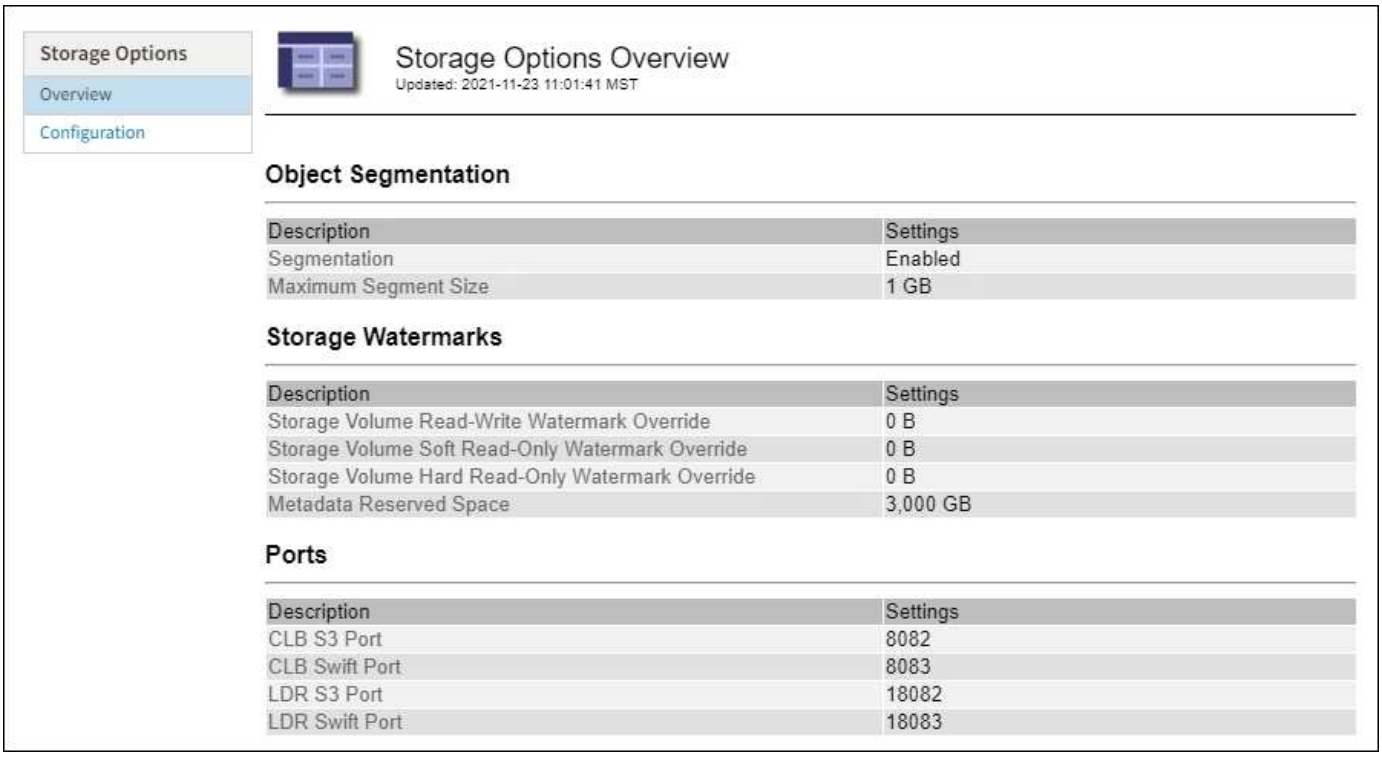
Para garantizar la redundancia y, por lo tanto, la protección contra la pérdida, se mantienen tres copias de metadatos de objetos en cada sitio. Las copias se distribuyen uniformemente por todos los nodos de almacenamiento de cada sitio. Esta replicación no puede configurarse y se realiza de forma automática.

Gestione el almacenamiento de metadatos de objetos

Gestionar opciones de almacenamiento

Las opciones de almacenamiento incluyen la configuración de segmentación de objetos, los valores actuales para las marcas de agua del volumen de almacenamiento y la configuración de espacio reservado de metadatos. También es posible ver los puertos S3 y Swift que utiliza el servicio CLB obsoleto en los nodos de puerta de enlace y el servicio LDR en los nodos de almacenamiento.

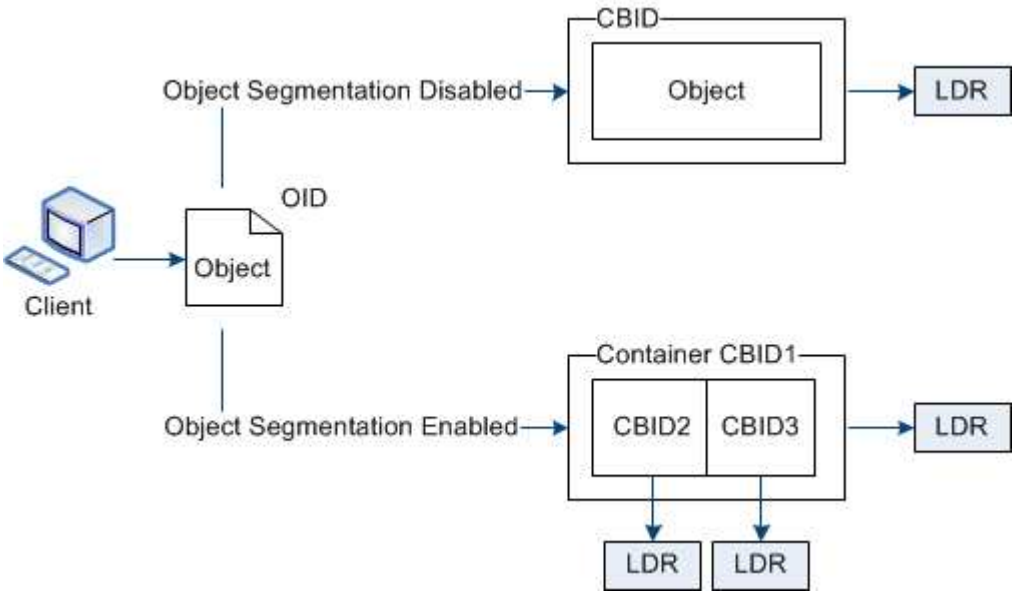
Para obtener información acerca de las asignaciones de puertos, consulte Resumen: Direcciones IP y puertos para conexiones cliente.



¿Qué es la segmentación de objetos?

La segmentación de objetos es el proceso de dividir un objeto en una colección de objetos de tamaño fijo más pequeños para optimizar el uso del almacenamiento y los recursos 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 están almacenados 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:

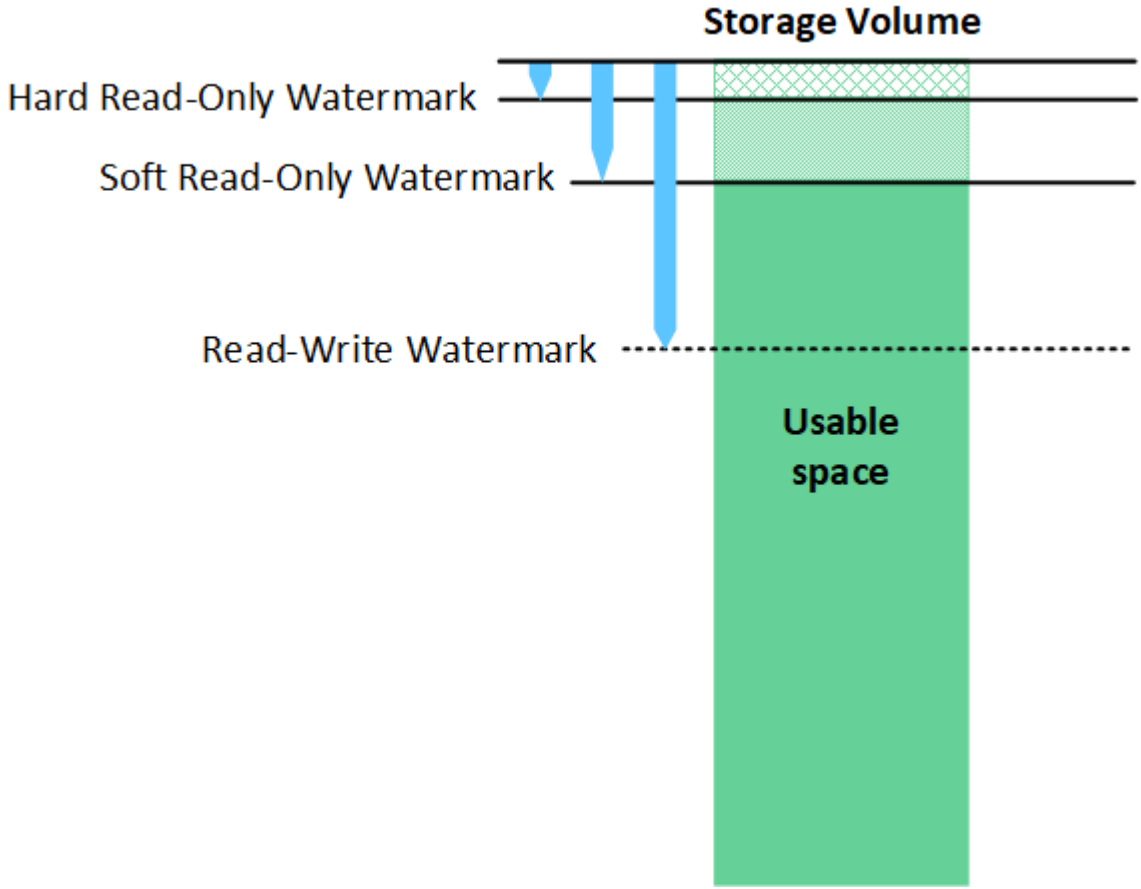
contenedor de segmentos + segmento 1 + segmento 2 = tres objetos almacenados

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 los ajustes.

Lo que necesitará

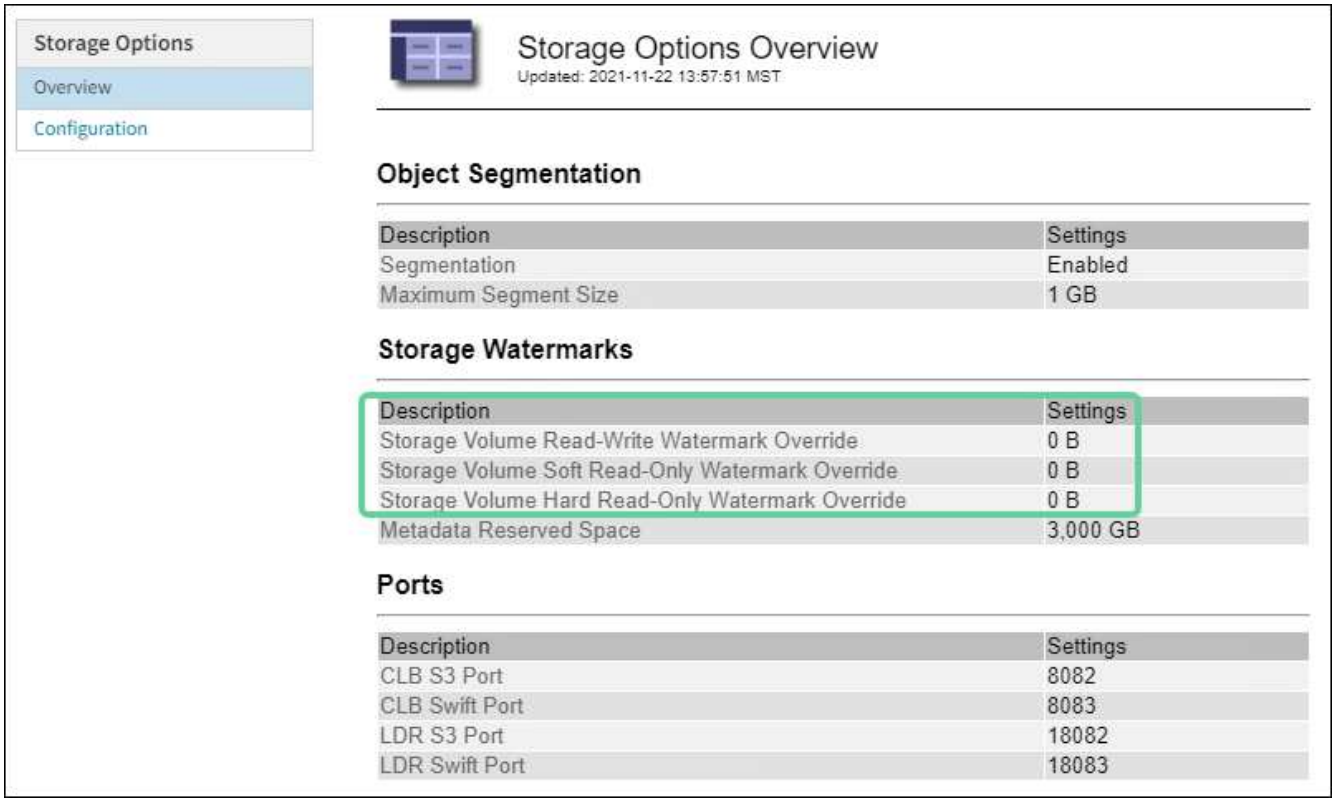
- Ha completado la actualización a StorageGRID 11.6.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

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. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de almacenamiento**.
2. En la sección Marcas de agua de almacenamiento, observe los ajustes para las tres anulaciones de la Marca de agua de volumen de almacenamiento.



   - Si las anulaciones de la Marca de agua son **0**, las tres marcas de agua están optimizadas 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 debe actualizar estos valores. Según sea necesario, puede opcionalmente Vea las marcas de agua de almacenamiento optimizadas.

   - Si las anulaciones de la Marca de agua son valores distintos de 0, se utilizan 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.

Vea las 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:

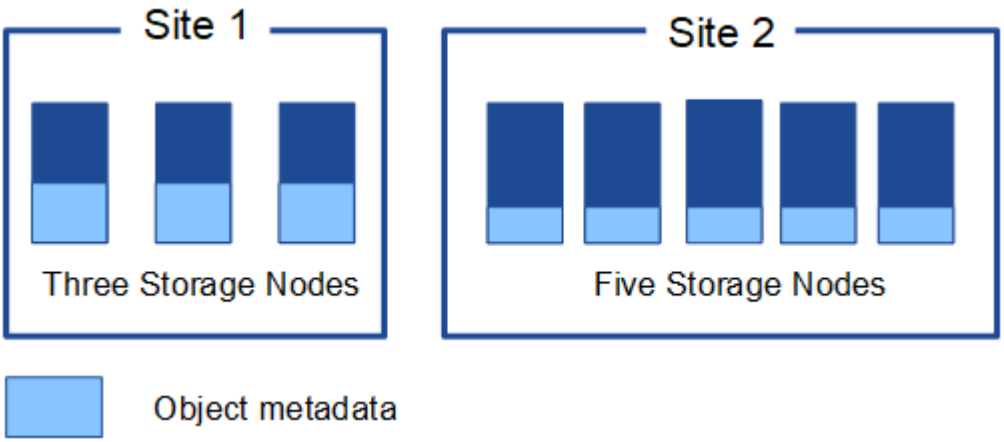
- Metadatos del sistema, incluidos un ID único para cada objeto (UUID), el nombre del objeto, el nombre del bloque de S3 o el contenedor Swift, el nombre o el ID de la cuenta de inquilino, el tamaño lógico del objeto, la fecha y la hora en que se creó el objeto por primera vez, y la fecha y hora en que 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?

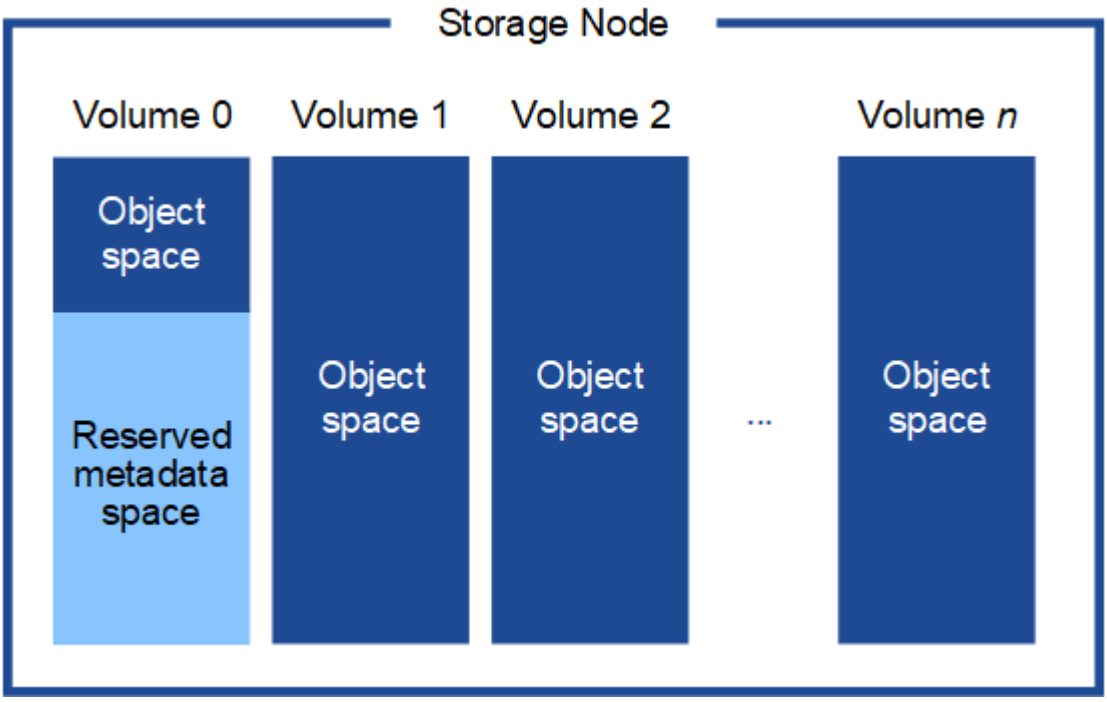
StorageGRID mantiene los metadatos de objetos en una base de datos de Cassandra, que se almacena independientemente de los datos de objetos. Para proporcionar redundancia y proteger los metadatos de objetos de la pérdida, StorageGRID almacena tres copias de los metadatos para todos los objetos del sistema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

Esta figura representa los nodos de almacenamiento de dos sitios. Cada sitio tiene la misma cantidad de metadatos de objetos, que está igualmente distribuido entre 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 que se reserva para metadatos de objetos en un nodo de almacenamiento determinado depende de varios factores, que se describen a continuación.

Configuración de espacio reservado de metadatos

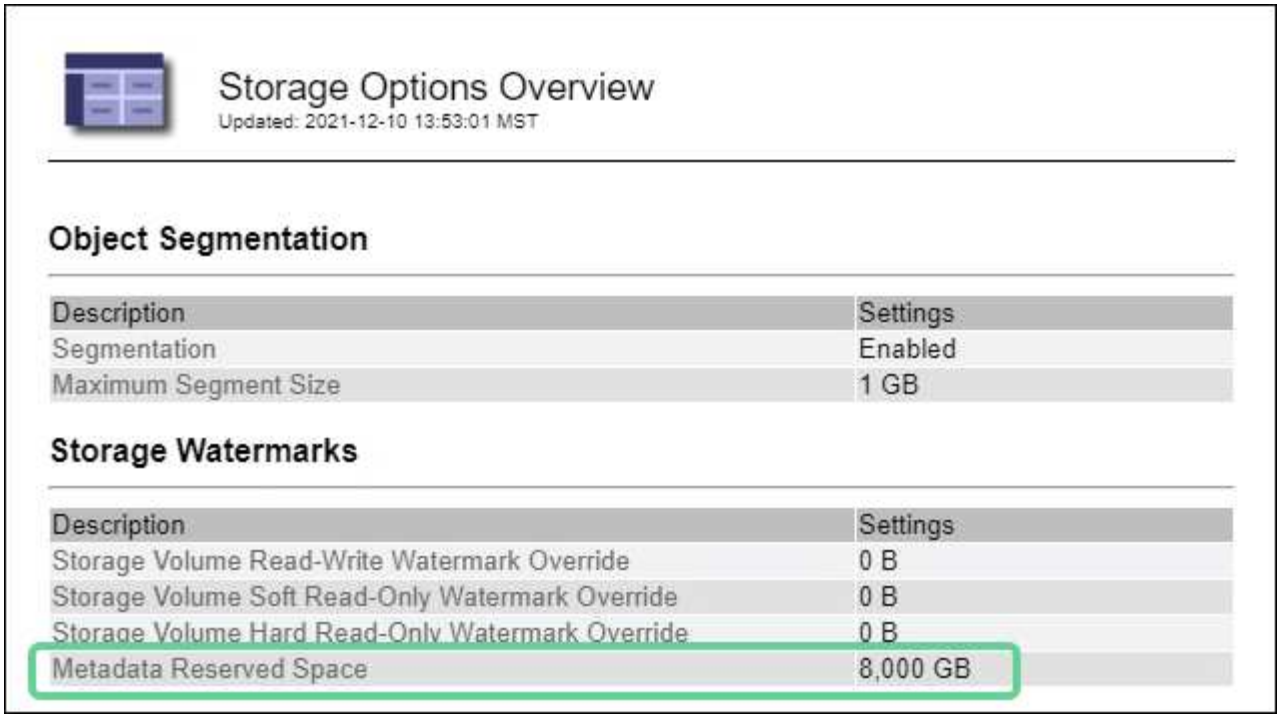
El *Metadata Reserved Space* es una configuración para todo el sistema que representa la cantidad de espacio que se reservará para metadatos en el volumen 0 de cada nodo de almacenamiento. Tal como se muestra en la tabla, el valor predeterminado de esta configuración para StorageGRID 11.6 se basa en lo siguiente:

- 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	Configuración de espacio reservado de metadatos predeterminado para StorageGRID 11.6
11.5/11.6	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)
	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)

Para ver la configuración del espacio reservado de metadatos para el sistema StorageGRID:

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de almacenamiento**.
2. En la tabla Marcas de agua de almacenamiento, busque **espacio reservado de metadatos**.



En la captura de pantalla, el valor **espacio reservado de metadatos** es 8,000 GB (8 TB). Esta es la configuración predeterminada para una nueva instalación de StorageGRID 11.6 en la que cada nodo de almacenamiento tiene 128 GB o más de RAM.

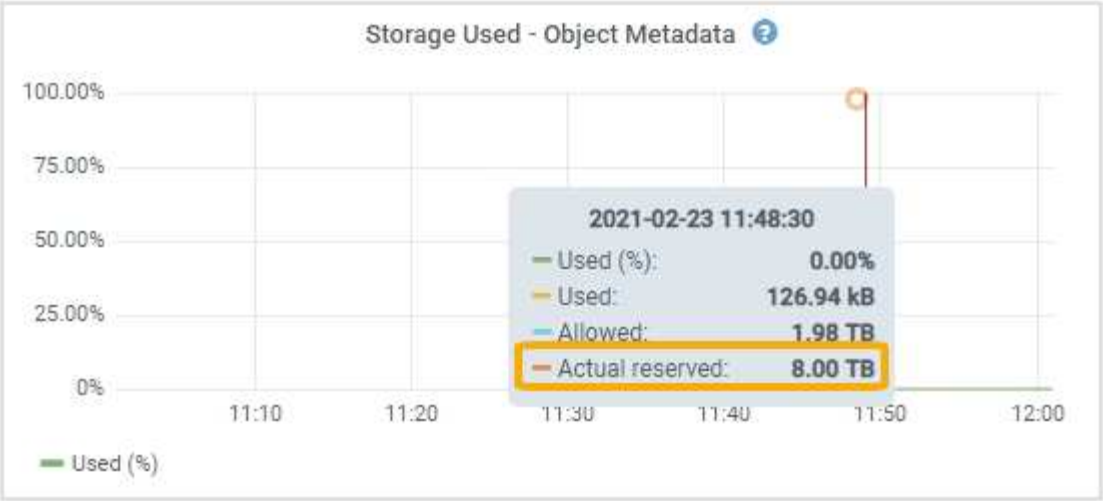
Espacio reservado real para los metadatos

A diferencia de la configuración espacio reservado de metadatos para todo el sistema, se determina el *espacio reservado real* para los metadatos del objeto para cada nodo de almacenamiento. Para un nodo de almacenamiento determinado, el espacio reservado real para los metadatos depende del tamaño del volumen 0 para el nodo y de la configuración del espacio reservado de metadatos* para todo el sistema.

El tamaño del volumen 0 para el nodo	Espacio reservado real para los metadatos
Menos de 500 GB (no uso en producción)	10% del volumen 0
500 GB o más	El menor de estos valores: • Volumen 0 • Configuración de espacio reservado de metadatos

Para ver el espacio reservado real para los metadatos en un nodo de almacenamiento determinado:

1. En Grid Manager, seleccione **NODES** > ***Storage Node***.
2. Seleccione la ficha **almacenamiento**.
3. Pase el cursor sobre el gráfico almacenamiento utilizado — metadatos de objeto y localice el valor **reservado real**.



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 la configuración de espacio reservado de metadatos para todo el sistema es menor que el volumen 0 para este nodo de almacenamiento, el espacio reservado real para este nodo es igual a la configuración de espacio reservado de metadatos.

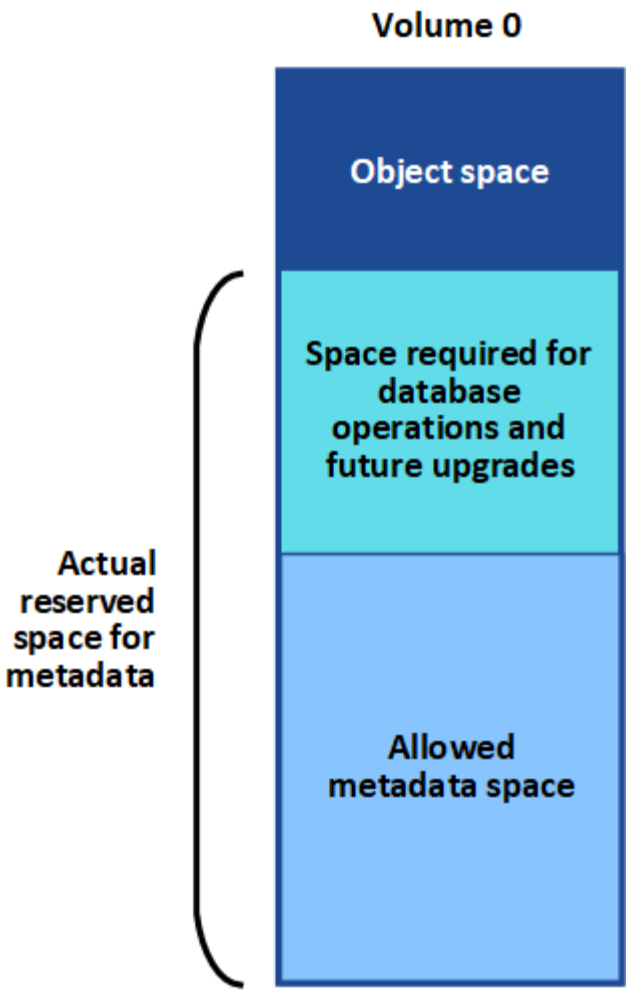
Ejemplo de espacio de metadatos reservado real

Suponga que instala un nuevo 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 de metadatos* para todo el sistema está establecido en 8 TB. (Este es el valor predeterminado para una nueva instalación de StorageGRID 11.6 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. (El volumen completo se reserva porque el volumen 0 es menor que la configuración **espacio reservado de metadatos**).

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.



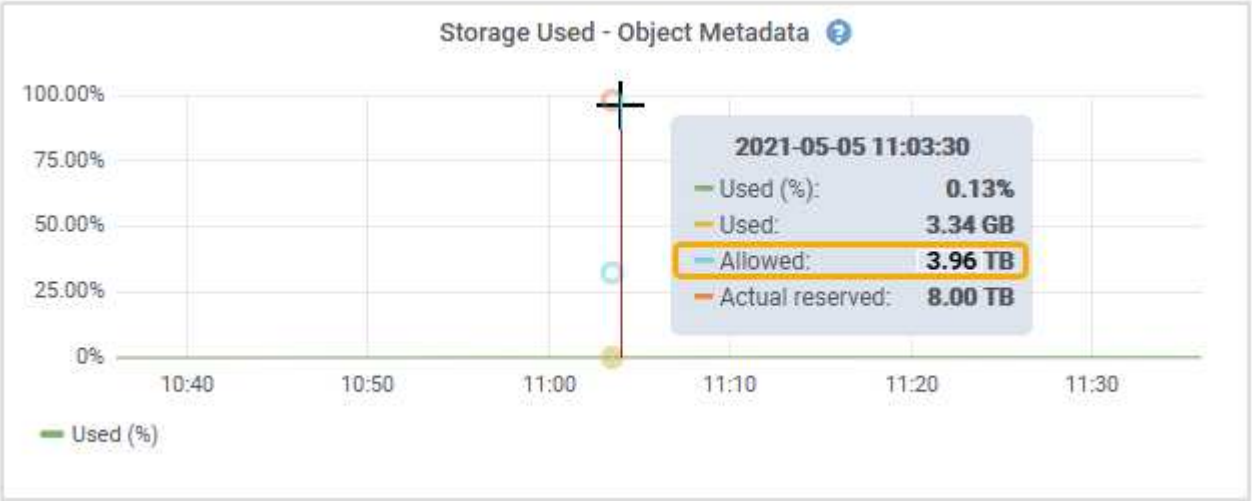
En la tabla siguiente se muestra cómo StorageGRID calcula el **espacio de metadatos permitido** para diferentes nodos de almacenamiento, en función de la cantidad de memoria del nodo y del espacio reservado real para los metadatos.

		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

Para ver el espacio de metadatos permitido para un nodo de almacenamiento:

1. En Grid Manager, seleccione **NODES**.
2. Seleccione el nodo de almacenamiento.

3. Seleccione la ficha **almacenamiento**.
4. Coloque el cursor sobre el gráfico almacenamiento usado — metadatos de objeto y busque el valor **permitido**.



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 de metadatos* para todo el sistema está establecido en 8 TB. (Este es el valor predeterminado para StorageGRID 11.6 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. (El volumen completo se reserva porque el volumen 0 es menor que la configuración **espacio reservado de metadatos**).
- 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.

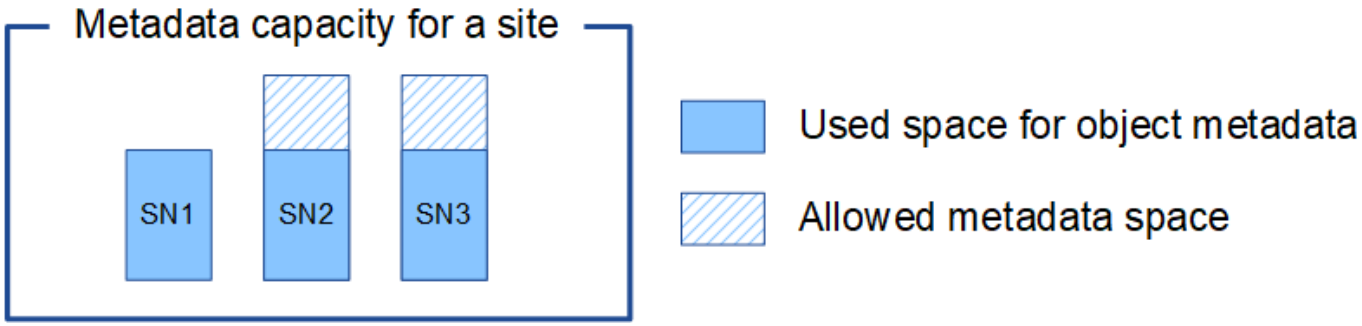
Observe el siguiente ejemplo:

- Hay una cuadrícula de un solo sitio que contiene tres nodos de almacenamiento de distintos tamaños.

- El ajuste **espacio reservado de 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 de metadatos permitidos 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 saber cómo supervisar la capacidad de metadatos de objetos para cada nodo de almacenamiento, vaya a. Supervisión y solución de problemas.
- Para aumentar la capacidad de metadatos de los objetos del sistema, añada nuevos nodos de almacenamiento. Vaya a. Amplíe su grid.

Configurar la configuración global de los objetos almacenados

Configurar la compresión de objetos almacenados

Puede utilizar la opción de cuadrícula comprimir objetos almacenados para reducir el tamaño de los objetos almacenados en StorageGRID, de modo que los objetos consuman menos espacio de almacenamiento.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

- Tiene permisos de acceso específicos.

Acerca de esta tarea

La opción de cuadrícula Compress Stored Objects está desactivada de forma predeterminada. Si habilita esta opción, StorageGRID intenta comprimir cada objeto al guardarlo utilizando una 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 esta opción, tenga en cuenta lo siguiente:

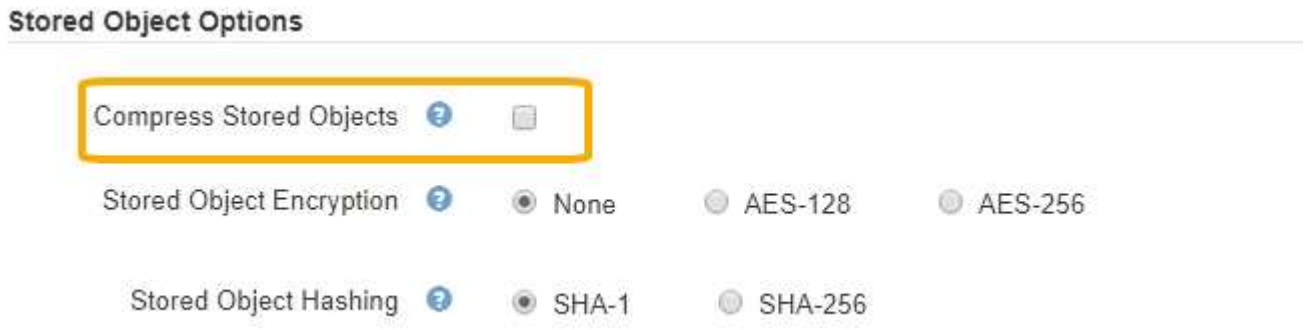
- No debe activar la compresión a menos que sepa que los datos almacenados son comprimibles.
- Las aplicaciones que guardan objetos en StorageGRID pueden comprimir objetos antes de guardarlos. Si una aplicación cliente ya ha comprimido un objeto antes de guardarlo en StorageGRID, la activación de comprimir objetos almacenados no reducirá aún más el tamaño de un objeto.
- No active la compresión si utiliza FabricPool de NetApp con StorageGRID.
- Si la opción de cuadrícula Compress Stored Objects está habilitada, las aplicaciones cliente S3 y Swift deberían evitar realizar operaciones GET Object que especifiquen un intervalo de bytes que se devolverán. Estas operaciones de «lectura de rango» son ineficientes, ya que StorageGRID debe descomprimir de forma efectiva los objetos 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 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.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de objeto almacenado , active la casilla de verificación **comprimir objetos almacenados** .



3. Seleccione **Guardar**.

Configurar el cifrado de objetos almacenados

Puede cifrar objetos almacenados si desea garantizar que los datos no se puedan recuperar de forma legible si un almacén de objetos está comprometido. De forma

predeterminada, los objetos no se cifran.

Lo que necesitará

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

Acerca de esta tarea

El cifrado de objetos almacenados permite el cifrado de todos los datos de objetos cuando se ingieren mediante S3 o Swift. 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 ingeridos no se cifran.

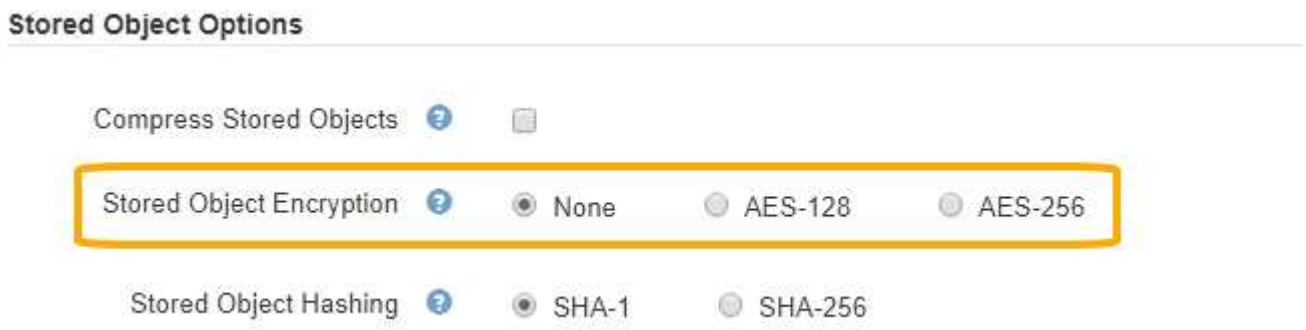
> Si cambia este ajuste, el nuevo ajuste tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para el rendimiento y el escalado.

Los objetos almacenados se pueden cifrar utilizando el algoritmo de cifrado AES-128 o AES-256.

La configuración de cifrado de objetos almacenados se aplica solo a objetos S3 que no se hayan cifrado mediante cifrado a nivel de bloque u objeto.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de objeto almacenado, cambie el cifrado de objetos almacenados a **Ninguno** (predeterminado), **AES-128** o **AES-256**.



3. Seleccione **Guardar**.

Configurar los hash de objetos almacenados

La opción de hash de objetos almacenados especifica el algoritmo de hash utilizado para verificar la integridad del objeto.

Lo que necesitará

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

Acerca de esta tarea

De forma predeterminada, los datos de objeto se procesan mediante el algoritmo SHA-1. El algoritmo SHA-256 requiere recursos de CPU adicionales y generalmente no se recomienda para la verificación de integridad.

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.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**.
2. En la sección Opciones de objeto almacenado, cambie el hash de objetos almacenados a **SHA-1** (predeterminado) o **SHA-256**.

3. Seleccione **Guardar**.

Opciones de configuración del nodo de almacenamiento

Cada nodo de almacenamiento utiliza una serie de 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.

Para acceder a las opciones de configuración y los contadores de un nodo de almacenamiento:

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 del protocolo HTTP para S3, Swift y otro tráfico interno de StorageGRID: • 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 contenido nuevo. 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.

Nombre de atributo	Codificación	Descripción
Tasa de verificación	VPRI	Establecer la velocidad a la que se realiza la verificación en segundo plano. Consulte la información sobre cómo configurar 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). Para obtener más detalles, consulte las instrucciones para supervisar y solucionar problemas de StorageGRID.
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.
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.

Nombre de atributo	Codificación	Descripción
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 deshabilitada, los objetos se pueden recuperar del nodo de almacenamiento para copiar 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 sólo lectura.
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 deshabilitada, los objetos se pueden copiar a este nodo de almacenamiento, pero no es posible recuperar objetos del nodo de almacenamiento que se van a copiar en otras ubicaciones del sistema StorageGRID. El servicio LDR es de sólo escritura.

Información relacionada

Supervisión y solución de problemas

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

Qué es un nodo de administrador

Los nodos de administración, que proporcionan servicios de gestión como configuración, supervisión y registro del sistema. Cada grid debe tener un nodo de administrador primario y puede tener cualquier cantidad de nodos de administrador no primarios por motivos de redundancia.

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, 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.

Los nodos de administración alojan los siguientes servicios:

- Servicio AMS
- Servicio CMN
- Servicio NMS
- Servicio Prometheus
- Equilibrador de carga y servicios de alta disponibilidad (para admitir el tráfico de cliente S3 y Swift)

Los nodos de administración también admiten la interfaz de programa de aplicaciones de gestión (API de gestión) para procesar las solicitudes desde la API de gestión de grid y la API de gestión de inquilinos. Consulte Utilice la API de gestión de grid.

Qué es el servicio AMS

El servicio sistema de gestión de auditorías (AMS) realiza un seguimiento de la actividad y los eventos del sistema.

En qué consiste el servicio CMN

El servicio nodo de gestión de configuración (CMN) administra las configuraciones de todo el sistema de las características de conectividad y protocolo necesarias para todos los servicios. Además, el servicio CMN se utiliza para ejecutar y supervisar tareas de cuadrícula. Solo hay un servicio CMN por instalación de StorageGRID. El nodo de administración que aloja el servicio CMN se conoce como nodo de administración principal.

Qué es el servicio NMS

El servicio sistema de administración de red (NMS) activa las opciones de supervisión, generación de informes y configuración que se muestran a través de Grid Manager, la interfaz basada en explorador del sistema StorageGRID.

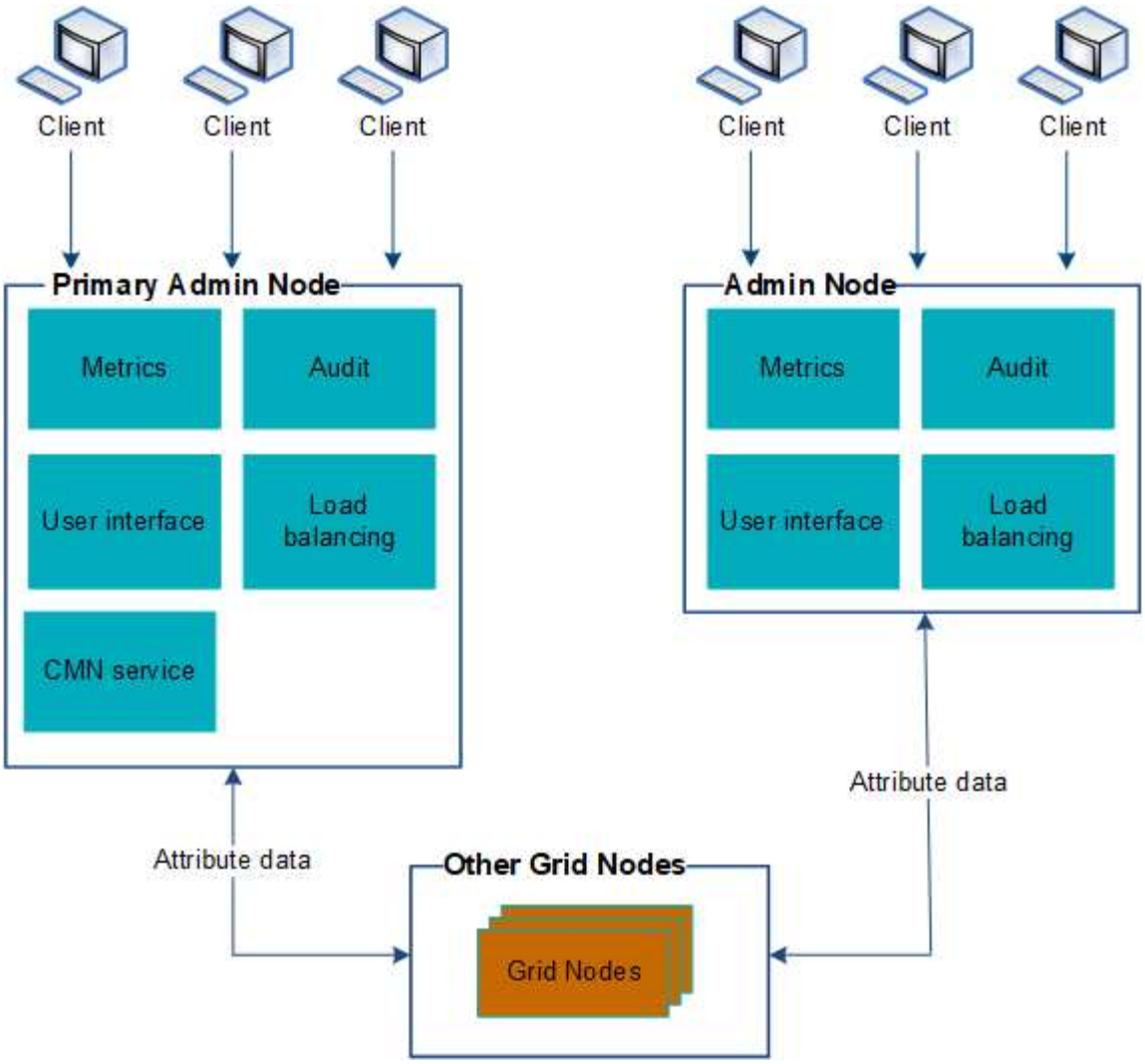
Qué es el servicio Prometheus

El servicio Prometheus recopila métricas de series temporales de los servicios de todos los nodos.

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 alarmas (sistema heredado) aún se activan y las notificaciones por correo electrónico y los mensajes de AutoSupport siguen enviados. Sin embargo, disponer de varios nodos de administrador no proporciona protección contra conmutación al nodo de respaldo, excepto notificaciones y mensajes de AutoSupport. En particular, las confirmaciones de alarma realizadas desde un nodo de administración no se copian a 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.

> Cuando se utiliza un grupo de alta disponibilidad, se interrumpe el acceso si falla el nodo de administración maestro. 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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.

Seleccione un remitente preferido

Si la implementación de StorageGRID incluye varios nodos de administrador, puede seleccionar qué nodo de administrador debe ser el remitente preferido de notificaciones. De forma predeterminada, se selecciona el nodo de administración principal, pero cualquier nodo de administración puede ser el remitente preferido.

Lo que necesitará

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

Acerca de esta tarea

La página **CONFIGURATION** > **System** > **Opciones de visualización** muestra qué nodo de administración está seleccionado actualmente para ser el emisor preferido. El nodo de administrador principal está seleccionado de forma predeterminada.

En operaciones normales del sistema, solo el remitente preferido envía las siguientes notificaciones:

- Mensajes de AutoSupport
- Notificaciones SNMP
- Mensajes de correo electrónico de alerta
- Correos electrónicos de alarma (sistema heredado)

Sin embargo, todos los demás nodos de administración (remitentes en espera) supervisan al remitente preferido. Si se detecta un problema, un remitente en espera también puede enviar estas notificaciones.

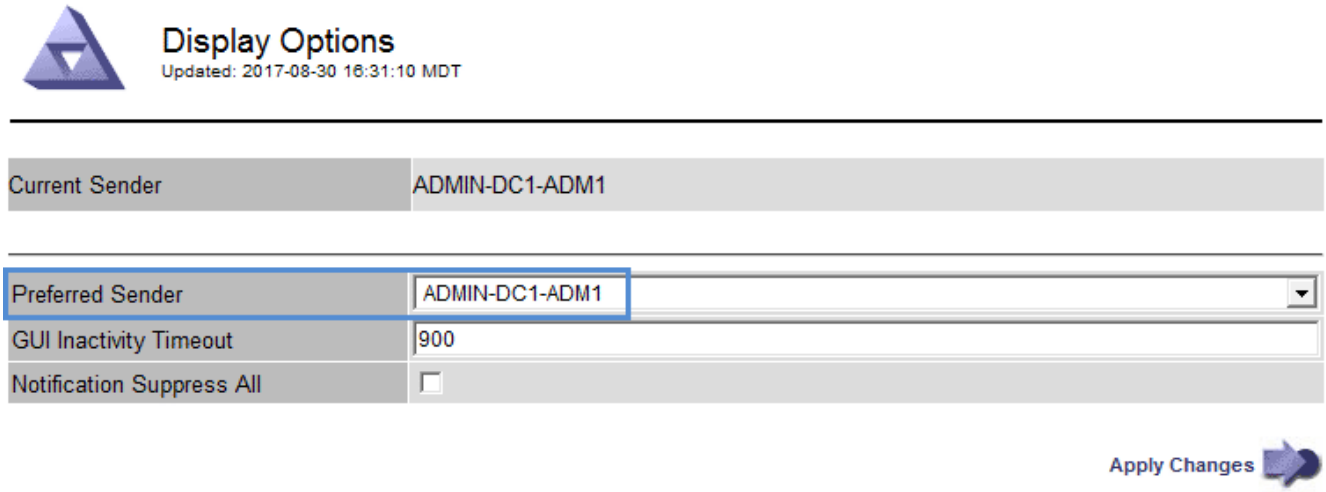
Tanto el remitente preferido como el remitente en espera pueden enviar notificaciones en los siguientes casos:

- Si los nodos de administración se convierten en "'desembarcados'" entre sí, tanto el remitente preferido como los remitentes en espera intentarán enviar notificaciones, y pueden recibirse varias copias de las notificaciones.
- Después de que un remitente en espera detecta problemas con el remitente preferido y comienza a enviar notificaciones, es posible que el remitente preferido recupere su capacidad de 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 notificaciones de alarma y mensajes de AutoSupport, todos los nodos administrador envían el correo electrónico de prueba. Cuando prueba las notificaciones de alerta, debe iniciar sesión en cada nodo de administrador para verificar la conectividad.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de pantalla**.
2. En el menú Opciones de pantalla, seleccione **Opciones**.
3. Seleccione el nodo de administración que desea establecer como remitente preferido de la lista desplegable.



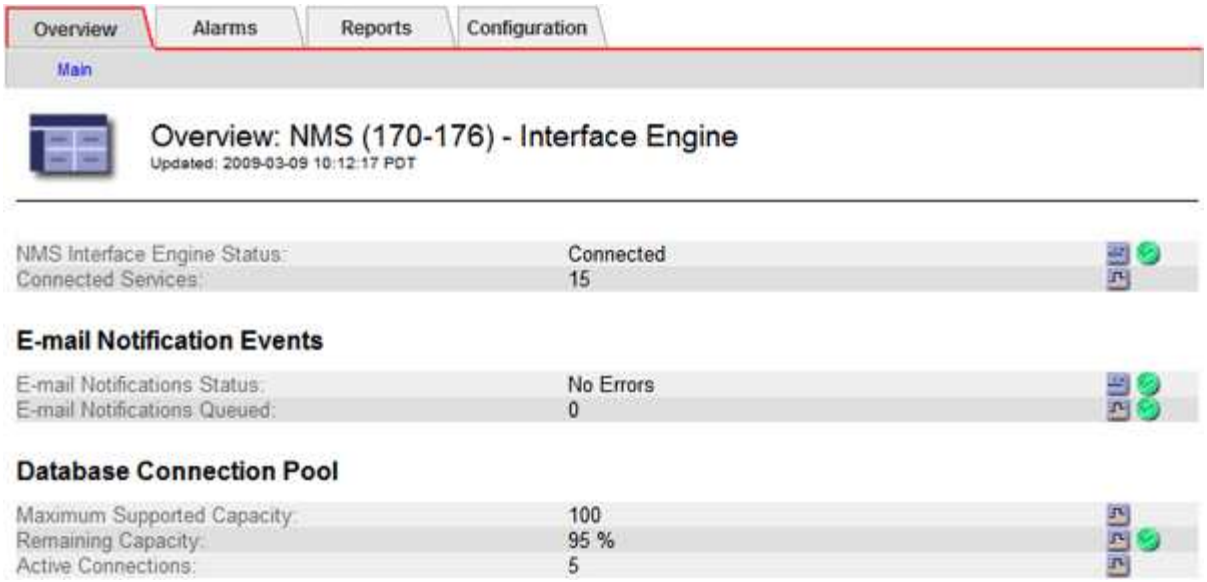
4. Seleccione **aplicar cambios**.

   El nodo de administrador se establece como el remitente preferido de notificaciones.

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**.

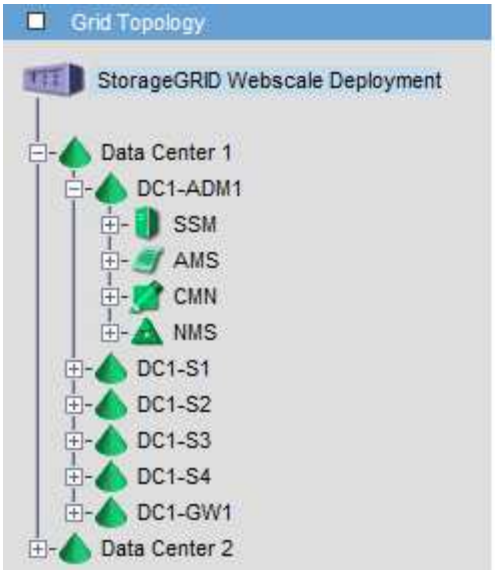


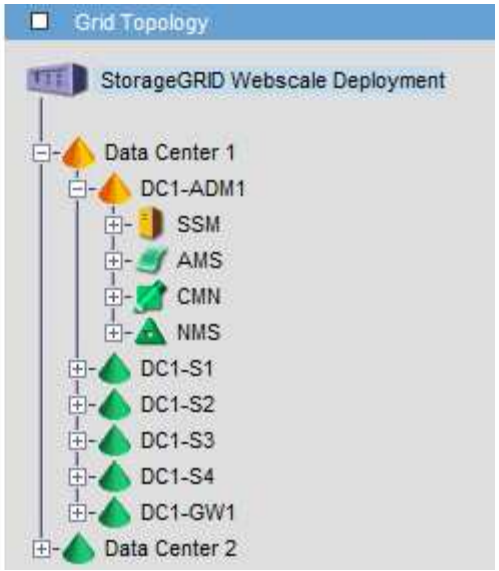
Las notificaciones se procesan a través de la cola de notificaciones de correo electrónico y se envían al servidor de correo una tras otra en el orden en que se activan. Si hay un problema (por ejemplo, un error de conexión de red) y el servidor de correo no está disponible cuando se intenta enviar la 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. En el caso de que una notificación se descarta de la cola sin enviarse, se activa la alarma Minor DE MINUTOS (Estado de notificación por 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. Debido a que las confirmaciones no se copian en otros nodos de administración, es posible que el árbol de topología de cuadrícula no tenga 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

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. Para facilitar el acceso a los registros de auditoría, puede configurar el acceso de los clientes a recursos compartidos de auditoría de CIFS y NFS.

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.

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID. Si dispone de la opción de utilizar CIFS o NFS, elija NFS.

Configurar clientes de auditoría para CIFS

El procedimiento utilizado para configurar un cliente de auditoría depende del método de autenticación: Windows Workgroup o Windows Active Directory (AD). Cuando se añade, el recurso compartido de auditoría se habilita automáticamente como un recurso compartido de solo lectura.

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

Configurar clientes de auditoría para Workgroup

Realice este procedimiento para cada nodo de administrador en una implementación de StorageGRID desde la que desea recuperar mensajes de auditoría.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

Acerca de esta tarea

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

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: `storagegrid-status`

   Si todos los servicios no están en ejecución ni verificados, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos y pulse **Ctrl+C**.
4. Inicie la utilidad de configuración CIFS: `config_cifs.rb`

```
----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
----------------------------------------------------------------------
```

5. Establezca la autenticación para el grupo de trabajo de Windows:

   Si ya se ha establecido la autenticación, aparece un mensaje de aviso. Si ya se ha configurado la autenticación, vaya al paso siguiente.

   a. Introduzca: `set-authentication`
   b. Cuando se le solicite la instalación de Windows Workgroup o Active Directory, introduzca: `workgroup`
   c. Cuando se le solicite, escriba un nombre del grupo de trabajo: *`workgroup_name`*

d. Cuando se le solicite, cree un nombre NetBIOS significativo: *netbios_name*

   o.

   Pulse **Intro** para utilizar el nombre de host del nodo de administración como nombre NetBIOS.

La secuencia de comandos reinicia el servidor Samba y se aplican los cambios. Esto debería tardar menos de un minuto. Después de establecer la autenticación, agregue un cliente de auditoría.

a. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de CIFS.

6. Agregar un cliente de auditoría:

   a. Introduzca: `add-audit-share`

      El recurso compartido se añade automáticamente como de solo lectura.

   b. Cuando se le solicite, agregue un usuario o grupo: *user*
   c. Cuando se le solicite, introduzca el nombre de usuario de auditoría: *audit_user_name*
   d. Cuando se le solicite, escriba una contraseña para el usuario de auditoría: *password*
   e. Cuando se le solicite, vuelva a introducir la misma contraseña para confirmarla: *password*
   f. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de CIFS.

      No es necesario introducir un directorio. El nombre del directorio de auditoría está predefinido.

7. Si se permite que más de un usuario o grupo acceda al recurso compartido de auditoría, agregue los usuarios adicionales:

   a. Introduzca: `add-user-to-share`

      Se muestra una lista numerada de los recursos compartidos habilitados.

   b. Cuando se le solicite, escriba el número del recurso compartido auditoría-exportación: *share_number*
   c. Cuando se le solicite, agregue un usuario o grupo: `user`

      1. `group`

   d. Cuando se le solicite, introduzca el nombre del usuario o grupo de auditoría: *audit_user or audit_group*
   e. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de CIFS.

   f. Repita estos subpasos para cada usuario o grupo adicional que tenga acceso al recurso compartido de auditoría.

8. Si lo desea, compruebe la configuración: `validate-config`

Los servicios se comprueban y visualizan. Puede ignorar con toda tranquilidad los siguientes mensajes:

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. Cuando se le solicite, pulse **Intro**.

   Se muestra la configuración del cliente de auditoría.

b. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de CIFS.

9. Cierre la utilidad de configuración CIFS: `exit`
10. Inicie el servicio Samba: `service smbd start`
11. Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.

    o.

    De manera opcional, si la implementación de StorageGRID incluye nodos de administración en otros sitios, habilite este recurso compartido 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 los pasos para configurar el recurso compartido 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`
12. Cierre la sesión del shell de comandos: `exit`

Configurar clientes de auditoría para Active Directory

Realice este procedimiento para cada nodo de administrador en una implementación de StorageGRID desde la que desea recuperar mensajes de auditoría.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Tiene el nombre de usuario y la contraseña de CIFS Active Directory.

- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

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: `storagegrid-status`

   Si todos los servicios no están en ejecución ni verificados, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos y pulse **Ctrl+C**.
4. Inicie la utilidad de configuración CIFS: `config_cifs.rb`

```
----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
----------------------------------------------------------------------
```

5. Establezca la autenticación de Active Directory: `set-authentication`

   En la mayoría de las implementaciones, debe establecer la autenticación antes de agregar el cliente de auditoría. Si ya se ha establecido la autenticación, aparece un mensaje de aviso. Si ya se ha configurado la autenticación, vaya al paso siguiente.

   a. Cuando se le solicite la instalación de Workgroup o Active Directory: `ad`
   b. Cuando se le solicite, escriba el nombre del dominio de AD (nombre de dominio corto).
   c. Cuando se le solicite, introduzca la dirección IP o el nombre de host DNS del controlador de dominio.
   d. Cuando se le solicite, escriba el nombre completo del dominio.

      Utilice letras mayúsculas.

e. Cuando se le solicite que habilite el soporte winbind, escriba **y**.

   Winbind se utiliza para resolver la información de usuarios y grupos desde los servidores AD.

f. Cuando se le solicite, introduzca el nombre NetBIOS.

g. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de CIFS.

6. Únase al dominio:

   a. Si no se ha iniciado todavía, inicie la utilidad de configuración de CIFS: `config_cifs.rb`

   b. Únase al dominio: `join-domain`

   c. Se le solicitará que pruebe si el nodo de administración es actualmente un miembro válido del dominio. Si este nodo de administrador no se ha Unido previamente al dominio, introduzca: `no`

   d. Cuando se le solicite, indique el nombre de usuario del administrador: *`administrator_username`*

      donde *`administrator_username`* Es el nombre de usuario de CIFS Active Directory, no el de StorageGRID.

   e. Cuando se le solicite, proporcione la contraseña del administrador: *`administrator_password`*

      lo eran *`administrator_password`* Es el nombre de usuario de CIFS Active Directory, no la contraseña de StorageGRID.

   f. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de CIFS.

7. Compruebe que se ha Unido correctamente al dominio:

   a. Únase al dominio: `join-domain`

   b. Cuando se le solicite que compruebe si el servidor es actualmente un miembro válido del dominio, especifique: `y`

      Si recibe el mensaje "'Join is OK,'" se ha Unido correctamente al dominio. Si no obtiene esta respuesta, intente configurar la autenticación y unirse al dominio de nuevo.

   c. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de CIFS.

8. Agregar un cliente de auditoría: `add-audit-share`

   a. Cuando se le solicite agregar un usuario o grupo, escriba: `user`

   b. Cuando se le solicite que introduzca el nombre de usuario de auditoría, introduzca el nombre de usuario de auditoría.

   c. Cuando se le solicite, pulse **Intro**.

      Aparece la utilidad de configuración de CIFS.

9. Si se permite que más de un usuario o grupo acceda al recurso compartido de auditoría, agregue usuarios

adicionales: `add-user-to-share`

Se muestra una lista numerada de los recursos compartidos habilitados.

a. Introduzca el número del recurso compartido auditoría-exportación.
b. Cuando se le solicite agregar un usuario o grupo, escriba: `group`

   Se le solicitará el nombre del grupo de auditoría.

c. Cuando se le solicite el nombre del grupo de auditoría, introduzca el nombre del grupo de usuarios de auditoría.
d. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de CIFS.

e. Repita este paso con cada usuario o grupo adicional que tenga acceso al recurso compartido de auditoría.

10. Si lo desea, compruebe la configuración: `validate-config`

    Los servicios se comprueban y visualizan. Puede ignorar con toda tranquilidad los siguientes mensajes:

    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-interfaces.inc`
    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-filesystem.inc`
    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-interfaces.inc`
    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-custom-config.inc`
    - No se encuentra el archivo de inclusión `/etc/samba/includes/cifs-shares.inc`
    - Rlimit_max: Aumentando rlimit_max (1024) al límite mínimo de Windows (16384)

    > No combine la configuración 'Security=ADS' con el parámetro 'Password Server'. (Por defecto Samba descubrirá el DC correcto para contactar automáticamente).

    i. Cuando se le solicite, pulse **Intro** para mostrar la configuración del cliente de auditoría.
    ii. Cuando se le solicite, pulse **Intro**.

       Aparece la utilidad de configuración de CIFS.

11. Cierre la utilidad de configuración CIFS: `exit`
12. Si la implementación de StorageGRID es un solo sitio, vaya al paso siguiente.

    o.

    De manera opcional, si la implementación de StorageGRID incluye nodos de administración en otros sitios, habilite 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 seguro remoto en Admin Node: `exit`

13. Cierre la sesión del shell de comandos: `exit`

Añada un usuario o un grupo a un recurso compartido de auditoría CIFS

Es posible añadir un usuario o un grupo a un recurso compartido de auditoría CIFS que esté integrado con la autenticación de AD.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

Acerca de esta tarea

El siguiente procedimiento es para un recurso compartido de auditoría integrado con la autenticación AD.

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

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 todos los servicios no están en ejecución ni verificados, resuelva los problemas antes de continuar.

3. Vuelva a la línea de comandos y pulse **Ctrl+C**.

4. Inicie la utilidad de configuración CIFS: `config_cifs.rb`

```
-----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-----------------------------------------------------------------------
```

5. Comenzar a agregar un usuario o grupo: `add-user-to-share`

   Se muestra una lista numerada de los recursos compartidos de auditoría configurados.

6. Cuando se le solicite, introduzca el número del recurso compartido de auditoría (auditoría-exportación): *`audit_share_number`*

   Se le preguntará si desea proporcionar a un usuario o grupo acceso a este recurso compartido de auditoría.

7. Cuando se le solicite, agregue un usuario o grupo: `user` o. `group`
8. Cuando se le solicite el nombre de usuario o grupo para este recurso compartido de auditoría de AD, escriba el nombre.

   El usuario o grupo se agrega como de solo lectura para el recurso compartido de auditoría tanto en el sistema operativo del servidor como en el servicio CIFS. La configuración de Samba se vuelve a cargar para permitir al usuario o grupo acceder al recurso compartido del cliente de auditoría.

9. Cuando se le solicite, pulse **Intro**.

   Aparece la utilidad de configuración de CIFS.

10. Repita estos pasos para cada usuario o grupo que tenga acceso al recurso compartido de auditoría.
11. Si lo desea, compruebe la configuración: `validate-config`

    Los servicios se comprueban y visualizan. Puede ignorar con toda tranquilidad los siguientes mensajes:

    - No se puede encontrar el archivo /etc/samba/includes/cifs-interfaces.inc.
    - No se puede encontrar el archivo /etc/samba/includes/cifs-filesystem.inc.
    - No se puede encontrar el archivo /etc/samba/includes/cifs-custom-config.inc.
    - No se puede encontrar el archivo /etc/samba/includes/cifs-shares.inc.
      i. Cuando se le solicite, pulse **Intro** para mostrar la configuración del cliente de auditoría.
      ii. Cuando se le solicite, pulse **Intro**.

12. Cierre la utilidad de configuración CIFS: `exit`

13. Determine si necesita habilitar recursos compartidos de auditoría adicionales, de la siguiente forma:
    - 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 de un 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.
        iii. Cierre el inicio de sesión de la shell segura remota en el nodo de administración remota: `exit`
14. Cierre la sesión del shell de comandos: `exit`

Quitar un usuario o un grupo de un recurso compartido de auditoría CIFS

No se puede eliminar el último usuario o grupo permitido para acceder al recurso compartido de auditoría.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con las contraseñas de la cuenta raíz (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

Acerca de esta tarea

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

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 CIFS: `config_cifs.rb`

```
-----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-----------------------------------------------------------------------
```

3. Comience a eliminar un usuario o grupo: `remove-user-from-share`

   Se muestra una lista numerada de los recursos compartidos de auditoría disponibles para el nodo de administración. El recurso compartido de auditoría se etiqueta audit-export.

4. Introduzca el número del recurso compartido de auditoría: *`audit_share_number`*
5. Cuando se le solicite que elimine un usuario o un grupo: `user` o. `group`

   Se muestra una lista numerada de usuarios o grupos para el recurso compartido de auditoría.

6. Introduzca el número correspondiente al usuario o grupo que desea eliminar: *`number`*

   Se actualiza el recurso compartido de auditoría y el usuario o grupo ya no tiene permiso de acceso al recurso compartido de auditoría. Por ejemplo:

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Cierre la utilidad de configuración CIFS: `exit`
8. Si la implementación de StorageGRID incluye nodos de administración en otros sitios, deshabilite el recurso compartido de auditoría en cada sitio según sea necesario.
9. Cierre la sesión de cada shell de comando cuando la configuración se haya completado: `exit`

Cambiar un nombre de usuario o de grupo de recurso compartido de auditoría CIFS

Es posible cambiar el nombre de un usuario o de un grupo de un recurso compartido de auditoría de CIFS. Para ello, añada un nuevo usuario o grupo y, a continuación, elimine el anterior.

Acerca de esta tarea

La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

Pasos

1. Agregue un nuevo usuario o grupo con el nombre actualizado al recurso compartido de auditoría.
2. Elimine el nombre de usuario o grupo anterior.

Información relacionada

- Añada un usuario o un grupo a un recurso compartido de auditoría CIFS
- Quitar un usuario o un grupo de un recurso compartido de auditoría CIFS

Compruebe la integración de la auditoría de CIFS

El recurso compartido de auditoría es de solo lectura. Los archivos de registro están diseñados para que los lean las aplicaciones del equipo y la verificación no incluye abrir un archivo. Se considera suficiente verificación de que los archivos de registro de auditoría aparecen en una ventana del Explorador de Windows. Tras la verificación de la conexión, cierre todas las ventanas.

Configurar el cliente de auditoría para NFS

El recurso compartido de auditoría se habilita automáticamente como recurso compartido de solo lectura.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con la contraseña root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).
- 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.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).
- 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/audit/export`

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.

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 comando de Linux de ejemplo es (introduzca en una línea):

   `mount -t nfs -o hard,intr` *`Admin_Node_IP_address`*`:/var/local/audit/export` *`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.

Lo que necesitará

- Usted tiene la `Passwords.txt` Archivo con la contraseña de la cuenta root/admin (disponible en DICHO paquete).
- Usted tiene la `Configuration.txt` Archivo (disponible en DICHO paquete).

Acerca de esta tarea

No se 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/audit/export`

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

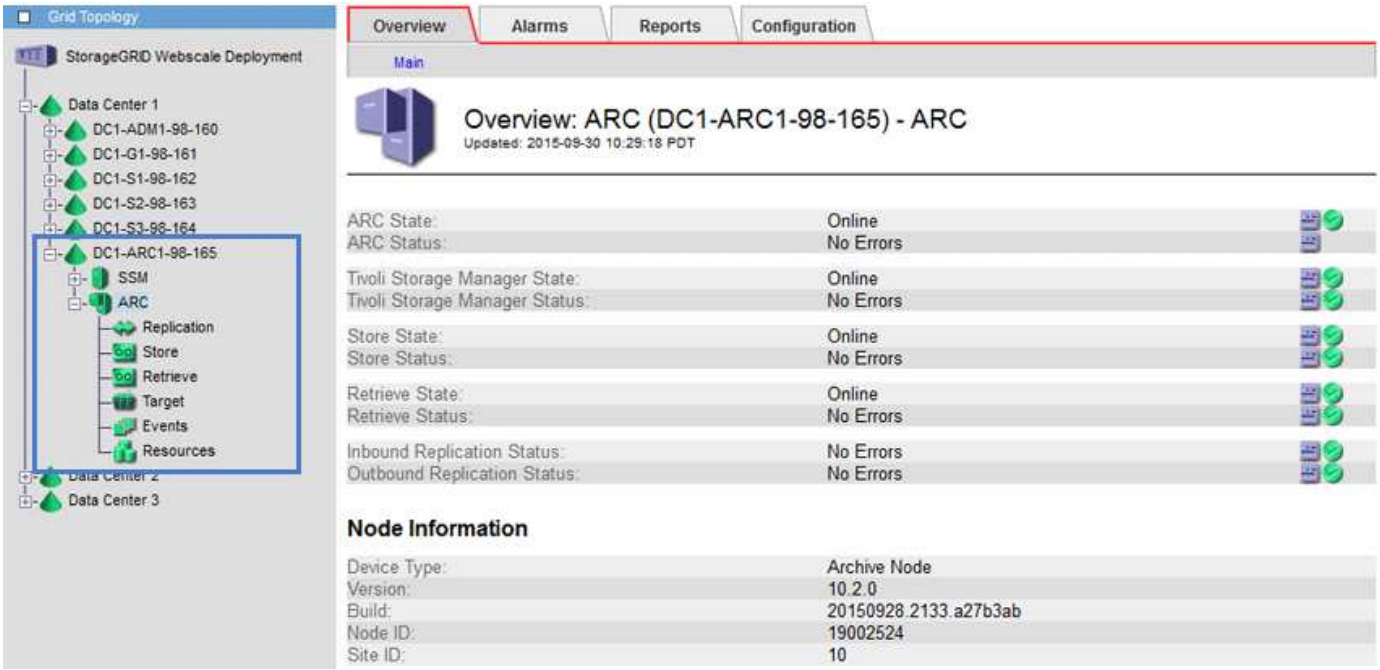
- Agregar un cliente de auditoría NFS a un recurso compartido de auditoría
- Eliminar un cliente de auditoría NFS del recurso compartido de auditoría

Gestione los nodos de archivado

Qué es un nodo de archivado

Opcionalmente, cada sitio del centro de datos StorageGRID se puede poner en marcha con un nodo de archivado, que permite conectarse a un sistema de almacenamiento de archivado externo específico, como Tivoli Storage Manager (TSM).

El nodo de archivado proporciona una interfaz a través de la cual se puede dirigir un sistema de almacenamiento de archivado externo para el almacenamiento a largo plazo de datos de objetos. El nodo de archivado también supervisa esta conexión y la transferencia de datos de objeto entre el sistema StorageGRID y el sistema de almacenamiento de archivado externo objetivo.



Después de configurar las conexiones con el destino externo, puede configurar el nodo de archivado para optimizar el rendimiento de TSM, desconectar un nodo de archivado cuando un servidor TSM se acerca a la

capacidad o no está disponible y configurar la configuración de replicación y recuperación. También puede establecer alarmas personalizadas para el nodo de archivado.

Los datos de objetos que no se pueden eliminar, pero a los que no se tiene acceso regularmente, se pueden trasladar en cualquier momento fuera de los discos giratorios de un nodo de almacenamiento y a un almacenamiento de archivado externo, como el cloud o la cinta. Este archivado de los datos de objetos se realiza mediante la configuración del nodo de archivado del sitio del centro de datos y, a continuación, con la configuración de las reglas de ILM donde este nodo de archivado se selecciona como el "destino" para obtener instrucciones de colocación de contenido. El nodo de archivado no gestiona los propios datos de objetos archivados, lo consigue el dispositivo de archivado externo.

> Los metadatos de objetos no se archivan, pero siguen en los nodos de almacenamiento.

Qué es el servicio ARC

El servicio de archivado (ARC) en nodos de archivado ofrece la interfaz de gestión que se puede utilizar para configurar conexiones a almacenamiento de archivado externo, como la cinta, a través de middleware TSM.

Se trata del servicio de ARC que interactúa con un sistema de almacenamiento de archivado externo, por lo que envía datos de objetos para almacenamiento near-line y realiza recuperaciones cuando una aplicación cliente solicita un objeto archivado. Cuando una aplicación cliente solicita un objeto archivado, un nodo de almacenamiento solicita los datos del objeto del servicio ARC. El servicio ARC realiza una solicitud al sistema de almacenamiento de archivos externo, que recupera los datos de objeto solicitados y los envía al servicio ARC. El servicio ARC verifica los datos del objeto y los reenvía al nodo de almacenamiento, que a su vez devuelve el objeto a la aplicación cliente solicitante.

Las solicitudes de datos de objetos archivados a cinta mediante TSM Middleware se gestionan por la eficiencia de las recuperaciones. Las solicitudes se pueden solicitar para que los objetos almacenados en orden secuencial en la cinta se soliciten en el mismo orden secuencial. A continuación, las solicitudes se colocan en la cola de espera para su envío al dispositivo de almacenamiento. En función del dispositivo de archivado, se pueden procesar simultáneamente varias solicitudes de objetos en diferentes volúmenes.

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.

> 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)** sigue siendo compatible, pero puede que prefiera implementar Cloud Storage Pools en su lugar.

Si actualmente utiliza un nodo de archivado con la opción **Cloud Tiering - simple Storage Service (S3)**, considere la posibilidad de migrar los objetos a un grupo de almacenamiento en cloud. Consulte las instrucciones para Gestión de objetos con 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.

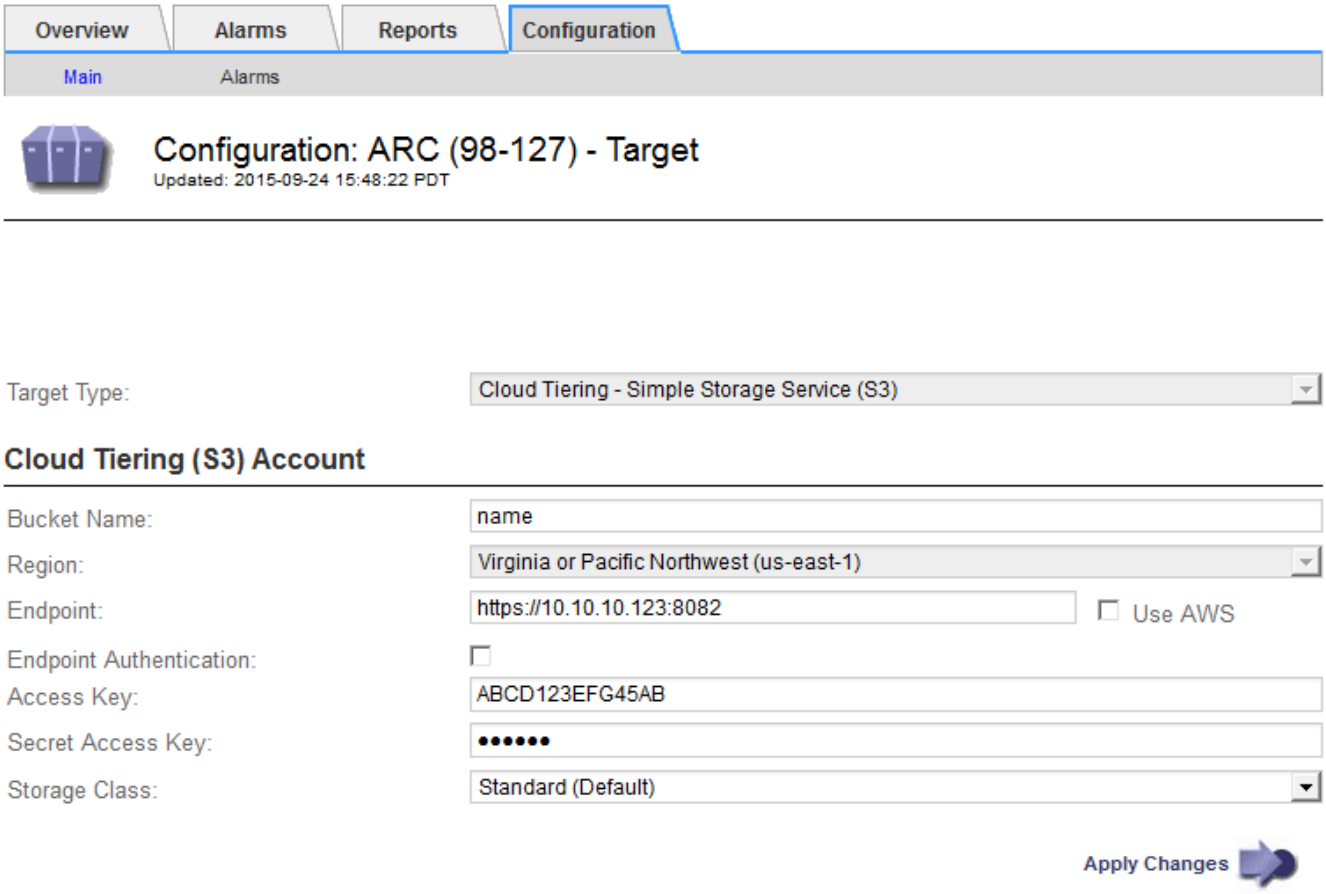
> El traslado de objetos de un nodo de archivado a un sistema de almacenamiento de archivado externo a través de la API de S3 ha sido sustituido por los pools de almacenamiento en cloud de ILM, que ofrecen más funcionalidades. La opción **Cloud Tiering - simple Storage Service (S3)** sigue siendo compatible, pero puede que prefiera implementar Cloud Storage Pools en su lugar.
>
> Si actualmente utiliza un nodo de archivado con la opción **Cloud Tiering - simple Storage Service (S3)**, considere la posibilidad de migrar los objetos a un grupo de almacenamiento en cloud. Consulte Gestión de objetos con ILM.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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 utilizarlo otros nodos de archivado ni 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 anular la selección de la casilla de verificación para deshabilitar la verificación de nombre de host y certificado SSL de punto final 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 seleccionada la casilla de verificación.

- **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. Una vez que se configura, 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.

Lo que necesitará

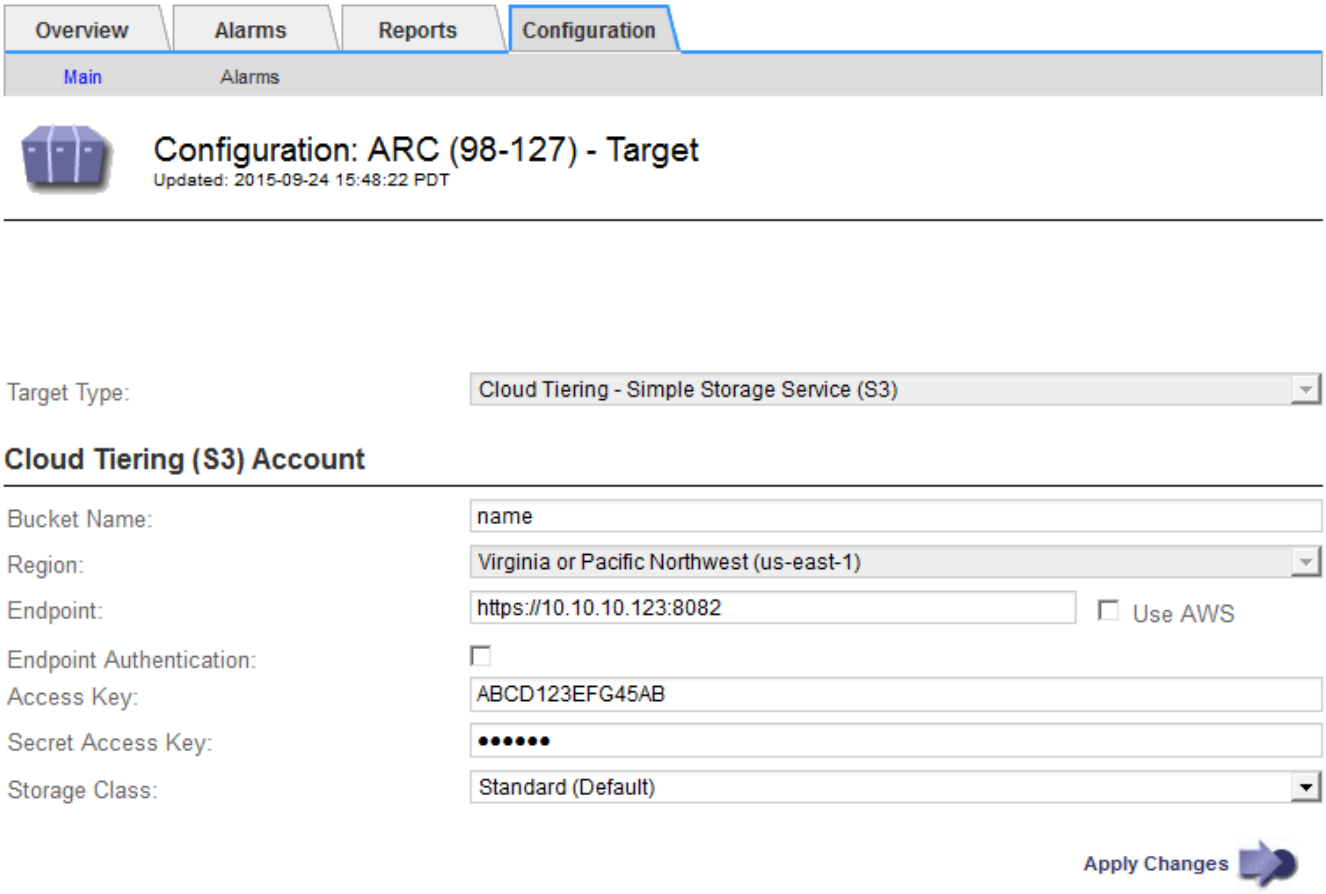
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

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 extremo, utilice los 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.

Lo que necesitará

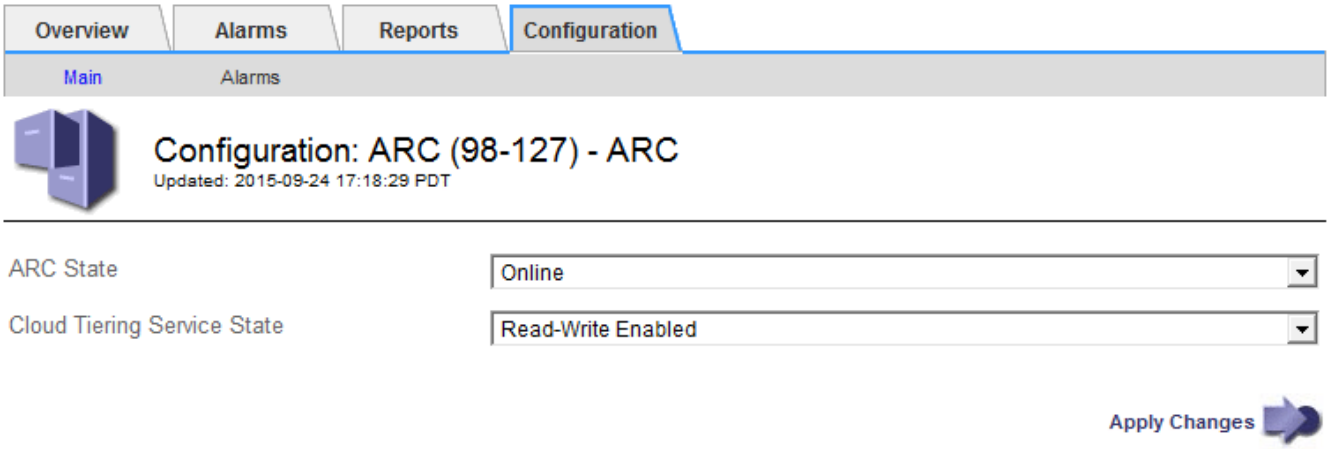
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener permisos de acceso específicos.
- Debe configurarse el nodo de archivado.

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

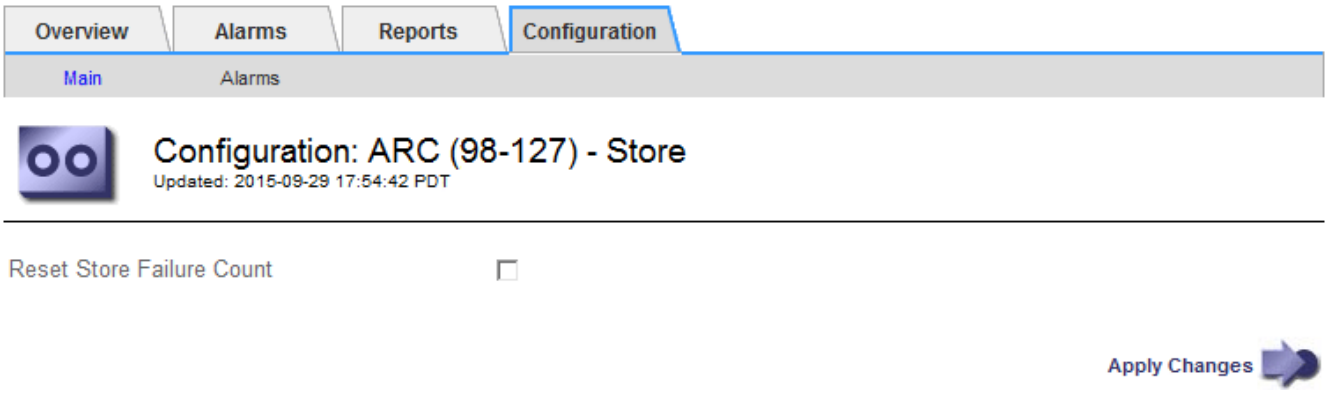
Si el nodo de archivado se conecta a un sistema de almacenamiento de archivado a través de la API de S3, puede restablecer el recuento de fallos de almacenamiento, que se puede utilizar para borrar la alarma de ARVF (fallos de almacenamiento).

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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 utiliza la función **Cloud Tiering - simple Storage Service (S3)** para organizar los datos de objetos en niveles en un bloque de S3, considere la posibilidad de 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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 dichos 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. Ubique cualquier regla de ILM en la política activa de ILM que provoque que los objetos se almacenen en el bloque de niveles del cloud.
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.

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).

Configurar conexiones al middleware TSM

Antes de que el nodo de archivado pueda comunicarse con el middleware Tivoli Storage Manager (TSM), debe configurar una serie de opciones.

Lo que necesitará

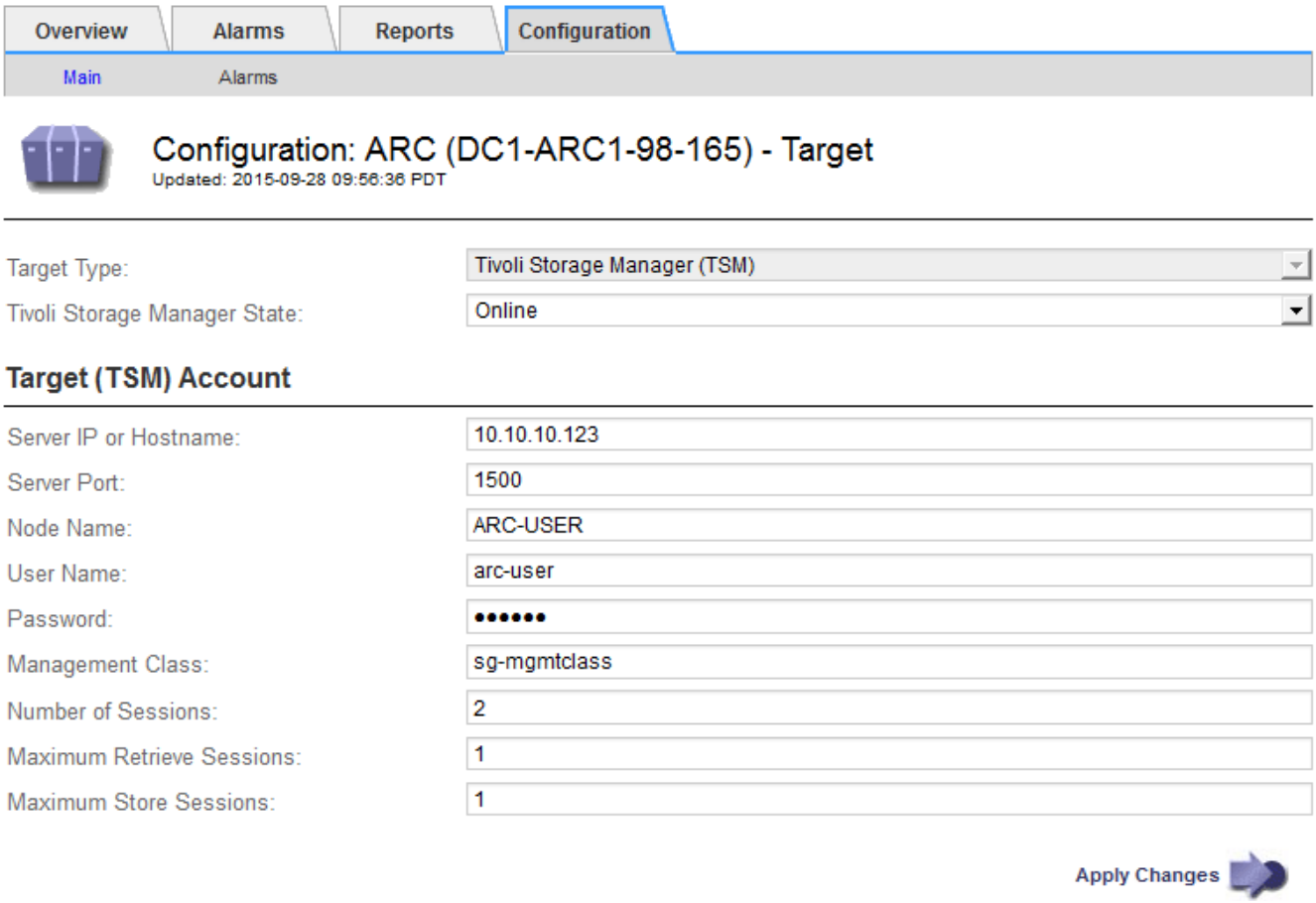
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

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.

Lo que necesitará

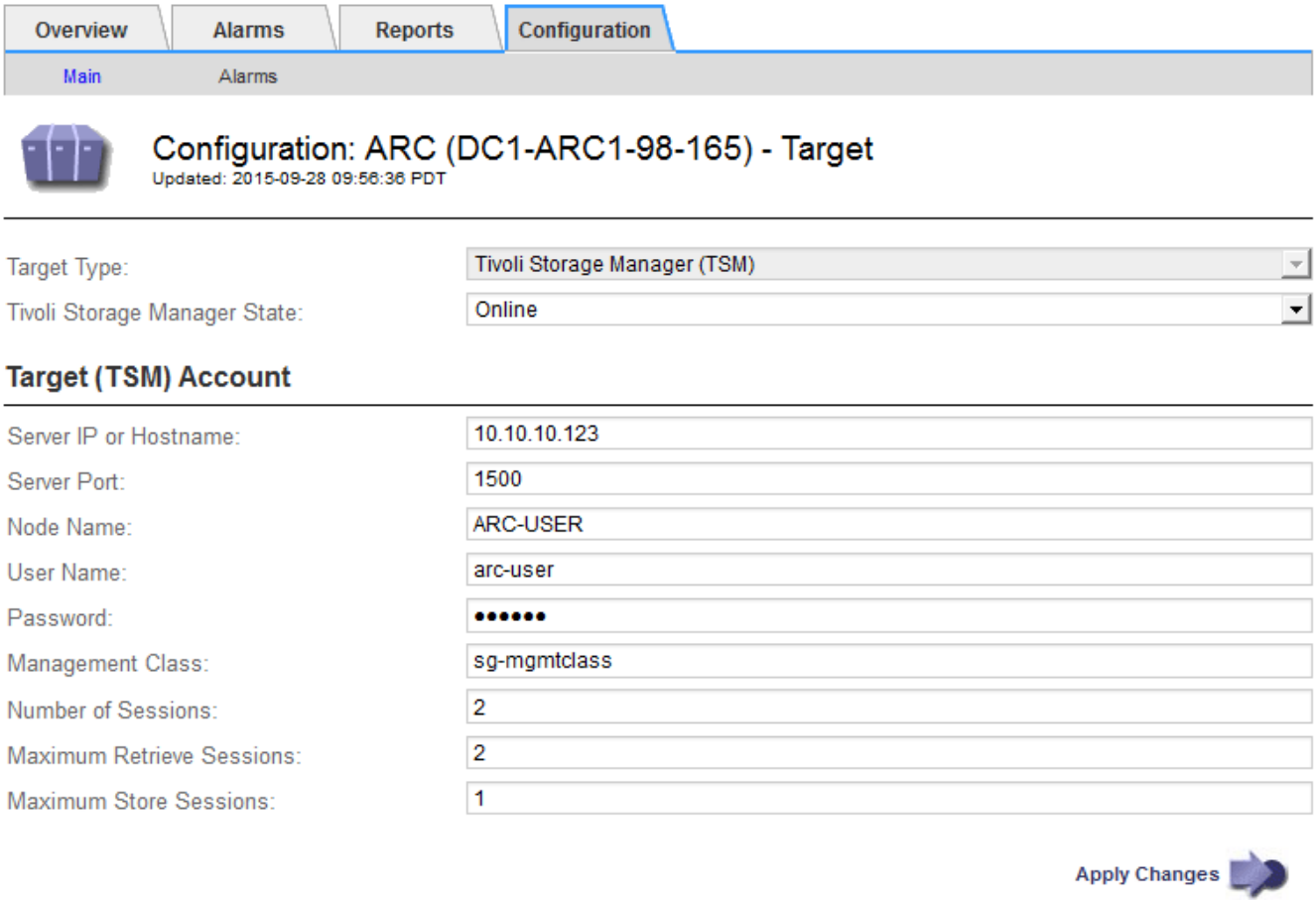
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.

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.

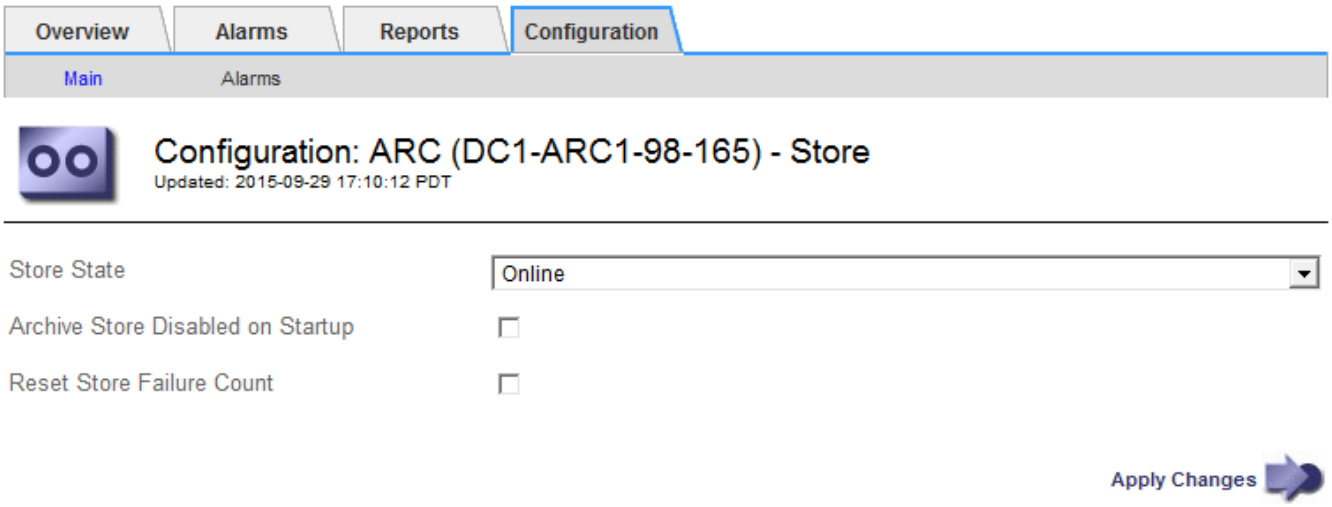
Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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.

Lo que necesitará

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

Acerca de esta tarea

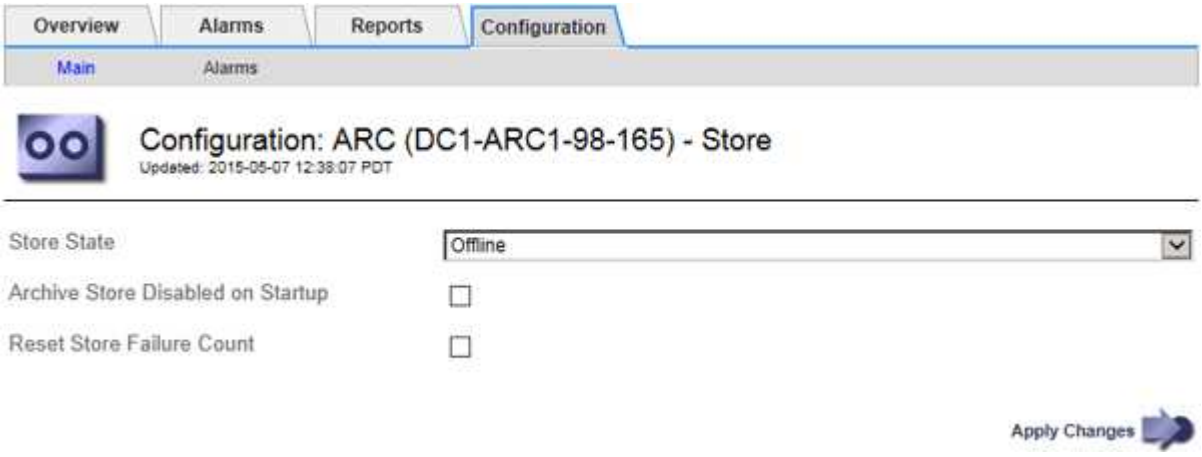
El nodo de archivado continúa aceptando datos de objetos para su transferencia al servidor TSM una vez que el servidor TSM deja de aceptar contenido nuevo. Este contenido no se puede escribir en medios gestionados por el servidor TSM. Si esto ocurre, se activa una alarma.

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

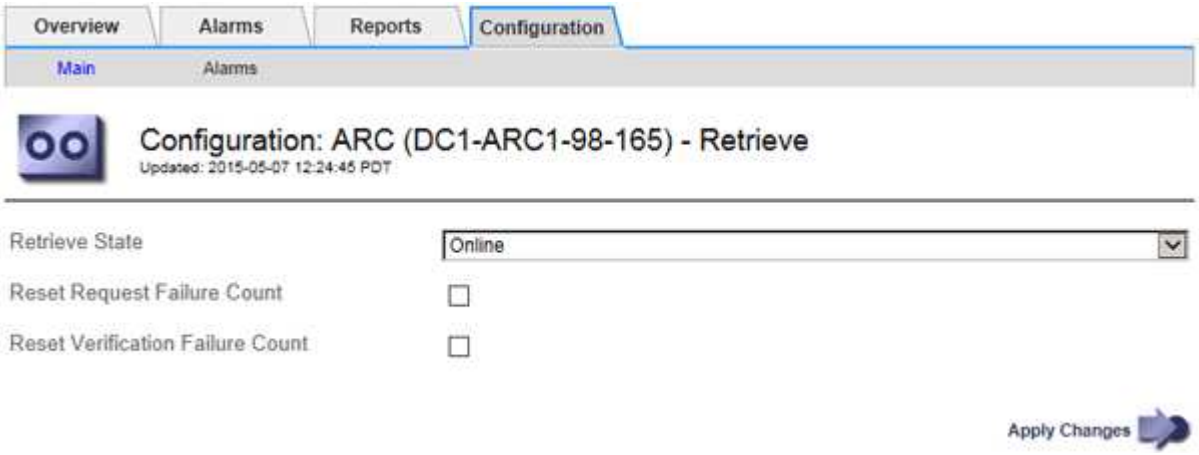
estado en línea o sin conexión, o restablecer los recuentos de fallos que se van a realizar el seguimiento de las alarmas asociadas.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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 verificación para restablecer el contador en caso 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 en busca de fallos de verificación en los datos del objeto recuperado. Esto se puede utilizar para borrar la alarma ARRV (fallos de verificación).
5. Seleccione **aplicar cambios**.

Configure la replicación del nodo de archivado

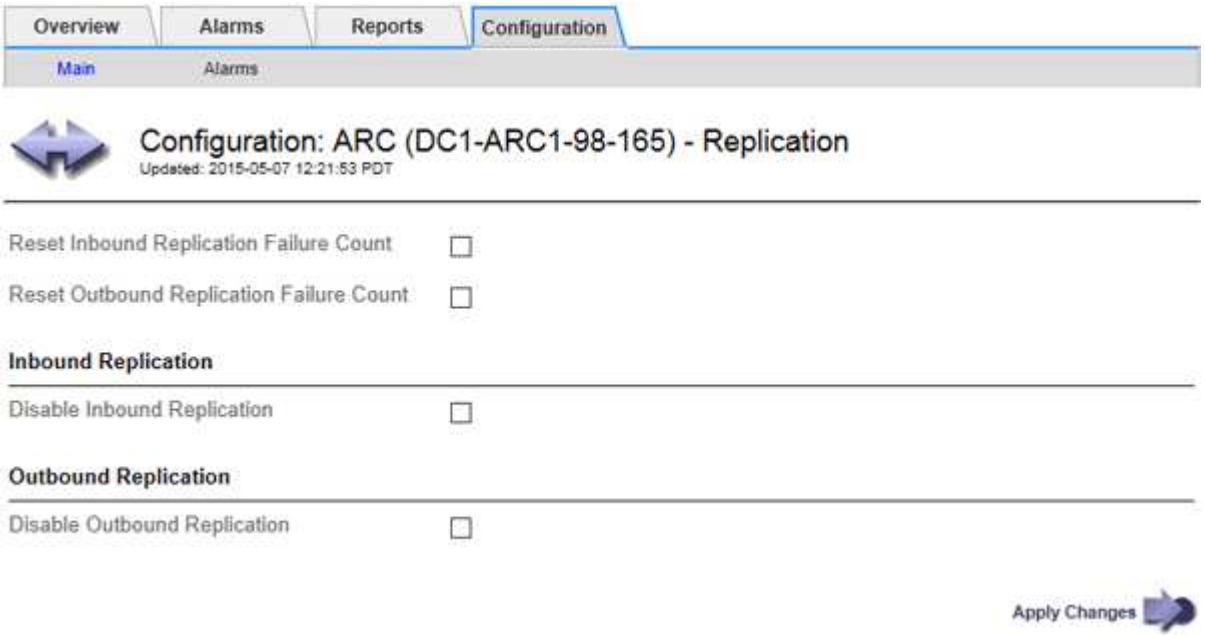
Puede configurar la configuración de replicación para un nodo de archivado y desactivar la replicación entrante y saliente, o restablecer los recuentos de fallos que se van a realizar el seguimiento de las alarmas asociadas.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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 deshabilitada, los datos de objeto se pueden recuperar desde el servicio ARC para su replicación a 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-.

   - **Desactivar la replicación saliente**: Active la casilla de verificación para desactivar la replicación saliente (incluidas las solicitudes de contenido para las recuperaciones HTTP) como parte de un procedimiento de mantenimiento o prueba. Deje sin marcar durante el funcionamiento normal.

     Cuando la replicación saliente está deshabilitada, 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 Supervisión y solución de problemas.

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 crean 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 para 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 administración 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 que implica la escritura de objetos directamente en la cinta u otro medio extraíble. 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 prácticas recomendadas 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 sólo para su guía; no están diseñadas para sustituir la documentación de TSM ni para proporcionar instrucciones completas y completas 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 completar una serie de pasos en el servidor TSM para 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: «'bloque 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, «depósito de almacenamiento de 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 establece en un valor de 0 o 1, ya que el nodo de archivado no admite sesiones de almacenamiento simultáneas.

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 dominios es una versión modificada de la política de dominio "tandard", configurada para escribir en cinta y con el destino de archivado configurado como base 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 está utilizando una clase de administración 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 configurado `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 «'no backup copy group'» que aparece cuando se 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.

La siguiente sección es una guía para comprender y planificar 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 almacenamiento near-line (como la cinta), asegúrese de que el almacenamiento del nodo de archivado dispone de 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.. Supervisión y solución de problemas.

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.

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 con cuidado según las instrucciones de este capítulo para evitar que afecte a las operaciones diarias del sistema o, en casos extremos, colocarse 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 de forma continua el sistema StorageGRID para garantizar que no se superen los distintos valores de atributo.

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.

De ser posible, no programe la migración de datos durante periodos de alta actividad. 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: Información general

Para administrar los objetos de un sistema StorageGRID, configure las reglas y políticas de gestión de ciclo de vida de la información (ILM). Las reglas y políticas de ILM indican a StorageGRID cómo crear y distribuir copias de datos de objetos y cómo gestionarlos a lo largo del tiempo.

Acerca de estas instrucciones

El diseño e implementación de reglas de ILM y la política 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:

- Obtenga más información sobre ILM de StorageGRID, incluida la manera en que ILM funciona durante la vida de un objeto, así como sobre qué reglas y políticas de ILM son.
- Aprenda a configurar pools de almacenamiento, perfiles de código de borrado y reglas de ILM.
- Aprenda a crear y activar una política de ILM que protegerá los datos de objetos en uno o más sitios.
- Aprenda a gestionar objetos con el bloqueo de objetos de S3, que ayuda a garantizar que los objetos de bloques de S3 no se eliminen ni se sobrescriban por un periodo de tiempo específico.

Leer más

Para obtener más información, consulte estos vídeos:

- "Vídeo: Reglas de ILM para StorageGRID: Introducción"

- "Vídeo: Políticas de ILM de StorageGRID"

ILM y ciclo de vida de los objetos

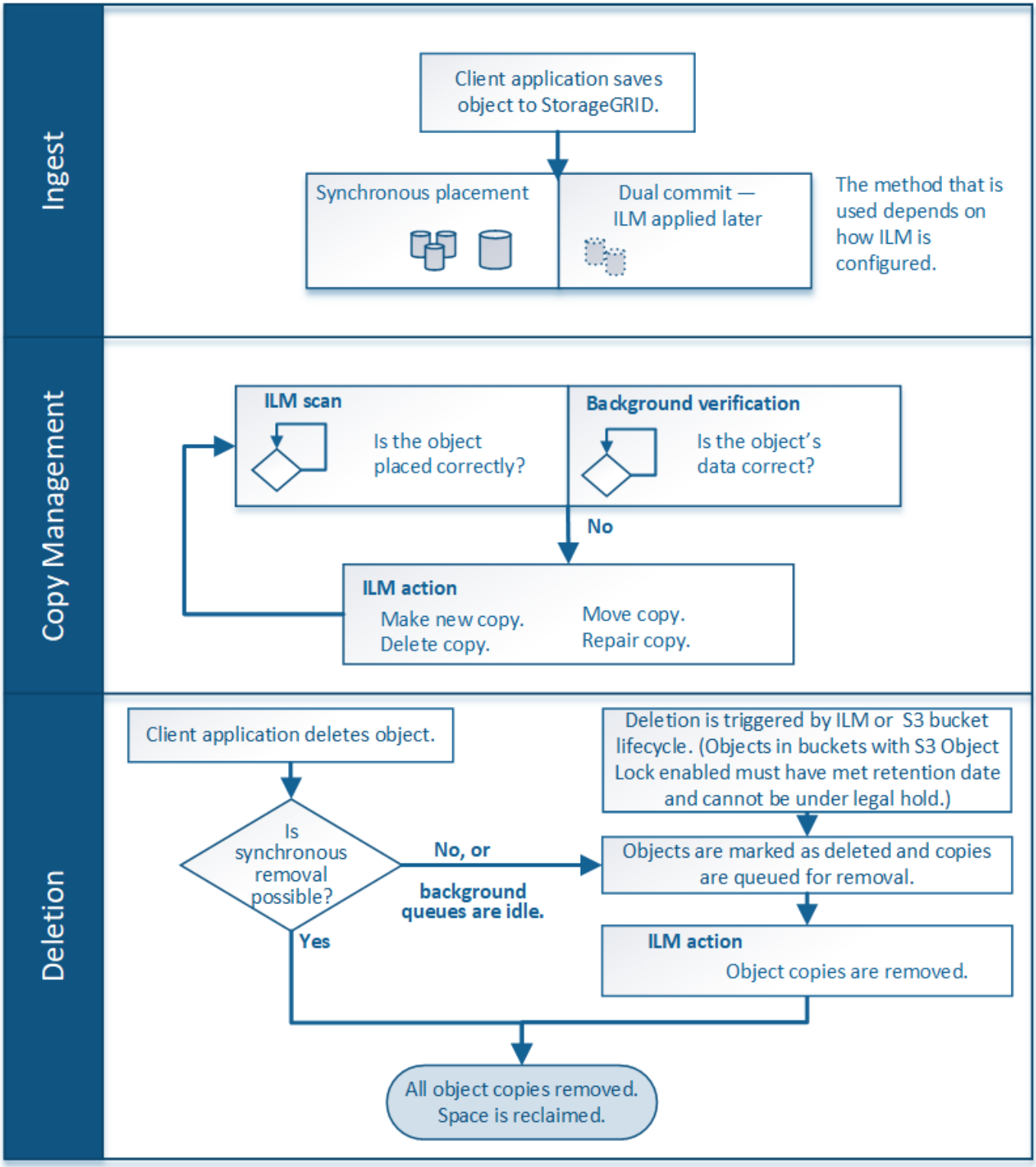
Cómo funciona ILM a lo largo de la vida de un objeto

Comprender cómo utiliza StorageGRID ILM para gestionar objetos durante cada fase de su vida útil puede ayudarle a diseñar una política más eficaz.

- **Ingesta**: 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 "'ingesta correcta'" 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 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 en segundo plano: StorageGRID realiza de forma continua verificación en segundo plano para comprobar la integridad de los datos de 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 las instrucciones para Supervisión y solución de problemas de StorageGRID.
- **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 bloque con el bloqueo de objetos S3 activado no se pueden eliminar si se encuentran en una retención legal o si se ha especificado una fecha de retención hasta pero aún no se ha cumplido.

El diagrama resume el funcionamiento de ILM a lo largo del ciclo de vida de un objeto.



Cómo se ingieren los objetos

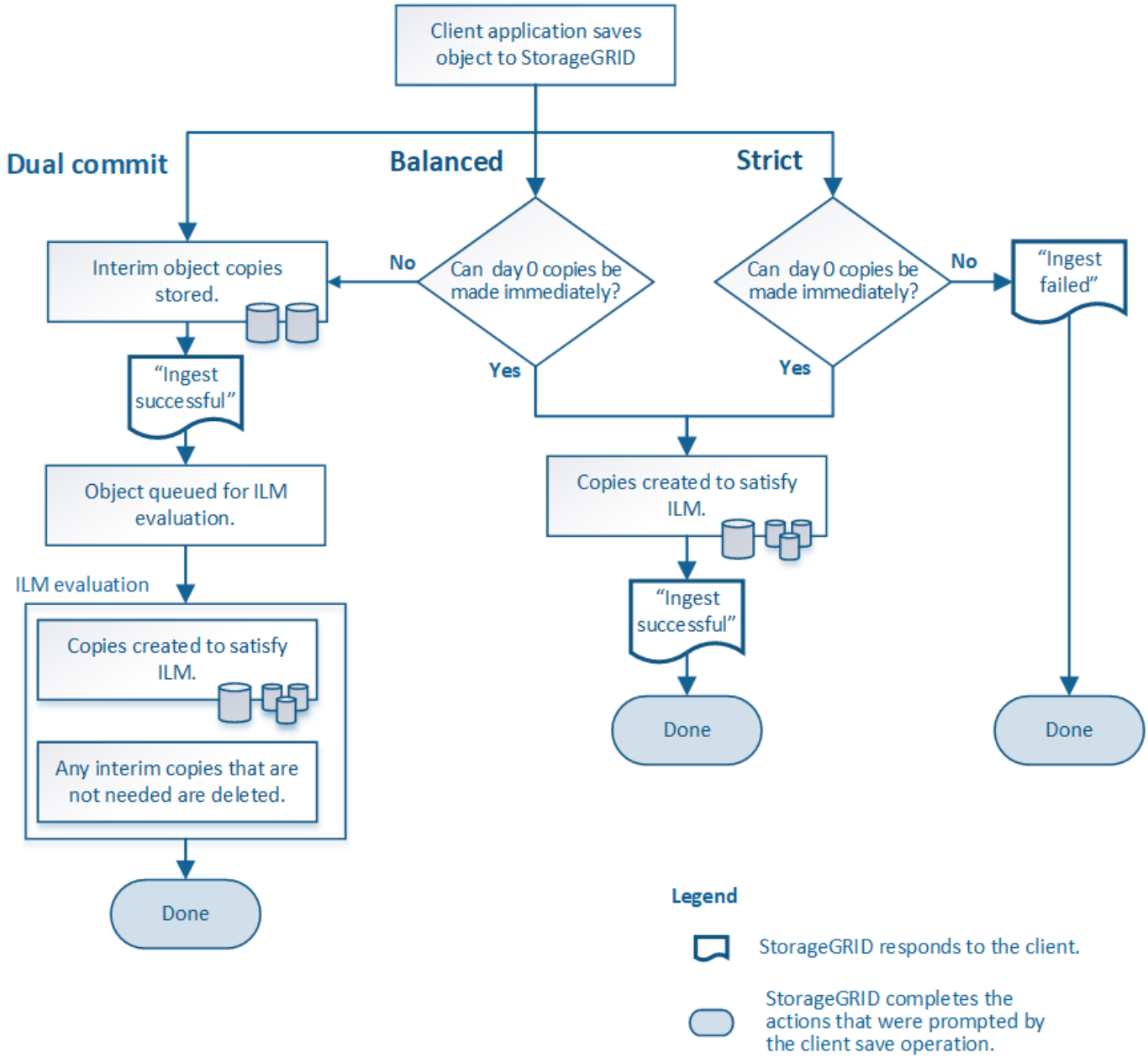
Opciones de protección de datos para consumo

Al crear una regla de ILM, debe especificar una de estas tres opciones para proteger los objetos durante la ingesta: Registro doble, equilibrado o estricto. 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 tres 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

Al seleccionar la opción de confirmación doble, StorageGRID realiza inmediatamente copias provisionales de objetos en dos nodos de almacenamiento diferentes y devuelve un mensaje «'ingesta correcta'» 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.

Cuándo utilizar la opción Dual COMMIT

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 usar el registro doble, debe asegurarse de que su grid puede realizar el trabajo adicional de crear y eliminar las copias de registro doble si no satisfacen el ILM. 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.

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. Error al procesar si StorageGRID no puede crear todas las copias, por ejemplo, porque una ubicación de almacenamiento necesaria no está disponible temporalmente. El cliente debe volver a intentar la operación.

Cuándo usar la opción estricta

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 tenga que utilizar la opción estricta y un filtro avanzado de restricción de ubicación para garantizar que los objetos no se almacenen nunca en un centro de datos determinado.

Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto

Equilibrado

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. A diferencia de la opción estricta, si StorageGRID no puede realizar todas las copias inmediatamente, utiliza la confirmación doble.

Cuándo utilizar la opción de equilibrio

Utilice la opción equilibrada para lograr la mejor combinación de protección de datos, rendimiento de grid y éxito de procesamiento. Balance es la opción predeterminada en el asistente de reglas de ILM.

Ventajas, inconvenientes y limitaciones de las opciones de protección de datos

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.

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 de equilibrio a menos que se requiera un comportamiento estricto de la ingesta o que la cuadrícula cumpla todos los criterios para la confirmación doble.
- **(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. Al utilizar las opciones equilibradas y estrictas, no se devuelve al cliente un mensaje «'ingesta correcta» hasta que se crean y almacenan todos los fragmentos codificados con borrado o copias replicadas. Sin embargo, lo más probable es que los datos de objetos lleguen a su ubicación final mucho más rápido.
- **(estricta) tasas más altas de error de procesamiento**: Con la opción estricta, la ingesta falla cuando StorageGRID no puede realizar de inmediato todas las copias especificadas en la regla 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 la carga de varias partes de S3, la gestión del ciclo de vida de la información se evalúa para cada parte del objeto según se ingiere y el objeto como un todo 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 haya colocado correctamente se coloca en la cola de repetición de la evaluación de ILM y se mueve a la ubicación correcta más adelante.
  - **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 cumplen 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 los cambios en la ubicación de objetos que se activan mediante la actualización no se realizan 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 colocación necesarios (por ejemplo, debido a que una ubicación recientemente requerida no está disponible), el objeto actualizado conserva su ubicación actual hasta que los cambios de colocación sean posibles.

Limitaciones en la colocación de objetos con las opciones equilibradas o estrictas

Las opciones equilibradas o estrictas no se pueden utilizar para las reglas de ILM que tengan cualquiera de las siguientes instrucciones de colocación:

- Ubicación en un pool de almacenamiento en cloud desde el día 0.
- Ubicación en un nodo de archivado en el día 0.
- Ubicaciones en un pool de almacenamiento en cloud o un nodo de archivado cuando la regla tiene un tiempo de creación definido por el usuario como su tiempo de referencia.

Estas restricciones existen porque StorageGRID no puede hacer copias de forma síncrona en un pool de almacenamiento en cloud o un nodo de archivado y un tiempo de creación definido por el usuario puede resolver este problema en el presente.

Cómo interactúan las reglas de ILM y los controles de coherencia para afectar a la protección de los datos

Tanto la regla de ILM como la elección del control de coherencia afectan a la forma en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, el comportamiento de ingesta seleccionado para una regla de ILM afecta la colocación inicial de las copias de objetos, mientras que el control de consistencia utilizado cuando se almacena un objeto afecta la colocación inicial de los metadatos de objetos. Dado que StorageGRID requiere acceso tanto a los metadatos de un objeto como a sus datos para cumplir con las solicitudes de los clientes, seleccionar los niveles de protección correspondientes para el nivel de coherencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas más predecibles del sistema.

A continuación encontrará un breve resumen de los controles de consistencia disponibles en StorageGRID:

- **All**: Todos los nodos reciben metadatos de objeto inmediatamente o la solicitud falla.
- **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 del objeto 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-after-write para nuevos objetos y eventual consistencia para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos.
- **Disponible** (eventual consistencia para las operaciones DE LA CABEZA): Se comporta igual que el nivel de consistencia "entre-después-nueva-escritura", pero sólo proporciona consistencia eventual para las operaciones DE LA CABEZA.

Antes de seleccionar un nivel de coherencia, lea la descripción completa de los controles de coherencia en las instrucciones para S3 o. Swift aplicaciones cliente. Debe comprender los beneficios y las limitaciones antes de cambiar el valor predeterminado.

Ejemplo de cómo puede interactuar el control de consistencia y la regla de ILM

Suponga que tiene una cuadrícula de dos sitios con la siguiente regla de ILM y la siguiente configuración de nivel de coherencia:

- **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.
- **Nivel de coherencia**: "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 su lugar usa la misma regla de ILM y el nivel de consistencia de «otrong-site», es posible que el cliente reciba un mensaje de éxito después de replicar los datos del objeto en el sitio remoto, pero antes de que los metadatos del objeto 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 los niveles de coherencia y las reglas del 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

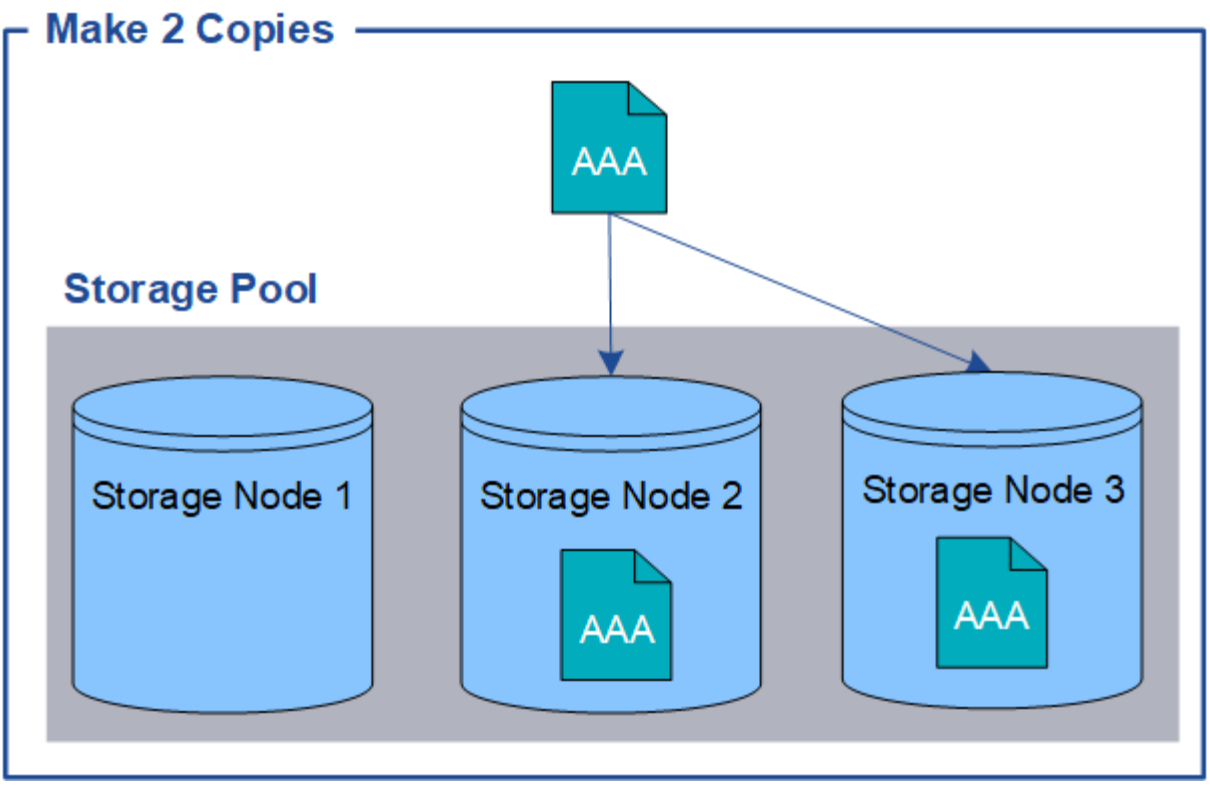
Cómo se almacenan los objetos (codificación de borrado o replicación)

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 un pool de almacenamiento
- Utilice varios pools de almacenamiento para la replicación entre sitios

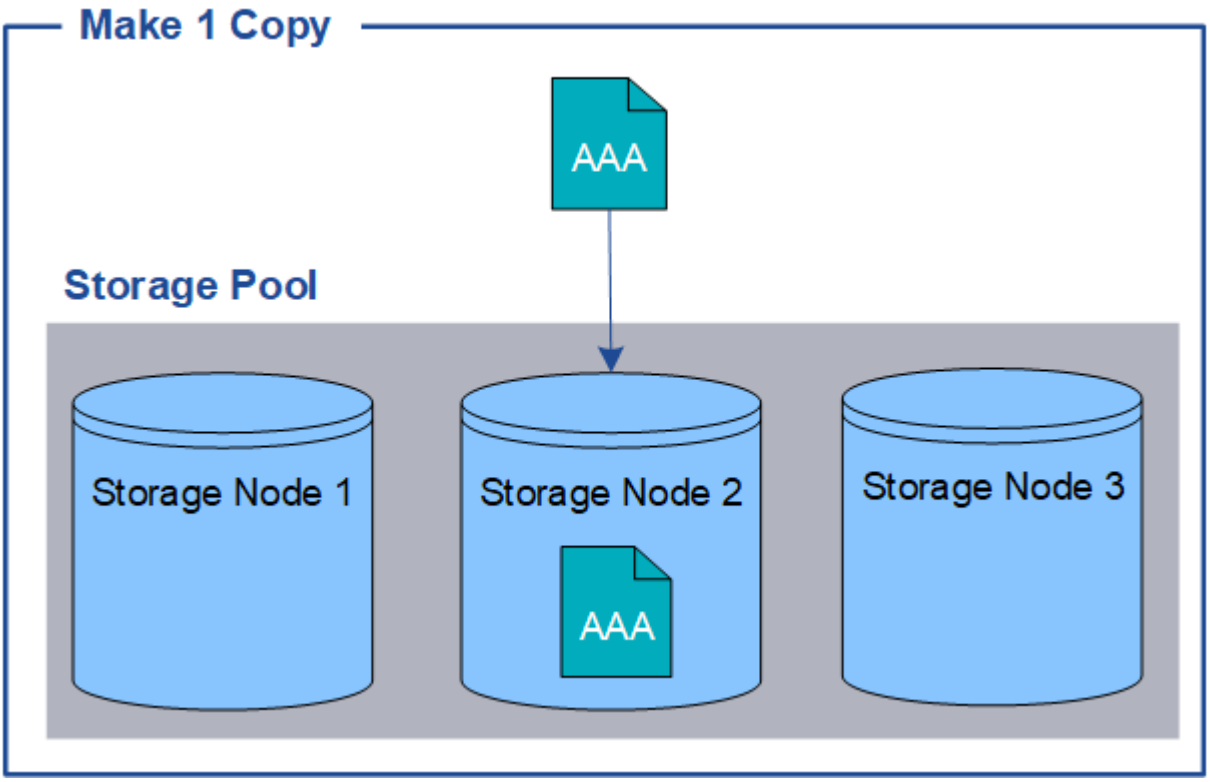
Por qué no se debe utilizar la replicación de copia única

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.

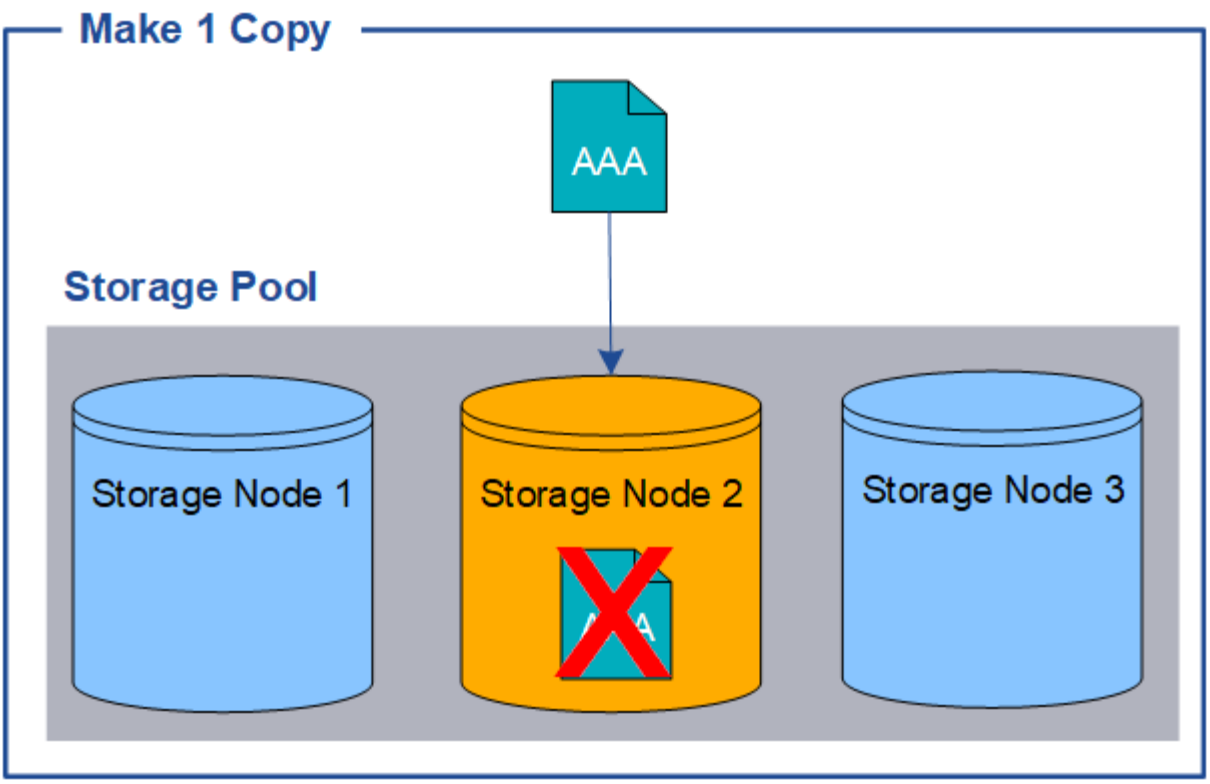
> No utilice una regla de ILM que solo cree una copia replicada durante un periodo de tiempo. Si sólo existe una copia replicada de un objeto, éste se pierde si falla un nodo de almacenamiento o tiene un error importante. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, 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

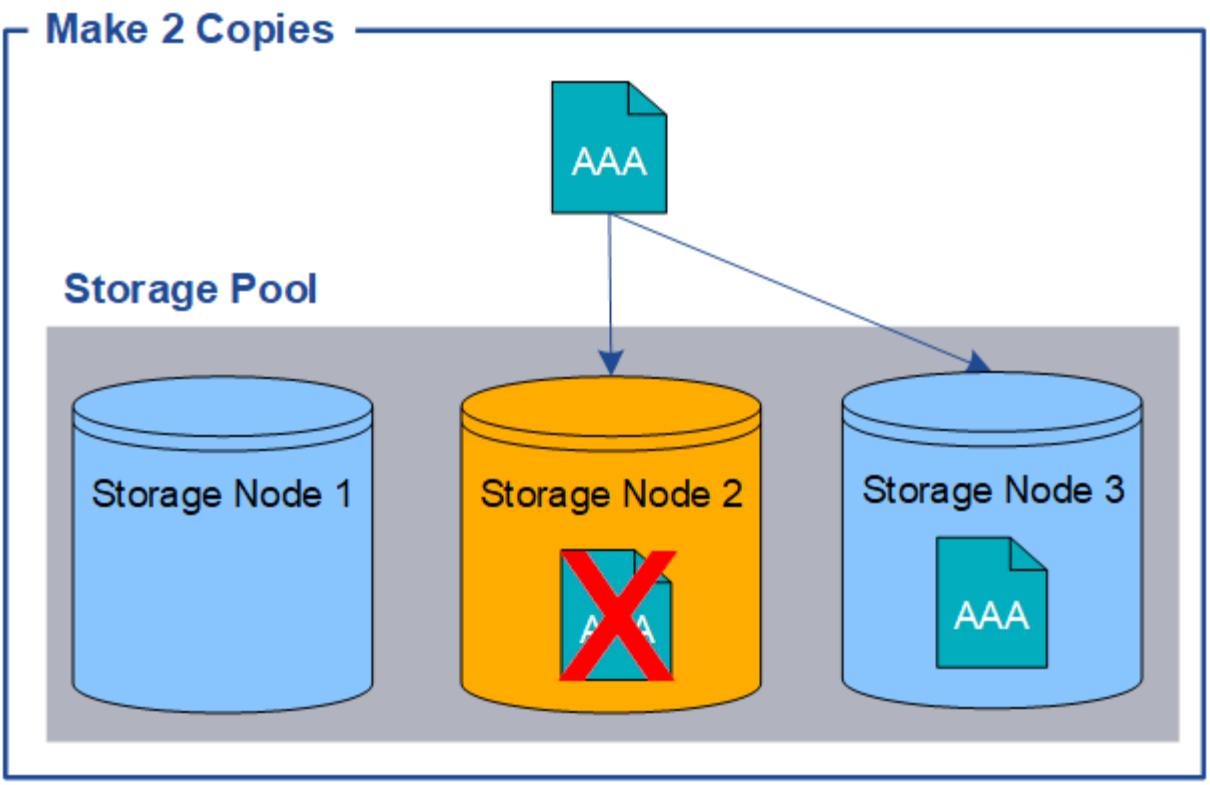
coincida con esta regla, StorageGRID coloca una sola copia en un solo nodo de almacenamiento.



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.



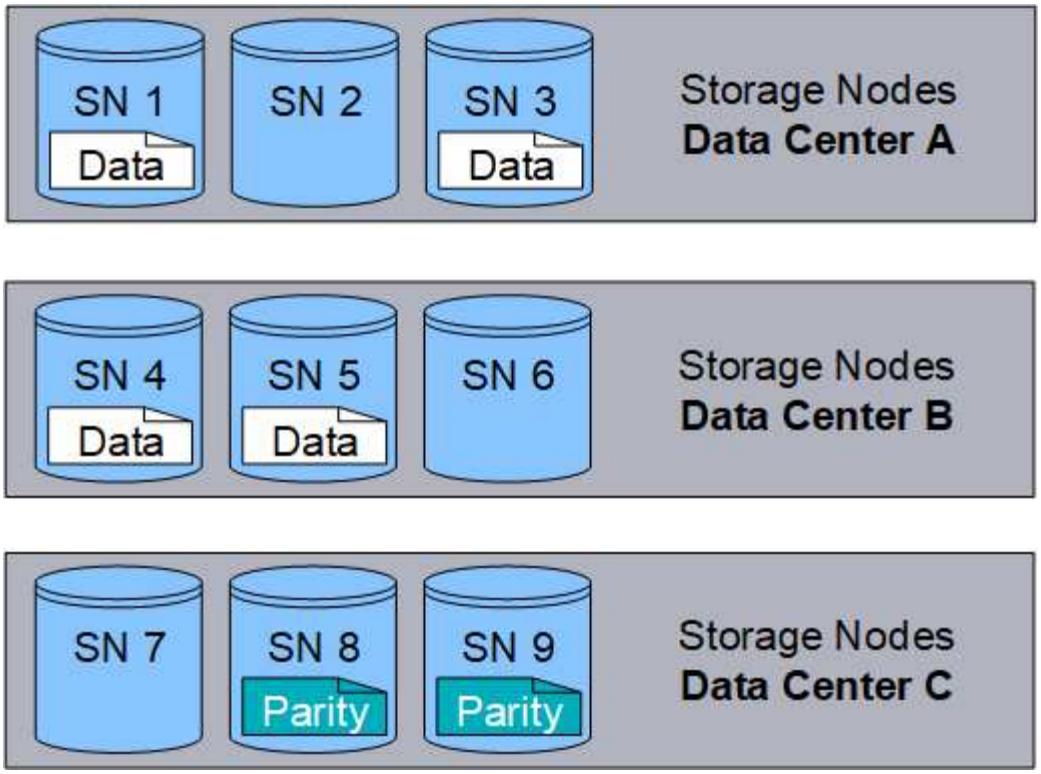
Para evitar la pérdida de datos de objetos, siempre debe realizar al menos dos copias de todos los objetos que desee proteger con replicación. Si existen dos o más copias, puede seguir teniendo acceso al objeto si un nodo de almacenamiento falla o se desconecta.



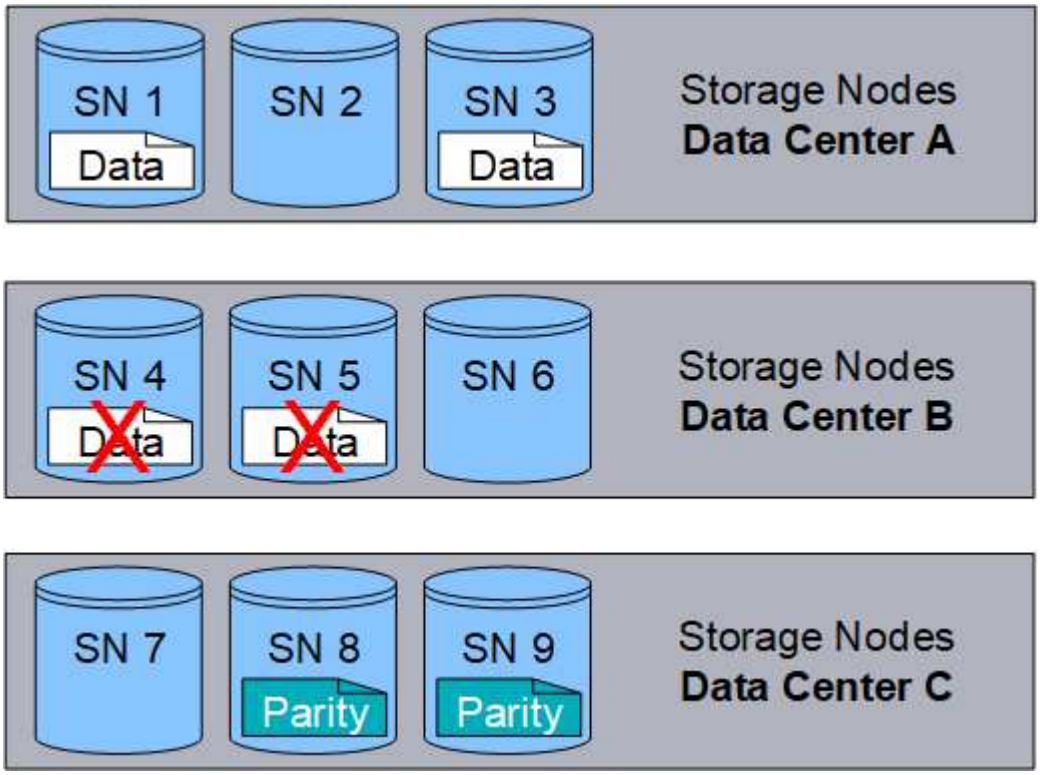
Qué es la codificación de borrado

El código de borrado es el segundo método que utiliza StorageGRID para almacenar datos de objetos. 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 código de borrado puede recrear ese fragmento con un subconjunto de los datos restantes y los fragmentos de paridad.

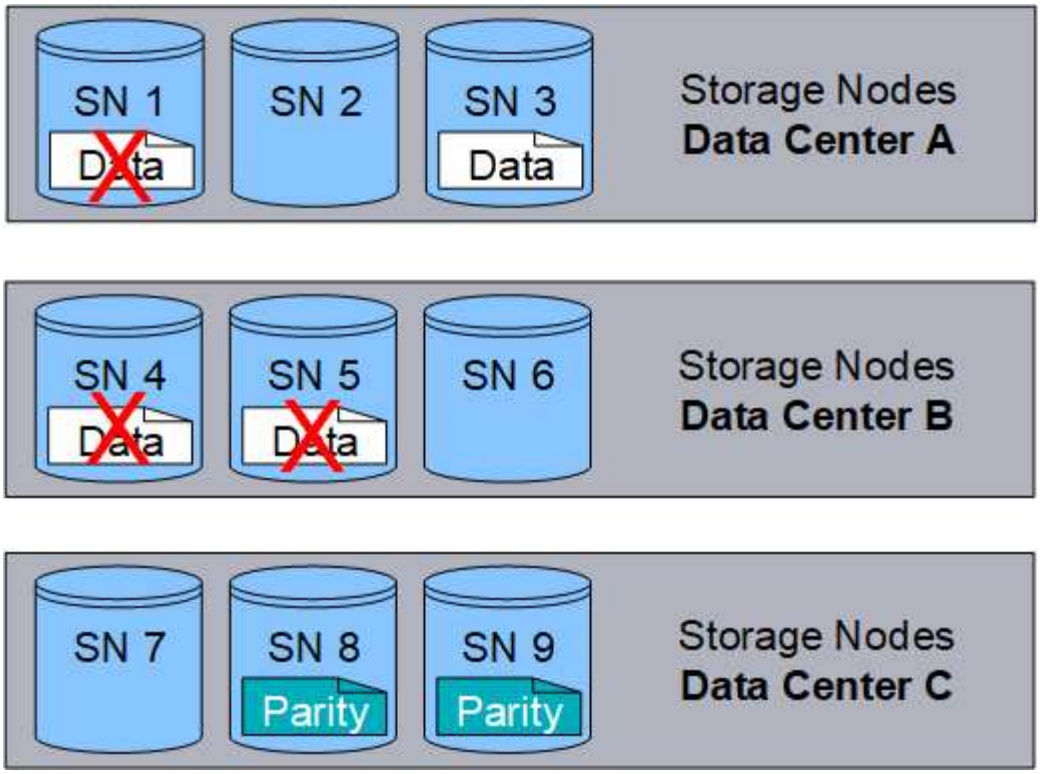
En el siguiente ejemplo, se muestra el uso de un algoritmo de codificación de borrado en los datos de un objeto. En este ejemplo, la regla ILM utiliza un esquema de codificación de borrado 4+2. Cada objeto se divide en cuatro fragmentos de datos iguales y dos fragmentos de paridad se calculan a partir 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 requiere un mínimo de nueve nodos de almacenamiento, con tres nodos de almacenamiento en cada uno de tres sitios diferentes. 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 completo del centro de datos, aún se puede recuperar o reparar el objeto, siempre que todos los demás fragmentos permanezcan accesibles.



Si se pierden más de dos nodos de almacenamiento, el objeto no se puede recuperar.



Información relacionada

- Qué es un pool de almacenamiento
- Qué son los esquemas de codificación de borrado
- Cree un perfil de código de borrado

Qué son los esquemas de codificación de borrado

Cuando configura el perfil de código de borrado para una regla de ILM, debe seleccionar un esquema de codificación de borrado disponible basado en la cantidad de nodos y sitios de almacenamiento que componen el pool de almacenamiento que planea utilizar. Los esquemas de codificación de borrado controlan cuántos fragmentos de datos se crean y cuántos fragmentos de paridad se crean para cada objeto.

El sistema StorageGRID utiliza el algoritmo de codificación de borrado Reed-Solomon. El algoritmo corta un objeto en fragmentos de datos k y calcula fragmentos de paridad m. Los fragmentos k + m = n se distribuyen en n nodos de almacenamiento para proporcionar protección de datos. Un objeto puede sostener hasta m fragmentos perdidos o corruptos. se necesitan fragmentos k para recuperar o reparar un objeto.

Al configurar un perfil de código de borrado, siga las siguientes directrices para los pools de almacenamiento:

- El pool de almacenamiento debe incluir tres o más sitios, o exactamente un sitio.

  > No es posible configurar un perfil de 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 el pool de almacenamiento predeterminado, todos los nodos de almacenamiento ni un grupo de almacenamiento que incluya el sitio predeterminado, todos los sitios.
- El pool de almacenamiento debe incluir al menos *k*+*m* +1 nodos de almacenamiento.

  La cantidad mínima de nodos de almacenamiento necesarios 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 codificación de borrado se calcula dividiendo el número de fragmentos de paridad (*m*) entre 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 con el valor total más bajo de *k*+*m* que se ajuste a sus necesidades. los esquemas de codificación de borrado con un menor número de fragmentos suelen ser más eficientes desde el punto de vista computacional, ya que se crean y distribuyen (o se recuperan) por objeto, pueden mostrar un mejor rendimiento debido al mayor tamaño de fragmento y pueden requerir menos nodos en una expansión cuando se necesita más almacenamiento. (Consulte las instrucciones para ampliar StorageGRID para obtener información sobre cómo planificar una ampliación de almacenamiento.)

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.

En el caso de los esquemas de codificación de borrado que proporcionan protección contra pérdida de sitio, la cantidad recomendada de nodos de almacenamiento en el pool de almacenamiento supera *k*+*m*+1 porque 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 %

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
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 aumenta al tener más segmentos de paridad (es decir, cuando *m* tiene un valor superior).
- **Tráfico de red**: Cuando se recupera de fallos, usando 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.

La cantidad mínima de nodos de almacenamiento necesarios es *k*+*m*, pero se recomienda un pool de almacenamiento con nodos *k*+*m*+1. 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 %

Información relacionada

Amplíe su grid

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 un objeto que se elimina en tres sitios con

un esquema de codificación 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 requiere un mayor número de nodos y sitios de almacenamiento. Por ejemplo, si utiliza un esquema de código de borrado de 6+3, debe tener al menos tres nodos de almacenamiento en tres sitios diferentes. Por el contrario, si simplemente replica datos de objetos, solo necesita un nodo de almacenamiento para cada copia.
- Aumento del coste y de la complejidad de las ampliaciones del almacenamiento. Para ampliar una puesta en marcha que usa la replicación, solo tiene que 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 que los nodos existentes estén llenos al 100 %, debe añadir al menos *k+m* nodos de almacenamiento, pero si expande cuando los nodos existentes están 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 objeto para un objeto que se codifica con borrado y se distribuyen en sitios remotos tardan más en recuperarse a través de conexiones WAN que los objetos que se replican y están disponibles 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 utilice la codificación de borrado para objetos de menos de 200 KB con el fin de evitar la sobrecarga de gestión de fragmentos codificados con borrado de muy pequeño tamaño.

- 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.
  - Cualquier método no puede eliminar una versión de objeto que esté bajo una retención legal.
  - Antes de que se alcance la fecha de retención de una versión de objeto, dicha versión no se puede eliminar mediante ningún método.
  - Los objetos en bloques con S3 Object Lock habilitado son mantenidos por ILM "'eternamente'". 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. 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 "'eternamente'" para las instrucciones de colocación.

Independientemente de quién controle cuánto tiempo se retienen los objetos, la configuración de ILM controla qué tipos de copias de objetos (replicadas o codificadas 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

La acción de caducidad en un ciclo de vida de bloque de S3 siempre anula la configuración de ILM. 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

Almacenar dos copias en nodos de almacenamiento «para 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

Almacenar dos copias en nodos de almacenamiento «para 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 de un contenedor que tiene habilitado el bloqueo de objetos S3 no se pueden eliminar si están en una reserva legal o si se ha especificado una fecha de retención, pero aún no se ha cumplido. • 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 objeto no está disponible temporalmente. ◦ 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 de S3 o Swift realizan solicitudes de eliminación, StorageGRID comienza agregando una serie de 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.

Cuánto tiempo se tarda en 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 de cerca el rendimiento de eliminación durante una eliminación masiva, puede observar que la tasa de eliminación aparece como 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.

Debe tener en cuenta que 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 se crea una versión de los objetos, 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 objetos simplemente crea un marcador de borrado como la versión actual del objeto, que hace que la versión anterior del objeto sea "'no actual'".

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, debe realizar una de las siguientes acciones:

- **Solicitud de cliente S3**: Especifique el número de versión del 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 objeto no se pueden recuperar.
- **ILM**: Agregue dos reglas ILM a su política de ILM. Utilice **tiempo no corriente** como tiempo de referencia en la primera regla para coincidir con las versiones no actuales del objeto. Utilice **tiempo de procesamiento** en la segunda regla para que coincida con la versión actual. La regla **tiempo no corriente** debe aparecer en la directiva por encima de la regla **tiempo de ingesta**.

Información relacionada

- Use S3
- Ejemplo 4: Reglas de ILM y políticas para objetos con versiones de S3

Qué es una política de ILM

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.

¿Cómo evalúa objetos una política de ILM?

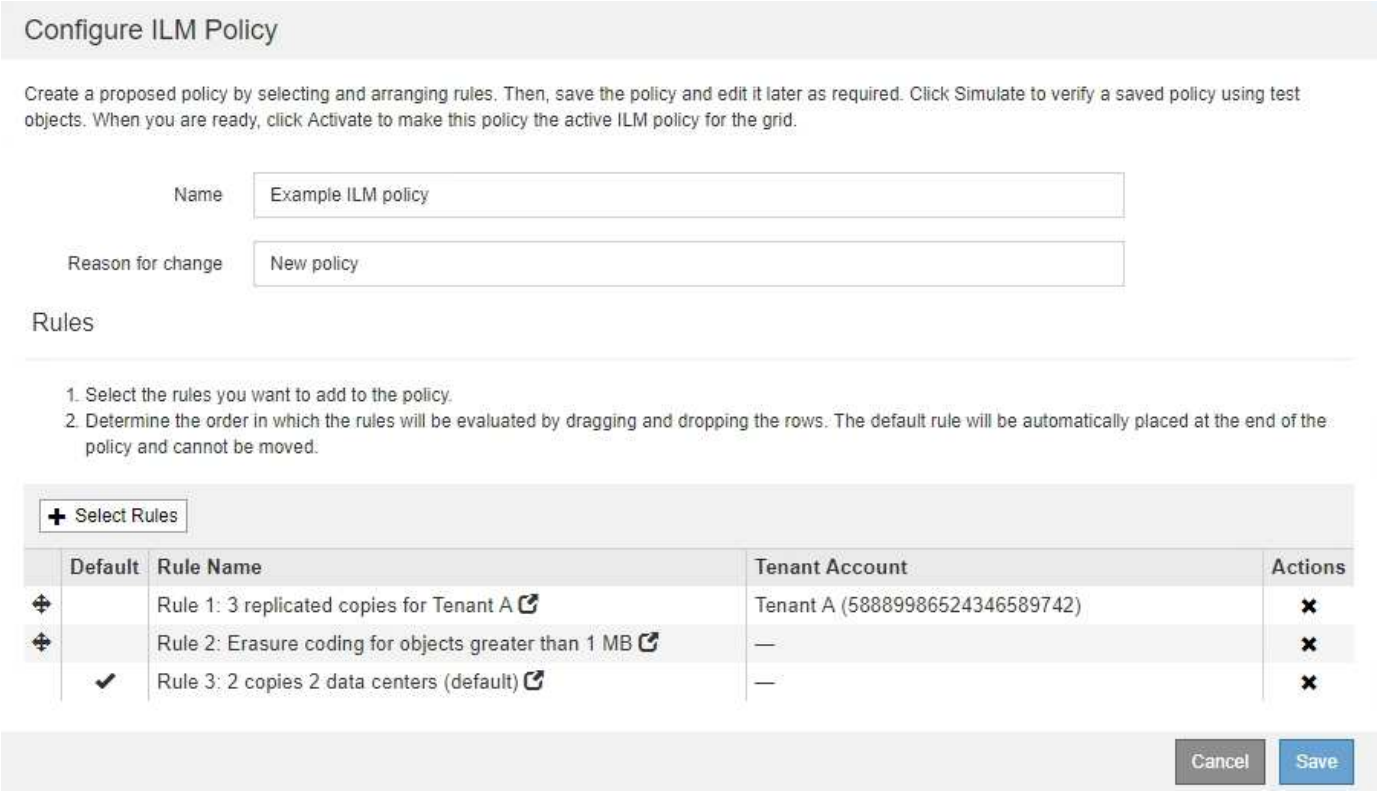
La política activa de ILM para su sistema StorageGRID controla la ubicación, la duración y la protección de datos de todos los objetos.

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 en función de cada regla posterior de la política hasta que se realice 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, todos los bloques y todas las versiones del objeto, y no puede utilizar ningún filtro avanzado.

Ejemplo de política de ILM

Este ejemplo de política de ILM usa tres reglas de ILM.

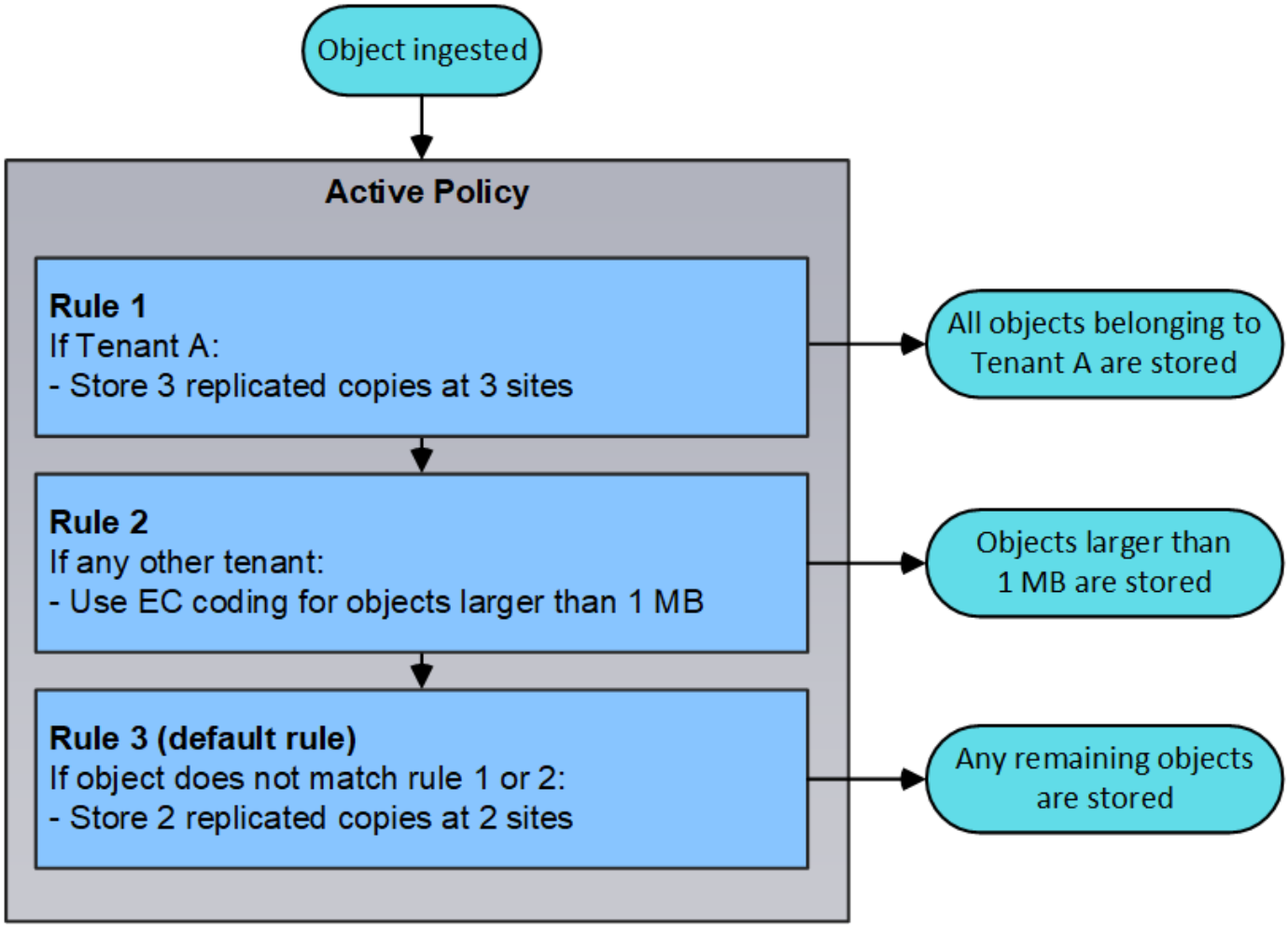


En este ejemplo, la regla 1 coincide con todos los objetos que pertenecen al arrendatario A. Estos objetos se almacenan como tres copias replicadas en tres sitios. Los objetos pertenecientes a otros arrendatarios no coinciden con la Regla 1, por lo que se evalúan en función de la Regla 2.

La regla 2 coincide con todos los objetos de otros arrendatarios, pero sólo si son superiores a 1 MB. Estos objetos de mayor tamaño se almacenan mediante codificación de borrado 6+3 en tres instalaciones. La regla

2 no coincide con los objetos de 1 MB o menos, por lo que estos objetos se evalúan en función de la regla 3.

La regla 3 es la última regla y la regla predeterminada de la política y no utiliza filtros. La regla 3 realiza dos copias replicadas de todos los objetos que no coinciden en la regla 1 o la regla 2 (objetos que no pertenecen al arrendatario A que son de 1 MB o menos).



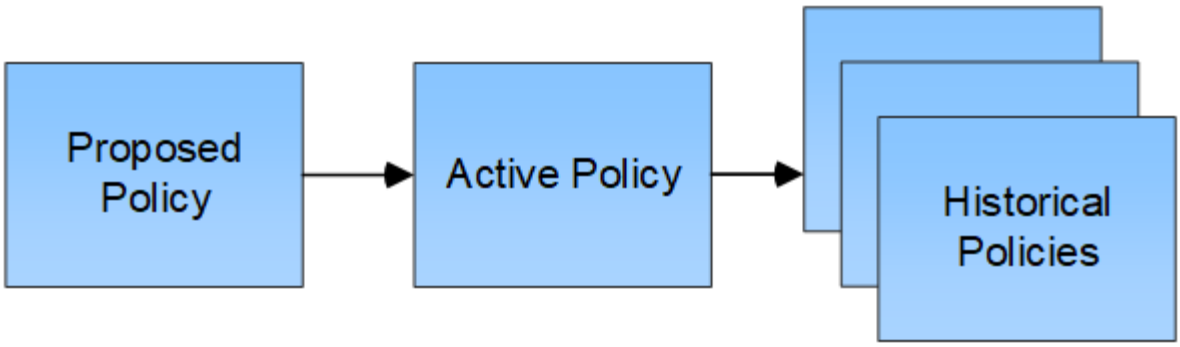
¿Qué son las políticas propuestas, activas e históricas?

Todos los sistemas StorageGRID deben tener una política de ILM activa. Un sistema StorageGRID también puede tener una política de ILM propuesta y cualquier número de políticas históricas.

Cuando se crea por primera vez una política de ILM, se crea una política propuesta seleccionando una o varias reglas de ILM y ordenándolas en un orden específico. Después de simular la política propuesta para confirmar su comportamiento, la activa para crear la política activa.

Cuando se activa una nueva política de ILM, StorageGRID utiliza esa política para gestionar todos los objetos, incluidos los objetos existentes y los objetos recién procesados. Es posible que los objetos existentes se muevan a nuevas ubicaciones cuando se implementen las reglas de ILM en la nueva política.

La activación de la directiva propuesta hace que la directiva previamente activa se convierta en una directiva histórica. No se pueden eliminar las políticas históricas de ILM.



Información relacionada

Cree una política de ILM

Qué es una regla de ILM

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.

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 se pueden replicar o codificar.
- Para las copias replicadas, el número de copias realizadas.
- Para las copias codificadas de borrado, se utiliza el esquema de codificación 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. Las copias se distribuyen uniformemente por todos los nodos de almacenamiento.

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.

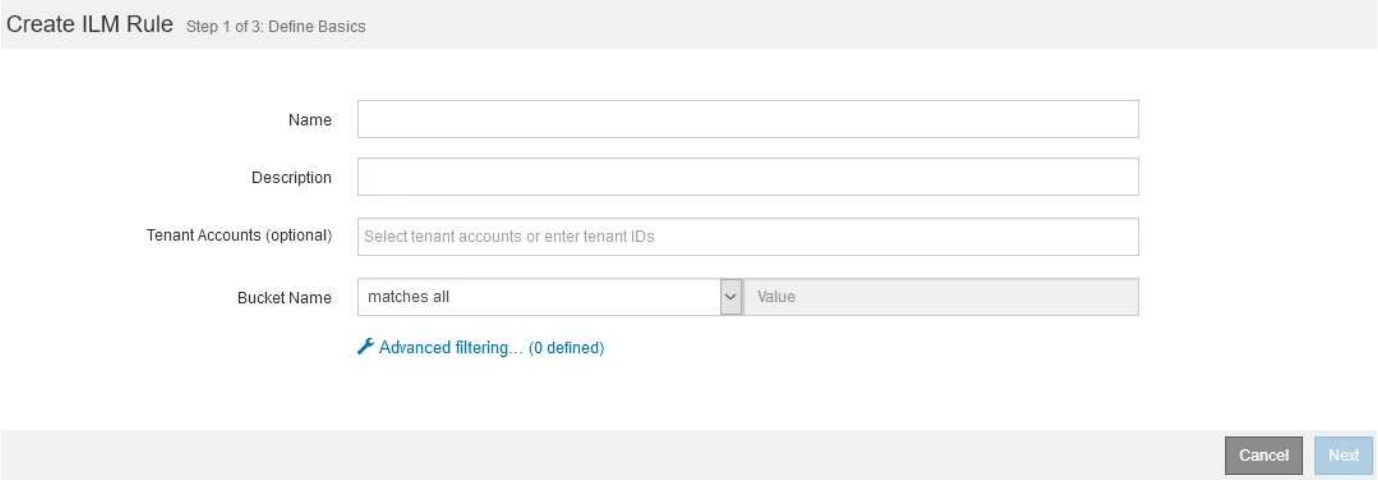
- **Instrucciones de colocación**: Las instrucciones de colocación de una regla definen el número, el tipo y la ubicación de las copias de objetos. Cada regla puede incluir una secuencia de instrucciones de colocación para cambiar el número, el tipo y la ubicación de las copias de objetos a lo largo 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 procesamiento**: El comportamiento de procesamiento de una regla define lo que ocurre cuando un cliente S3 o Swift guarda un objeto en la cuadrícula. 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.

Qué es el 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 los objetos que no coinciden con los filtros de otra regla.

Los filtros básicos permiten aplicar diferentes reglas a grupos grandes y distintos de objetos. Los filtros básicos de la página define Basics del asistente Create ILM Rule le permiten aplicar una regla a cuentas de inquilino específicas, bloques S3 específicos, contenedores Swift, o ambos.



Estos filtros básicos le proporcionan una forma 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.

La página **filtrado avanzado** del asistente Crear regla ILM le ofrece 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)
- Región de bloques de S3 (limitación de ubicación)

- Tamaño del objeto
- Metadatos del usuario
- Etiquetas de objetos de 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.

También puede combinar filtros básicos y avanzados 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, se pueden crear reglas que filtran por cuenta de arrendatario para separar los registros de cada departamento, al mismo tiempo que se utilizan filtros avanzados en cada regla para identificar el tipo específico de objetos al que se aplica la regla.

¿Qué son las instrucciones de colocación de 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.

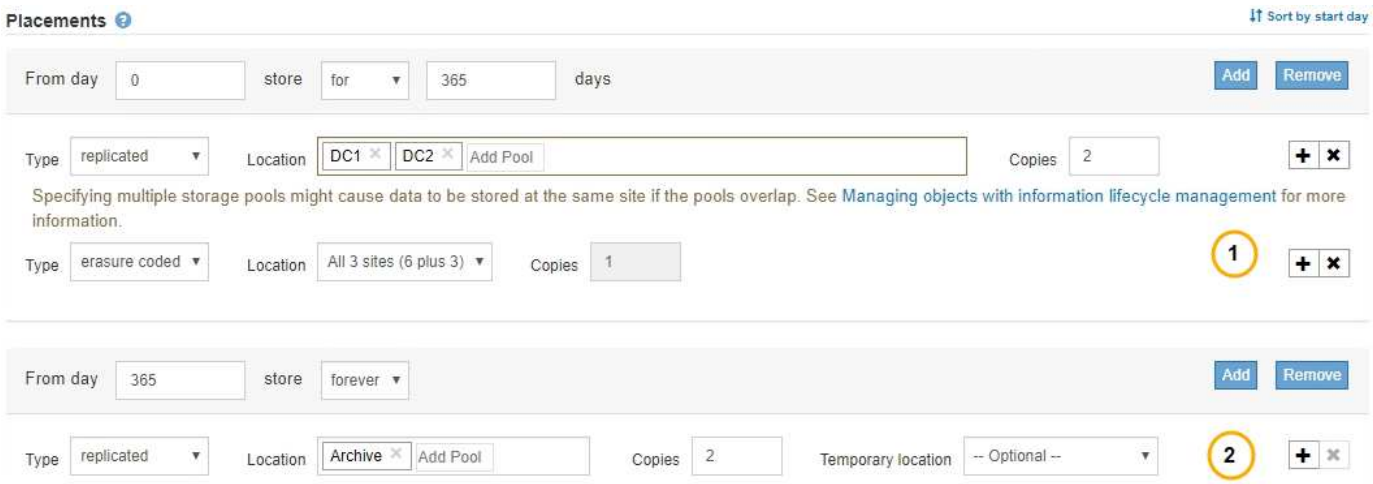
Al crear instrucciones de colocación:

- 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 podría comenzar en 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 único período de tiempo, seleccione el icono de signo más ➕ para agregar más de una línea para ese período de tiempo.
- Para colocar objetos en diferentes ubicaciones en diferentes períodos de tiempo, seleccione el botón **Agregar** para agregar el siguiente período de tiempo. A continuación, especifique una o más líneas dentro del período de tiempo.

El ejemplo muestra la página define colocaciones del asistente Create ILM Rule.



1	La primera instrucción de colocación tiene dos líneas para el primer año: 1. La primera línea crea dos copias de objetos replicadas en dos sitios de centro de datos. 2. La segunda línea crea una copia con código de borrado de 6+3 utilizando tres centros de datos.
2	La segunda instrucción de colocación crea dos copias archivadas después de un año y mantiene esas copias para siempre.

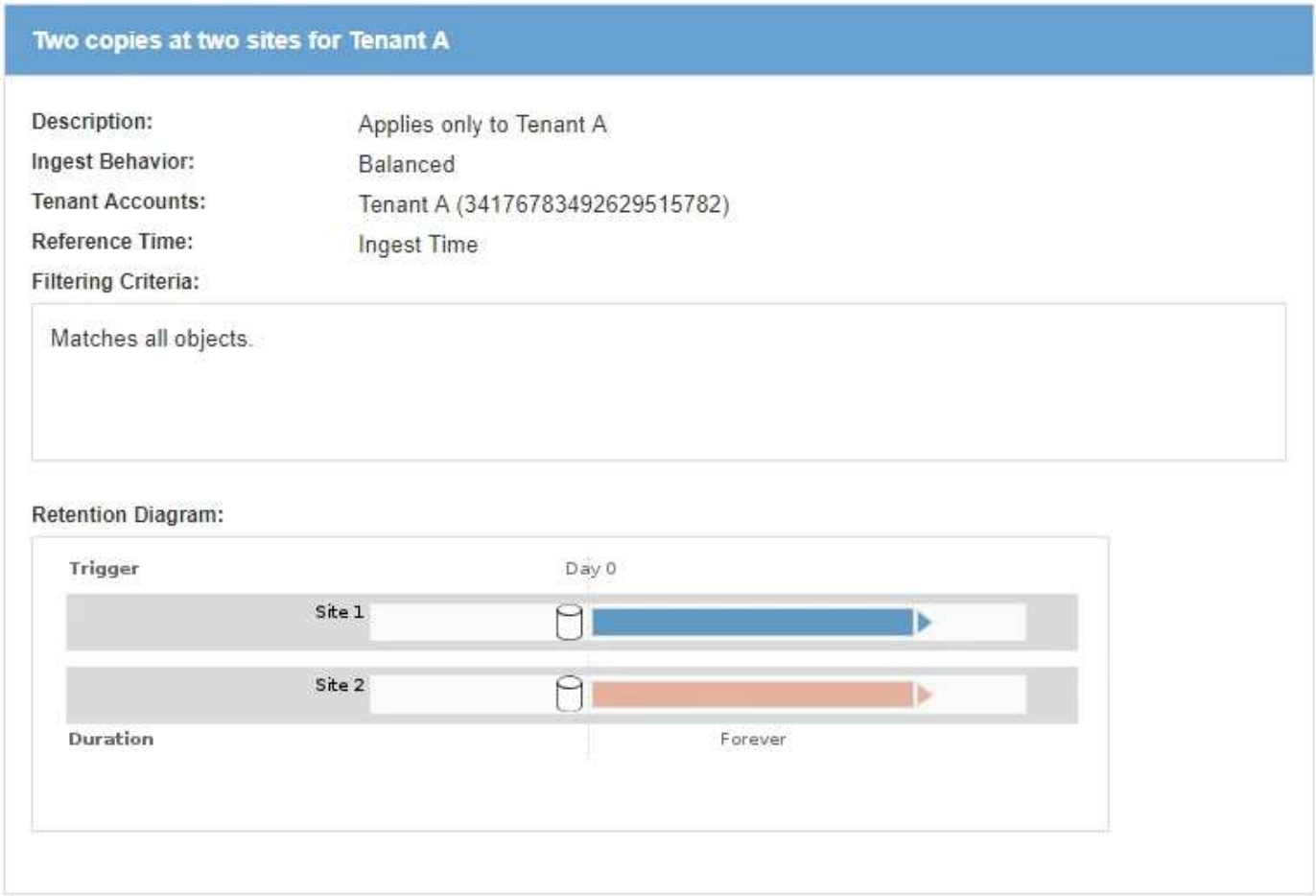
Cuando defina el conjunto de instrucciones de colocación para una regla, debe asegurarse de que al menos una instrucción de colocación comienza en el día 0, de que no haya espacios entre los períodos de tiempo definidos. y que la instrucción de colocación final continúa para siempre o hasta que ya no 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.

Regla de ILM de ejemplo

Esta regla de ILM de ejemplo se aplica a los objetos que pertenecen al inquilino A. Realiza dos copias replicadas de esos objetos y almacena cada copia en un sitio diferente. Las dos copias se conservan «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.

Esta regla utiliza la opción equilibrada para el comportamiento de procesamiento: La instrucción de colocación de dos sitios se aplica tan pronto como el inquilino A guarda un objeto en StorageGRID, a menos que no sea posible realizar de inmediato ambas copias necesarias. 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

- Opciones de protección de datos para consumo
- Qué es un pool de almacenamiento
- Qué es un pool de almacenamiento cloud

Crear grados de almacenamiento, pools de almacenamiento, perfiles de EC y regiones

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 colocan ciertos objetos en ciertos nodos de almacenamiento, en lugar de en todos los nodos del sitio. Por ejemplo, quizás desee almacenar determinados objetos en los nodos de almacenamiento más rápidos, como los dispositivos de almacenamiento all-flash StorageGRID.

Lo que necesitará

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

Acerca de esta tarea

Si utiliza más de un tipo de almacenamiento, puede crear, opcionalmente, un nivel de almacenamiento para identificar cada tipo. La creación de grados de almacenamiento permite seleccionar un tipo específico de nodo de almacenamiento al configurar pools de almacenamiento.

Si el grado de almacenamiento no es un problema (por ejemplo, todos los nodos de almacenamiento son idénticos), puede omitir este procedimiento y utilizar el grado de almacenamiento predeterminado todos los nodos al configurar pools de almacenamiento.

Cuando se añade un nuevo nodo de almacenamiento en una ampliación, dicho nodo se añade al nivel de almacenamiento predeterminado de todos los nodos de almacenamiento. Como resultado:

- Si una regla de ILM utiliza un pool de almacenamiento con el nivel All Storage Nodes, se puede usar el nodo nuevo inmediatamente después de que finalice la ampliación.
- Si una regla de ILM usa un pool de almacenamiento con un grado de almacenamiento personalizado, no se usará el nuevo nodo hasta que se asigne manualmente el grado de almacenamiento personalizado al nodo, como se describe a continuación.

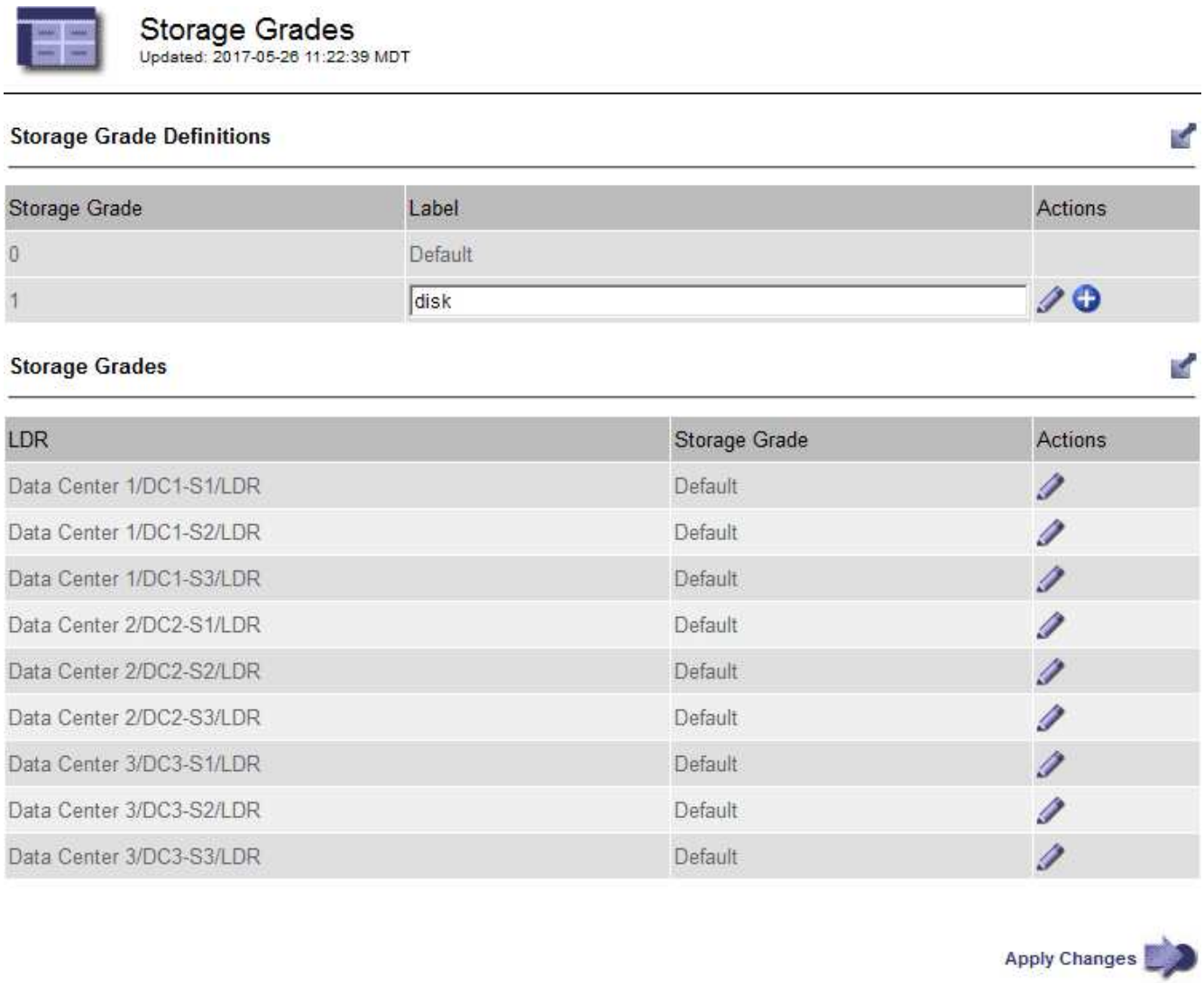
> Al crear grados de almacenamiento, no cree más grados de almacenamiento del necesario. Por ejemplo, no cree un grado de almacenamiento para cada nodo de almacenamiento. En su lugar, asigne cada grado de almacenamiento a dos o más nodos. Las leyes de almacenamiento asignadas a un solo nodo pueden provocar reversiones de ILM si ese nodo deja de estar disponible.

Pasos

1. Seleccione **ILM** > **grados de almacenamiento**.
2. Crear un grado de almacenamiento:

   a. Para cada grado de almacenamiento que necesita definir, seleccione **Insertar** para agregar una fila e introducir una etiqueta para el grado de almacenamiento.

      El grado de almacenamiento predeterminado no se puede modificar. Se reserva para los nuevos nodos de almacenamiento añadidos durante una ampliación del sistema StorageGRID.



a. Para editar un grado de almacenamiento existente, seleccione **Editar** y modifique la etiqueta según sea necesario.

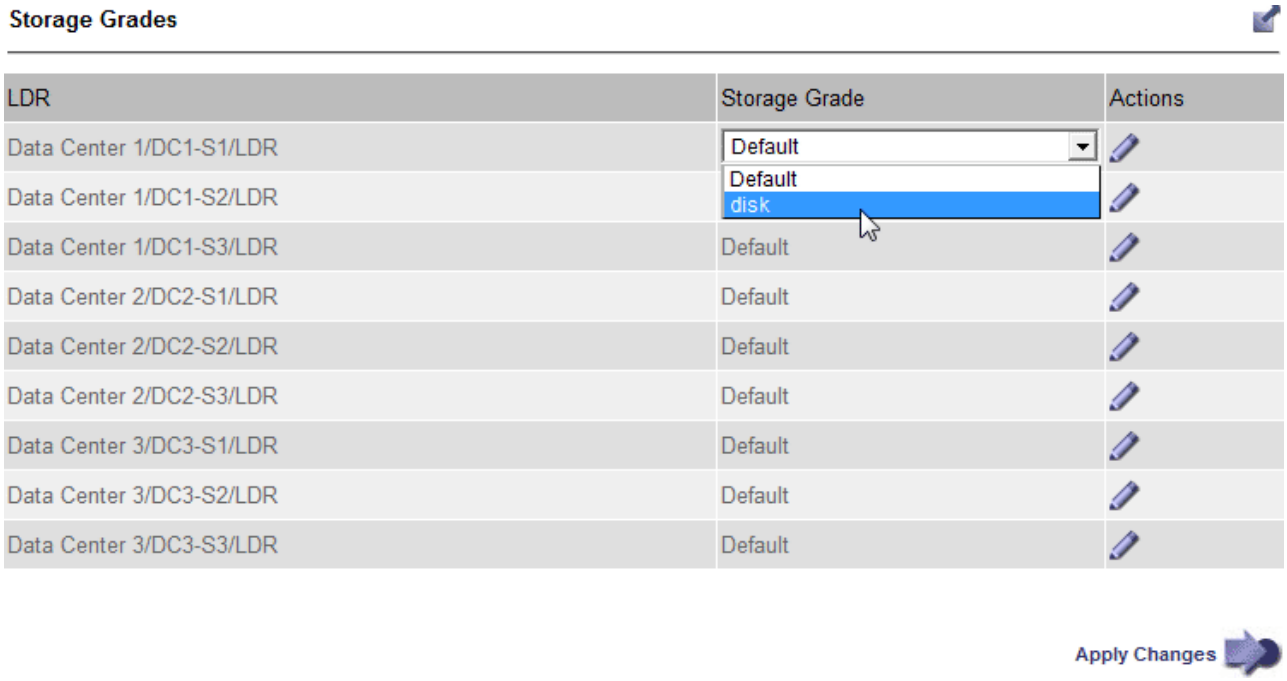
> No es posible eliminar grados de almacenamiento.

b. Seleccione **aplicar cambios**.

   Estas clases de almacenamiento ahora están disponibles para su asignación a nodos de almacenamiento.

3. Asigne un grado de almacenamiento a un nodo de almacenamiento:

   a. Para cada servicio LDR del nodo de almacenamiento, seleccione **Editar** y seleccione un grado de almacenamiento de 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**.

Configurar los 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. Los pools de almacenamiento se configuran para determinar dónde el sistema StorageGRID almacena los datos de objetos y el tipo de almacenamiento utilizado.

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.

Las reglas de ILM permiten utilizar los pools de almacenamiento para determinar dónde se almacenan los datos de objetos. 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

Al configurar y usar pools de almacenamiento, siga estas directrices.

Directrices para todos los pools de almacenamiento

- StorageGRID incluye un pool de almacenamiento predeterminado, todos los nodos de almacenamiento, que utiliza el sitio predeterminado, todos los sitios y el nivel de almacenamiento predeterminado, todos los nodos de almacenamiento. El pool de almacenamiento de todos los nodos de almacenamiento se actualiza automáticamente cada vez que se añaden nuevos sitios de centro de datos.

> No se recomienda utilizar el grupo de almacenamiento todos los nodos de almacenamiento o el sitio todos los sitios porque estos elementos se actualizan automáticamente para incluir los sitios nuevos que agregue en una expansión, lo que podría no ser el comportamiento que desea. Antes de usar el pool de almacenamiento todos los nodos de almacenamiento o el sitio predeterminado, revise con cuidado las directrices para las copias replicadas y codificadas de borrado.

- 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.

Directrices para los pools de almacenamiento utilizados para copias replicadas

- Cree una agrupación de almacenamiento diferente para cada sitio. A continuación, especifique uno o varios grupos de almacenamiento específicos del sitio en las instrucciones de colocación de cada regla. 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 grupo de almacenamiento para el sitio nuevo. A continuación, actualice las reglas de ILM para controlar qué objetos están almacenados en el nuevo sitio.
- En general, no utilice el pool de almacenamiento predeterminado, todos los nodos de almacenamiento ni ningún pool de almacenamiento que incluya el sitio predeterminado, todos los sitios.

Directrices para los pools de almacenamiento utilizados para las copias con código de borrado

- No se pueden usar nodos de archivado para los datos codificados mediante borrado.
- El número de nodos de almacenamiento y sitios que contiene el pool de almacenamiento determina qué esquemas de codificación de borrado están disponibles.
- Si un pool de almacenamiento incluye solo dos sitios, no podrá utilizar dicho pool de almacenamiento para codificar el borrado. No hay esquemas de codificación de borrado disponibles para un pool de almacenamiento que tenga dos ubicaciones.
- En general, no utilice el pool de almacenamiento predeterminado, todos los nodos de almacenamiento ni ningún pool de almacenamiento que incluya el sitio predeterminado, todos los sitios en ningún perfil de código de borrado.

> Si el grid incluye un solo sitio, no se podrá utilizar el pool de almacenamiento todos los nodos de almacenamiento ni el sitio predeterminado todos los sitios en un perfil de código de borrado. Este comportamiento impide que el perfil de código de borrado no sea válido si se agrega un segundo sitio.

- Si tiene requisitos de alto rendimiento, no se recomienda crear 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 que se pueden lograr para la ingesta y la recuperación de objetos (cuando se seleccionan valores estrictos o equilibrados como comportamiento de procesamiento) o que podrían provocar retrasos en la cola de ILM (cuando se selecciona el Dual Commit como comportamiento de procesamiento).
- 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.

Directrices para los pools de almacenamiento utilizados para copias archivadas

- No es posible crear un pool de almacenamiento que incluya nodos de almacenamiento y Archivo. 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 de bloqueo de objetos de S3 está habilitada y se crea una regla de ILM compatible, no se puede usar un pool de almacenamiento que incluya los 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. Consulte Administre StorageGRID.

Información relacionada

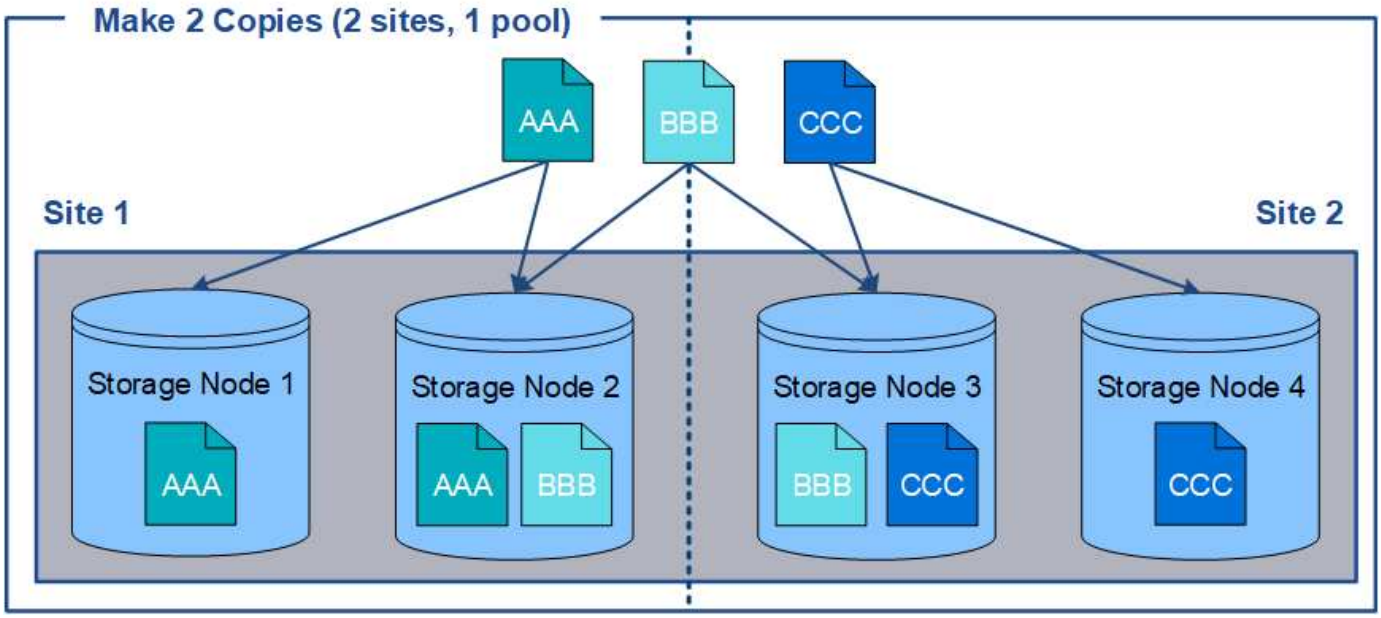
- Qué es la replicación
- Qué es la codificación de borrado
- Qué son los esquemas de codificación de borrado
- Utilice varios pools de almacenamiento para la replicación entre sitios

Utilice varios pools de almacenamiento para la replicación entre sitios

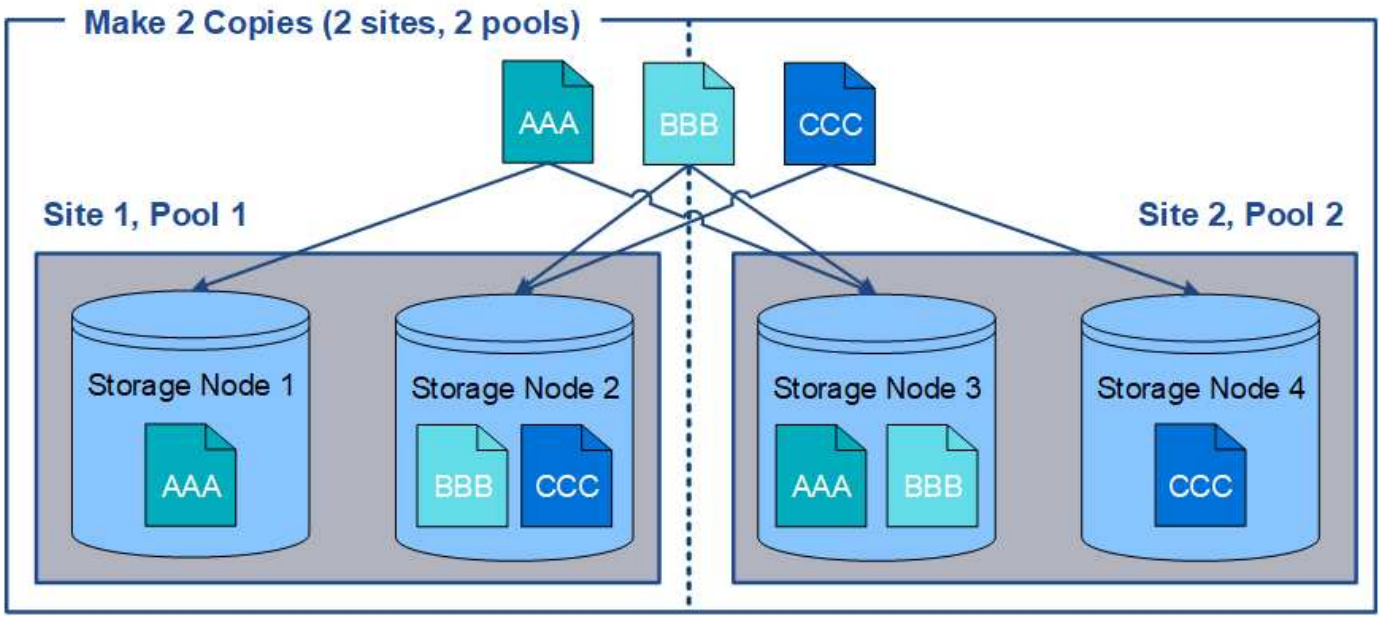
Si la implementación de StorageGRID incluye más de un sitio, puede habilitar la protección contra pérdida de sitio mediante la creación de un pool de almacenamiento para cada sitio y especificar ambos pools de almacenamiento en las instrucciones de ubicación de la regla. Por ejemplo, si configura una regla de ILM para realizar dos copias replicadas y especificar pools de almacenamiento en dos sitios, se colocará una copia de cada objeto en cada sitio. Si configura una regla para realizar dos copias y especifica

tres pools de almacenamiento, las copias se distribuyen para equilibrar el uso de disco entre los pools de almacenamiento, a la vez que se asegura de que las dos copias se almacenan en sitios diferentes.

El siguiente ejemplo ilustra qué puede suceder si una regla de ILM coloca copias de objetos replicadas en un único pool de almacenamiento que contiene nodos de almacenamiento de dos sitios. Como el sistema utiliza todos los nodos disponibles en el pool de almacenamiento cuando coloca las copias replicadas, es posible que se mantengan todas las copias de algunos objetos en solo uno de los sitios. En este ejemplo, el sistema almacenaba dos copias del objeto AAA en los nodos de almacenamiento del sitio 1 y dos copias del objeto CCC en los nodos de almacenamiento del sitio 2. Sólo se protege el objeto BBB si uno de los sitios falla o se vuelve inaccesible.



En cambio, este ejemplo muestra cómo se almacenan los objetos cuando se utilizan varios pools de almacenamiento. En el ejemplo, la regla de ILM especifica que se creen dos copias replicadas de cada objeto y que las copias se distribuyen en dos pools de almacenamiento. Cada pool de almacenamiento contiene todos los nodos de almacenamiento en un sitio. Debido a que una copia de cada objeto se almacena en cada sitio, los datos de objeto están protegidos de un fallo del sitio o falta de accesibilidad.



Al usar varios pools de almacenamiento, tenga en cuenta las siguientes reglas:

- Si crea n copias, debe añadir n o más pools de almacenamiento. Por ejemplo, si una regla está configurada para realizar tres copias, debe especificar tres o más 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 menor que el número de pools de almacenamiento, el sistema distribuye las copias para mantener el uso del disco entre los pools equilibrados y para garantizar que no se almacenen dos o más copias en la misma agrupación de almacenamiento.
- 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.

Usar un pool de almacenamiento como ubicación temporal (obsoleto)

Cuando crea una regla de ILM con una ubicación de objetos que incluya un solo pool de almacenamiento, se le solicita que especifique un segundo pool de almacenamiento que se usará como ubicación temporal.

Las ubicaciones temporales han quedado obsoletas y se eliminarán en un lanzamiento futuro. No debe seleccionar un pool de almacenamiento como ubicación temporal para una nueva regla de ILM.

> Si selecciona el comportamiento de procesamiento estricto (paso 3 del asistente Crear regla de ILM), se omitirá la ubicación temporal.

Información relacionada

Opciones de protección de datos para consumo

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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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. Seleccione el icono más ➕ para agregar una entrada para cada sitio.

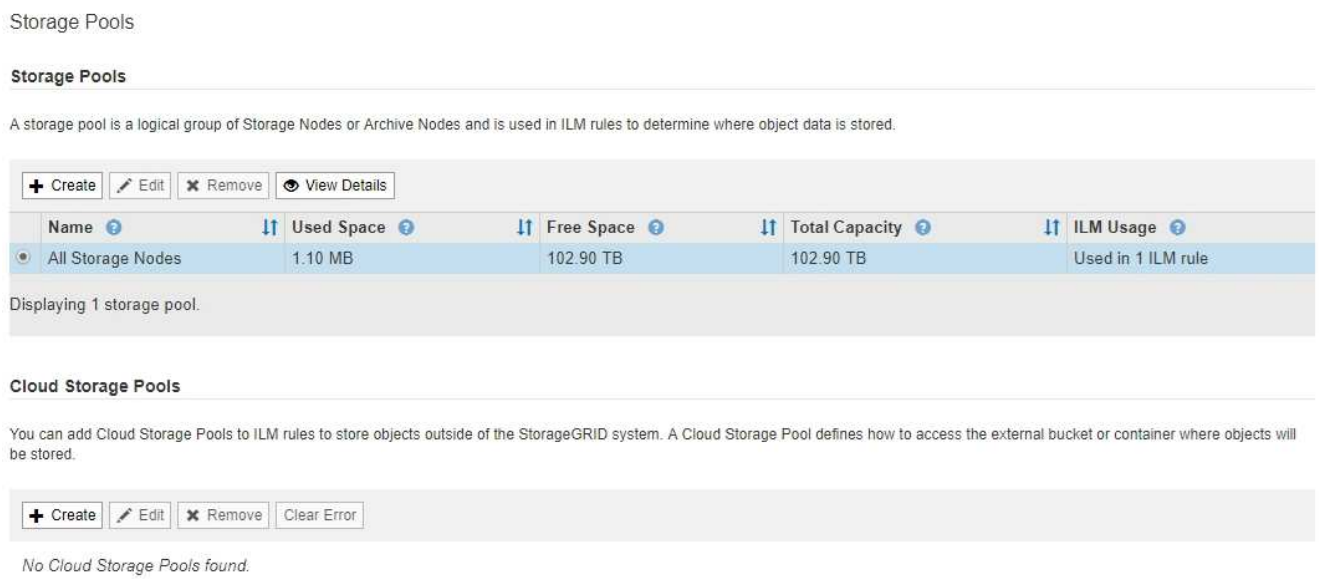
> No incluya el sitio predeterminado All Sites en un pool de almacenamiento que se utilizará en un perfil de código de borrado. En su lugar, añada una entrada independiente al pool de almacenamiento para cada instalación que almacenará los datos codificados de borrado. Consulte este paso por ejemplo.

- Si usted 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**.

   Se muestra la página Storage Pools, con una lista de todos los pools de almacenamiento definidos.



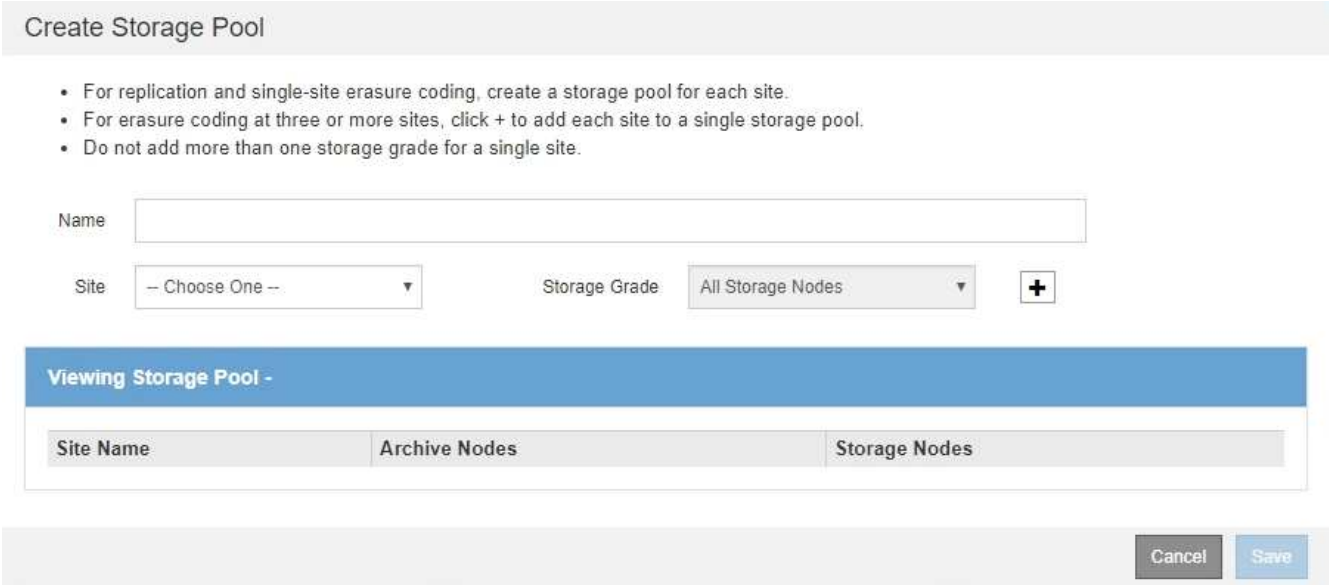
   La lista incluye el pool de almacenamiento predeterminado del sistema, todos los nodos de

almacenamiento, que utiliza el sitio predeterminado del sistema, todos los sitios y el grado de almacenamiento predeterminado, todos los nodos de almacenamiento.

> Dado que el pool de almacenamiento todos los nodos de almacenamiento se actualiza automáticamente cada vez que se agregan nuevos sitios de centros de datos, no se recomienda utilizar este pool de almacenamiento en las reglas de ILM.

2. Para crear una nueva agrupación de almacenamiento, seleccione **Crear**.

   Se muestra el cuadro de diálogo Crear un pool de almacenamiento.



3. Introduzca un nombre único para el pool de almacenamiento.

   Utilice un nombre que será 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.

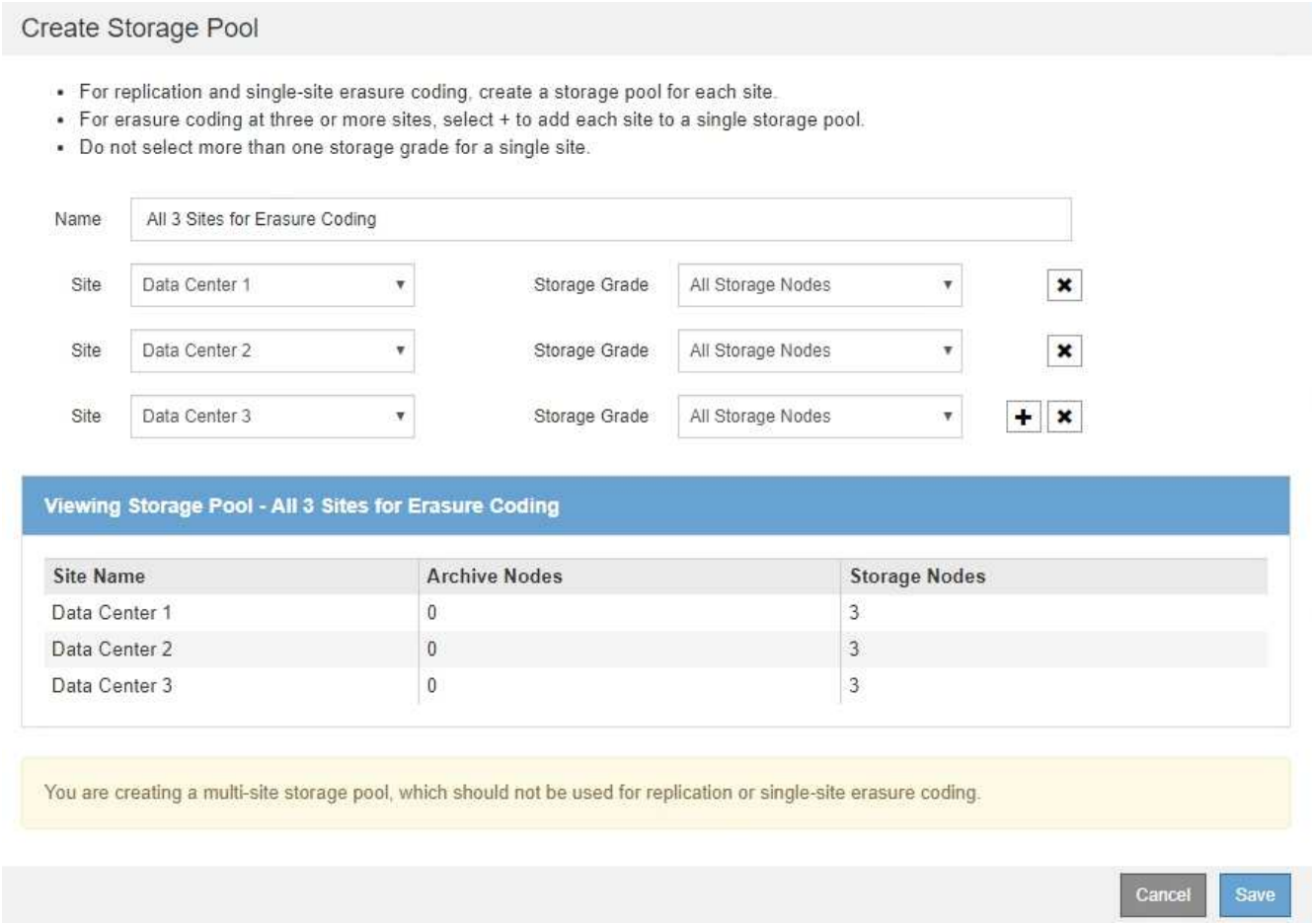
   En general, no utilice el sitio predeterminado All Sites de ningún grupo de almacenamiento. Las reglas de ILM que utilizan un pool de almacenamiento All Sites colocan los objetos en cualquier sitio disponible, lo que le otorga menos control de la ubicación de los objetos. Además, un pool de almacenamiento 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 **grado de almacenamiento**, seleccione el tipo de almacenamiento que se utilizará si una regla de ILM utiliza esta agrupación de almacenamiento.

   El nivel de almacenamiento predeterminado para todos los nodos 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 pool de almacenamiento en un perfil de codificación de borrado de varios sitios,

seleccione ➕ para agregar una entrada para cada sitio al grupo de almacenamiento.



> Se le impide crear entradas duplicadas o crear una agrupación de almacenamiento que incluya el grado de almacenamiento **nodos de archivo** y cualquier grado de almacenamiento que contenga nodos de almacenamiento.
>
> Usted es advertido si usted agrega más de una entrada para un sitio pero con diferentes grados de almacenamiento.

Para eliminar una entrada, seleccione ✖.

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.

Lo que necesitará

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

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

   Aparece la página Storage Pools. Esta página enumera todos los pools de almacenamiento definidos.

   Storage Pools

   Storage Pools

   A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

   + Create | Edit | Remove | View Details

Name	Used Space	Free Space	Total Capacity	ILM Usage
All Storage Nodes	1.88 MB	2.80 TB	2.80 TB	Used in 1 ILM rule
DC1	621.77 KB	932.42 GB	932.42 GB	Used in 2 ILM rules
DC2	675.82 KB	932.42 GB	932.42 GB	Used in 2 ILM rules
DC3	578.95 KB	932.42 GB	932.42 GB	Used in 1 ILM rule
All 3 Sites	1.88 MB	2.80 TB	2.80 TB	Used in 1 ILM rule and 1 EC profile
Archive	—	—	—	—

   Displaying 6 storage pools.

   Cloud Storage Pools

   You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

   + Create | Edit | Remove | Clear Error

   No Cloud Storage Pools found.

   En la tabla se incluye la siguiente información para cada pool de almacenamiento que incluye los nodos de almacenamiento:

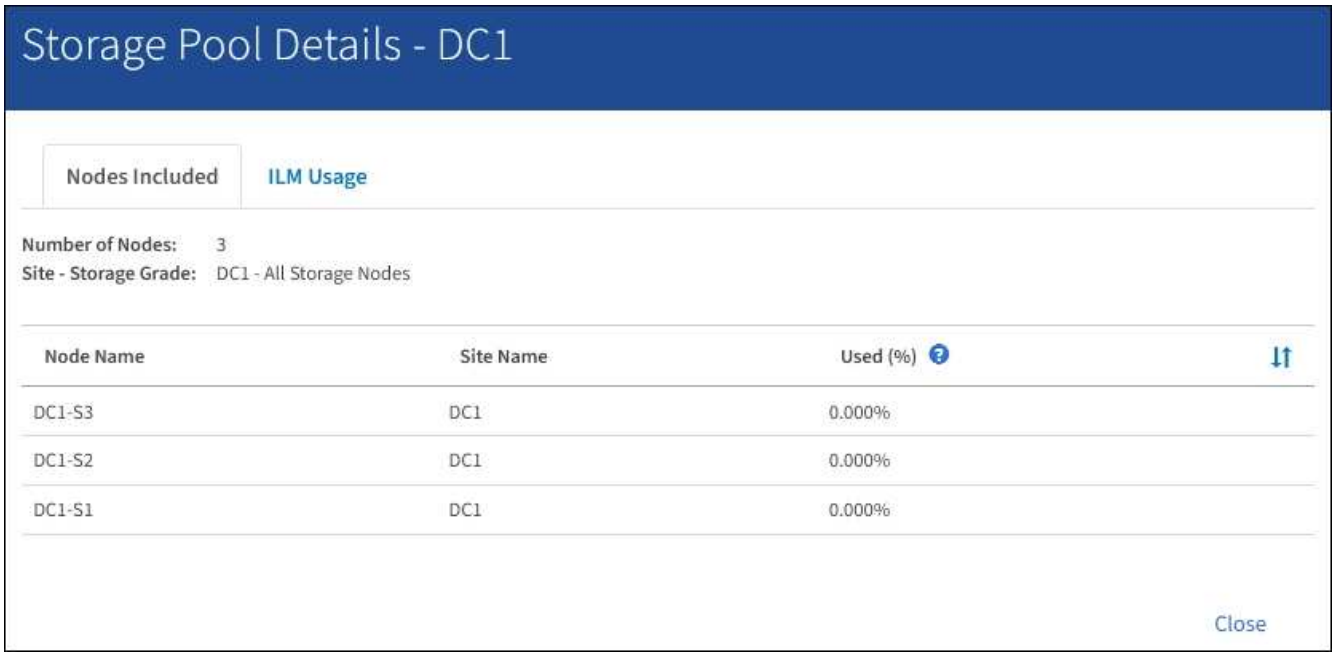
   - **Nombre**: El nombre exclusivo para mostrar de la agrupación de almacenamiento.
   - **Espacio usado**: Cantidad de espacio que se está utilizando actualmente para almacenar objetos en la agrupación de almacenamiento.
   - **Espacio libre**: La cantidad de espacio que queda disponible para almacenar objetos en la agrupación de almacenamiento.
   - **Capacidad total**: El tamaño de la agrupación de almacenamiento, que equivale a la cantidad total de espacio útil para los datos de los objetos de todos los nodos de la agrupación de almacenamiento .
   - **Uso de ILM**: Cómo se utiliza actualmente el pool de almacenamiento. Un pool de almacenamiento puede no utilizarse o utilizarse en una o varias reglas de ILM, perfiles de código de borrado o ambos.

     No se puede quitar un pool de almacenamiento si se está utilizando.

2. Para ver los detalles de una agrupación de almacenamiento específica, seleccione su botón de opción y seleccione **Ver detalles**.

   Aparecerá el mensaje Detalles del grupo de almacenamiento modal.

3. Consulte la ficha **nodos incluidos** para obtener información sobre los nodos de almacenamiento o los nodos de archivo incluidos en la agrupación de almacenamiento.



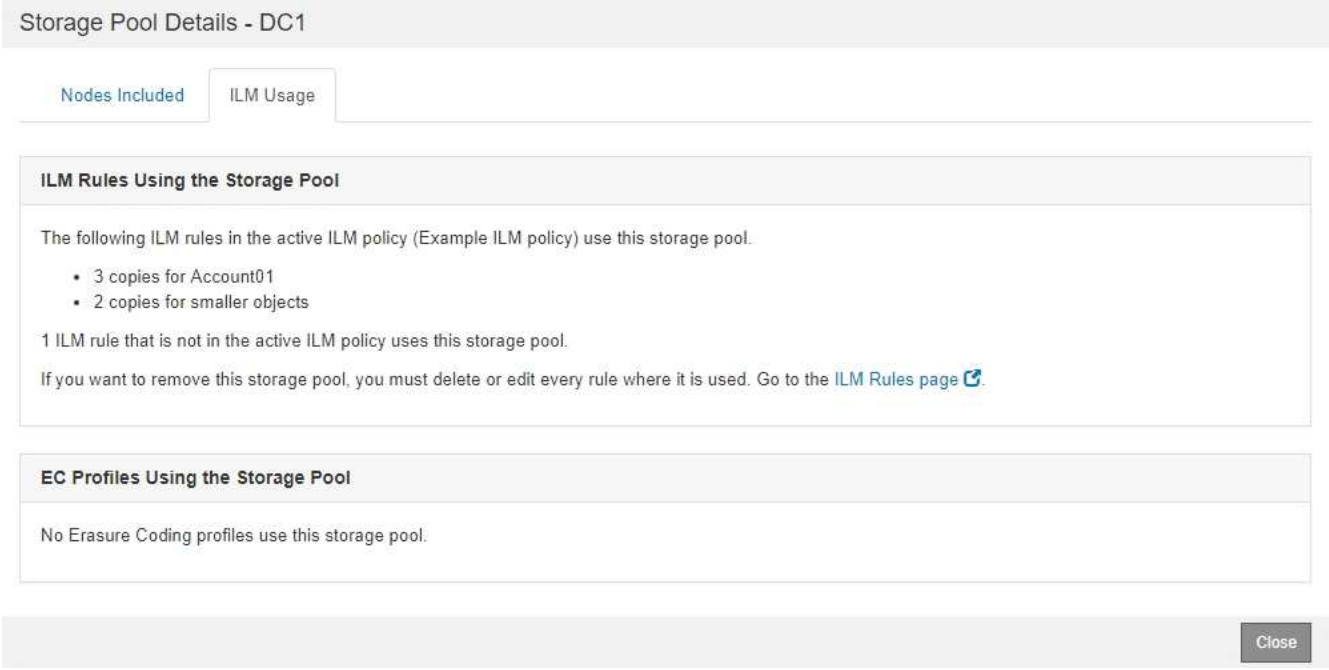
En la tabla se incluye la siguiente información para cada nodo:

- Nombre del nodo
- Nombre del sitio
- Usado (%): Para los nodos de almacenamiento, el porcentaje del espacio útil total para los datos de objeto que se han usado. Este valor no incluye metadatos de objetos.

> El mismo valor usado (%) también se muestra en el gráfico almacenamiento usado - datos de objeto para cada nodo de almacenamiento (seleccione **NODOS** > ***nodo de almacenamiento*** > **almacenamiento**).

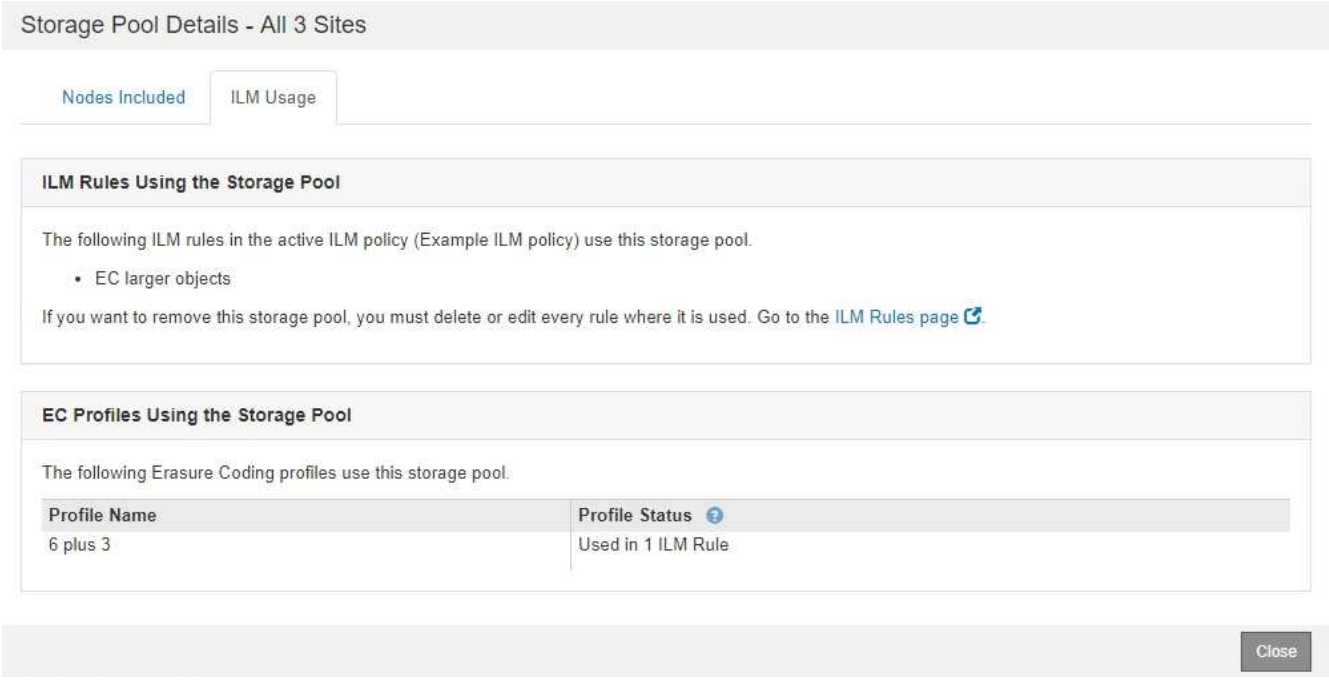
4. Seleccione la pestaña **uso de ILM** para determinar si el pool de almacenamiento se está utilizando actualmente en cualquier regla de ILM o perfil de código de borrado.

   En este ejemplo, el pool de almacenamiento de DC1 se utiliza en tres reglas de ILM: Dos reglas que están en la política de ILM activa y una regla que no está en la política activa.



No se puede quitar un pool de almacenamiento si se utiliza en una regla de ILM.

En este ejemplo, el grupo de almacenamiento All 3 Sites se utiliza en un perfil de código de borrado. A su vez, un perfil de código de borrado lo utiliza una regla de ILM en la política de ILM activa.



No se puede quitar un pool de almacenamiento si se utiliza en un perfil de código de borrado.

5. Si lo desea, visite la página **Reglas ILM** para obtener más información y administrar las reglas que utilizan el pool de almacenamiento.

   Consulte las instrucciones para trabajar con las reglas de ILM.

6. Cuando haya terminado de ver los detalles de la agrupación de almacenamiento, seleccione **Cerrar**.

Información relacionada

Trabaje con las reglas de ILM y las políticas 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Revisó las 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 nivel de almacenamiento a un pool de almacenamiento que utilice la normativa de gestión del ciclo de vida de la información activa, tenga en cuenta que los nodos de almacenamiento del nuevo nivel no se utilizarán automáticamente. Para forzar a StorageGRID a usar un nuevo nivel de almacenamiento, debe activar una nueva política de ILM después de guardar el pool de almacenamiento editado.

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

   Aparece la página Storage Pools.

2. Seleccione el botón de opción del pool de almacenamiento que desea editar.

   El pool de almacenamiento todos los nodos del almacenamiento no se puede editar.

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.

   > No podrá cambiar el sitio o el grado de almacenamiento si el pool de almacenamiento se utiliza en un perfil de código de borrado y el cambio provocaría que el esquema de codificación de borrado no sea 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 agregó un nuevo nivel de almacenamiento a un pool de almacenamiento usado en la política de ILM activa, active una nueva política de ILM para forzar a StorageGRID a usar el nuevo nivel de almacenamiento. Por ejemplo, Clone la política de ILM existente y luego active el clon.

Quitar un pool de almacenamiento

Es posible quitar un pool de almacenamiento que no se está usando.

Lo que necesitará

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

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

   Aparece la página Storage Pools.

2. Observe la columna ILM Usage de la tabla para determinar si puede eliminar el pool de almacenamiento.

   No se puede quitar un pool de almacenamiento si se está utilizando en una regla de ILM o en un perfil de código de borrado. Según sea necesario, seleccione **Ver detalles** > **uso de ILM** para determinar dónde se utiliza un pool de almacenamiento.

3. Si no se está utilizando la agrupación de almacenamiento que desea quitar, seleccione el botón de opción.
4. Seleccione **Quitar**.
5. Seleccione **OK**.

Utilice Cloud Storage Pools

Qué es un pool de almacenamiento 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 prefiera mover objetos a los que se accede con poca frecuencia a un almacenamiento en cloud de menor coste, como Amazon S3 Glacier, S3 Glacier Deep Archive o el nivel de acceso Archive en el almacenamiento 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).

En la siguiente tabla, se comparan los pools de almacenamiento con los pools de almacenamiento en el cloud y se muestran similitudes y diferencias de nivel elevado.

	Del banco de almacenamiento	Pool de almacenamiento en cloud
¿Cómo se crea?	Uso de la opción **ILM** > **agrupaciones de almacenamiento** en Grid Manager. Es necesario configurar las calificaciones de almacenamiento para poder crear el pool de almacenamiento.	Uso de la opción **ILM** > **agrupaciones de almacenamiento** 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.
¿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 o un contenedor de almacenamiento de Azure Blob que se encuentra 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 DE restauración DE objetos S3. • 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 grupo de almacenamiento en cloud. Las operaciones POSTERIORES a la restauración de objetos en el Cloud Storage Pool pueden verse afectadas por el ciclo de vida configurado.
¿Qué controla la ubicación de objetos?	Una regla de ILM en la política activa de ILM.	Una regla de ILM en la política activa de ILM.

	Del banco de almacenamiento	Pool de almacenamiento en cloud
¿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 puede almacenar un objeto en más de un grupo 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.

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.

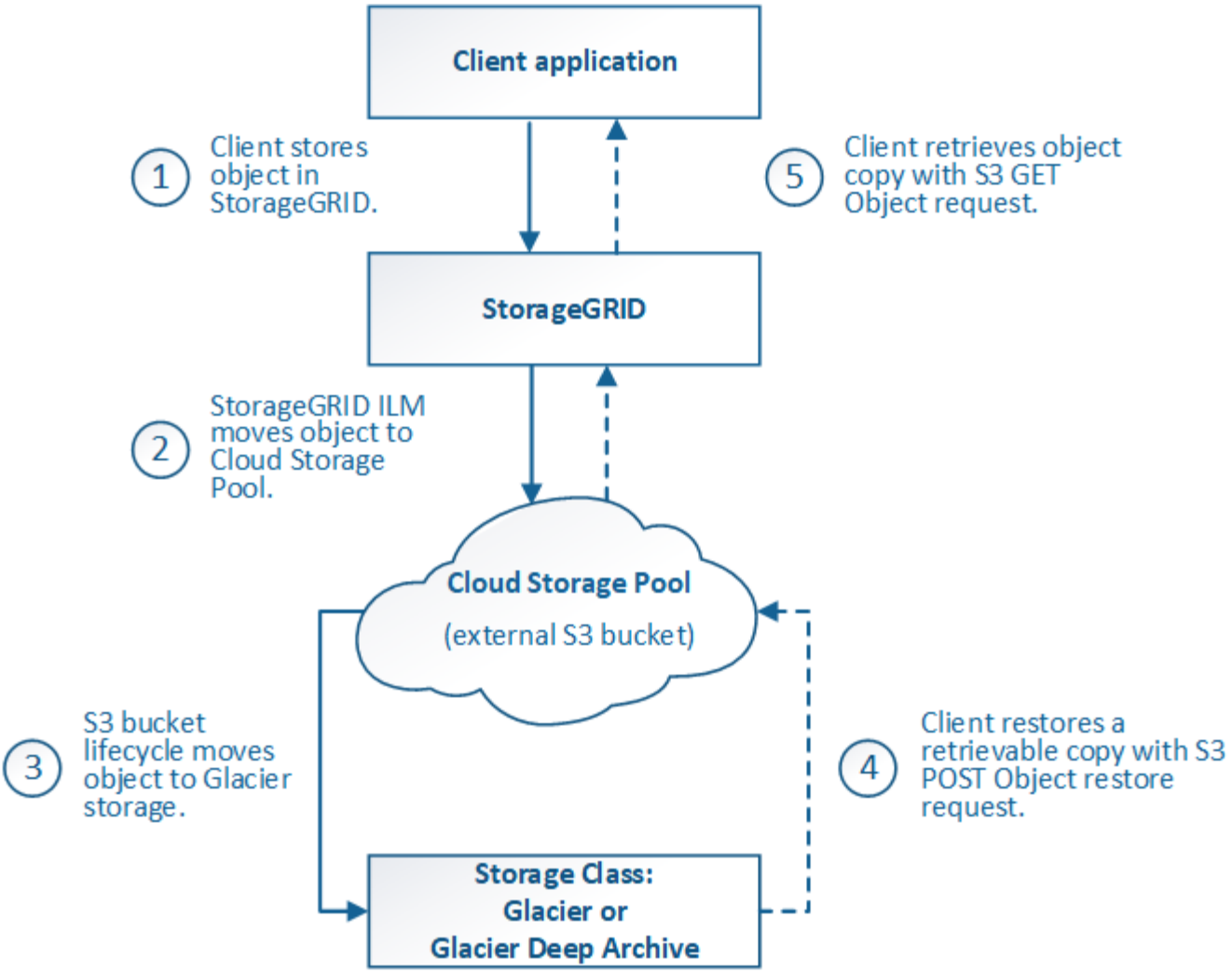
- S3: Ciclo de vida de un objeto de Cloud Storage Pool
- Azure: Ciclo de vida de un objeto de Cloud Storage Pool

S3: Ciclo de vida de un objeto de Cloud Storage Pool

En la figura, se muestran las etapas del ciclo de vida de un objeto almacenado en un pool de almacenamiento en cloud de S3.

> En la figura y las explicaciones, "'Glacier'" hace referencia 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 haya movido a S3 Cloud Storage Pool, la aplicación cliente puede recuperarlo con una solicitud DE OBJETO GET de S3 de StorageGRID, a menos que el objeto se haya migrado al almacenamiento 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 de ciclo de vida para el bloque de S3 externo y debe usar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y sea compatible con la API DE restauración DE objetos S3 POSTERIOR.

> No use Cloud Storage Pools para los objetos que han sido procesados por los clientes de Swift. Swift no admite solicitudes DE restauración POSTERIOR de objetos, por lo que StorageGRID no podrá recuperar objetos Swift que se hayan migrado 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 usar una solicitud DE objeto HEAD de S3 para supervisar el estado del objeto.

4. **Objeto restaurado desde el almacenamiento Glacier**

   Si se ha realizado la transición de un objeto al almacenamiento Glacier, la aplicación cliente puede emitir una solicitud DE restauración DE objetos S3 POSTERIOR para restaurar una copia recuperable al pool de almacenamiento en cloud de 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.

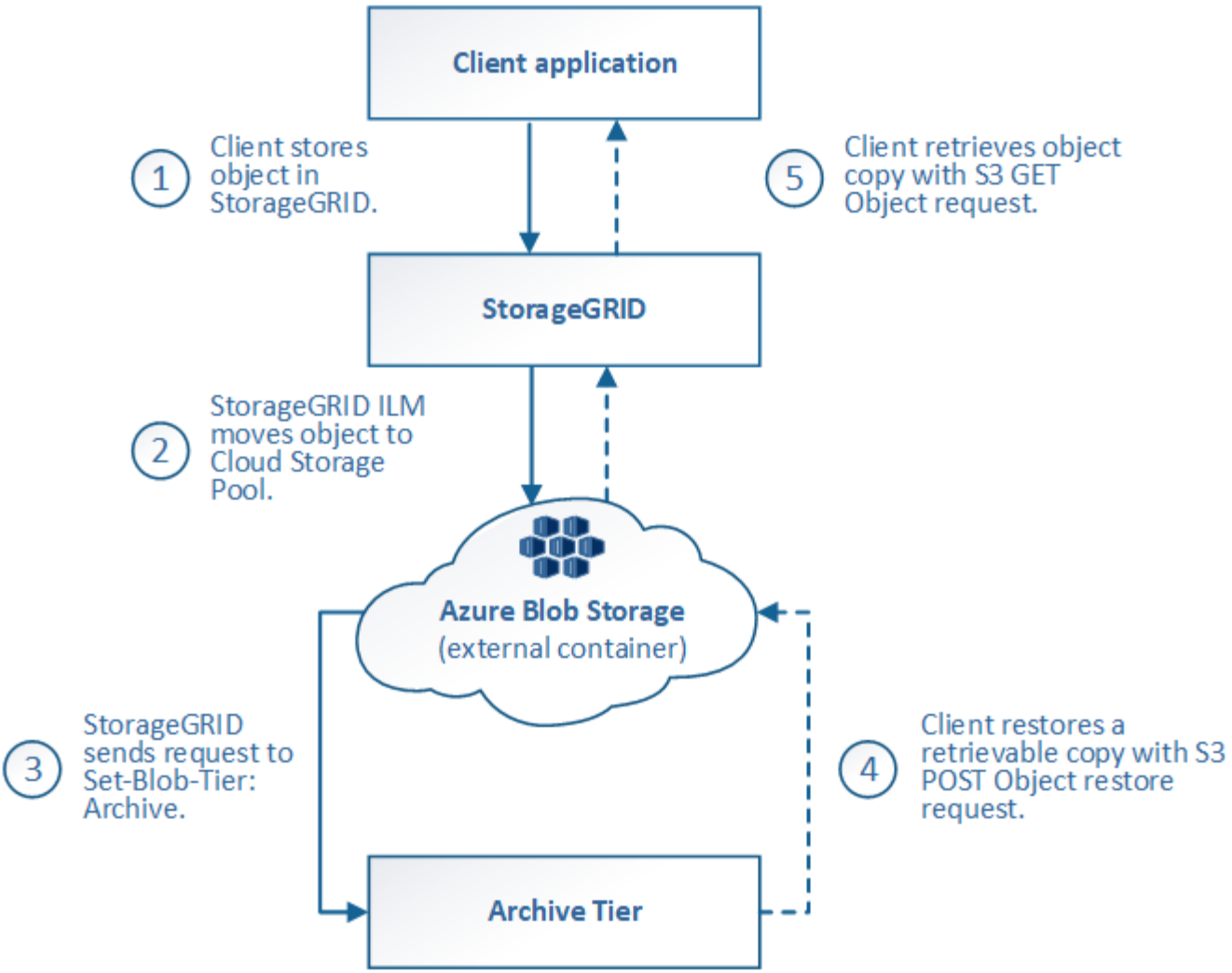
   > Si también hay una o varias copias del objeto en los nodos de almacenamiento de StorageGRID, no es necesario restaurar el objeto desde Glacier con una solicitud DE restauración POSTERIOR a objeto. En su lugar, la copia local se puede recuperar directamente, utilizando UNA solicitud GET Object.

5. **Objeto recuperado**

   Una vez restaurado un objeto, la aplicación cliente puede emitir UNA solicitud GET Object para recuperar el objeto restaurado.

Azure: Ciclo de vida de un objeto de Cloud Storage Pool

En la figura, se muestran las etapas del ciclo de vida de un objeto almacenado 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 ILM que utiliza un Azure Cloud Storage Pool como ubicación de ubicación, StorageGRID mueve el objeto al contenedor de almacenamiento externo de Azure Blob especificado por el Cloud Storage Pool

   > No use Cloud Storage Pools para los objetos que han sido procesados por los clientes de Swift. Swift no admite solicitudes POSTERIORES a la restauración de objetos, por lo que StorageGRID no podrá recuperar objetos de Swift que se hayan migrado 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 se ha realizado la transición de un objeto al nivel de archivado, la aplicación cliente puede emitir una solicitud DE restauración DE objetos S3 POSTERIOR para restaurar una copia recuperable a Azure Cloud Storage Pool.

Cuando StorageGRID recibe LA restauración DE objetos POSTERIOR, este realiza una transición temporal del objeto al nivel de refrigeración del almacenamiento de Azure Blob. Tan pronto como se alcanza la fecha de vencimiento de la solicitud DE restauración DE objeto POSTERIOR, StorageGRID realiza la transición del objeto de nuevo al nivel de archivado.

> Si también existen una o varias copias del objeto en los nodos de almacenamiento dentro de StorageGRID, no es necesario restaurar el objeto desde el nivel de acceso de archivado mediante la emisión de una solicitud DE restauración DE objetos POSTERIOR. En su lugar, la copia local se puede recuperar directamente, utilizando UNA solicitud GET Object.

5. **Objeto recuperado**

   Una vez que se ha restaurado un objeto en Azure Cloud Storage Pool, la aplicación cliente puede emitir una solicitud GET Object para recuperar el objeto restaurado.

Información relacionada

Use S3

Cuándo usar Cloud Storage Pools

Los pools de almacenamiento en cloud pueden proporcionar ventajas importantes en diversos casos de uso.

Realizar backup de los datos de StorageGRID en una ubicación externa

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 deba emitir la solicitud de restauración DE objetos S3 POST para acceder a la copia de objeto de backup en el 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.

Organizar en niveles los datos de StorageGRID en 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 pools de almacenamiento en cloud si desea organizar en niveles o realizar backups de datos de objetos en más de un cloud. Los filtros de las reglas de ILM permiten especificar los objetos que se almacenan en cada Cloud Storage Pool. Por ejemplo, puede que desee almacenar objetos de algunos inquilinos o bloques en Amazon S3 Glacier y objetos de otros inquilinos o bloques 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 utilice varios pools de almacenamiento en cloud, tenga en cuenta que un objeto se puede almacenar solo en un pool de almacenamiento en cloud 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 use Cloud Storage Pools para los objetos que han sido procesados por los clientes de Swift. Swift no admite solicitudes POSTERIORES a la restauración de objetos, por lo que StorageGRID no podrá recuperar objetos de Swift que se hayan migrado al almacenamiento S3 Glacier ni al nivel 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.

Información necesaria para crear un pool de almacenamiento en cloud

Antes de poder crear un Cloud Storage Pool, debe crear el bloque de S3 externo o el contenedor de almacenamiento externo de Azure Blob que utilizará para el Cloud Storage Pool. A continuación, cuando cree el pool de almacenamiento en cloud en StorageGRID, debe especificar la siguiente información:

- El tipo de proveedor: Almacenamiento Amazon S3 o Azure Blob.
- Si selecciona Amazon S3, si Cloud Storage Pool va a utilizarse con la región secreta de AWS (**CAP (Portal de acceso C2S)**).
- El nombre exacto del contenedor o contenedor.
- El extremo de servicio necesario para acceder al bloque o contenedor.
- La autenticación necesaria para acceder al bloque o contenedor:
  - **S3**: Opcionalmente, un ID de clave de acceso y una clave de acceso secreta.
  - **C2S**: La dirección URL completa para obtener credenciales temporales del servidor CAP; un certificado de CA del servidor, un certificado de cliente, una clave privada para el certificado de cliente y, si la clave privada está cifrada, la frase de acceso para descifrarla.
  - **Almacenamiento de Azure Blob**: Un nombre de cuenta y una clave de cuenta. Estas credenciales deben tener permiso completo para el contenedor.
- De manera opcional, un certificado de CA personalizado para verificar las conexiones TLS al bloque o contenedor.

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 Configure 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, sólo tiene que volver a configurar las reglas y la política 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 externo S3 especificado en el Cloud Storage Pool está controlado por las reglas de ILM y la política activa de ILM 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 bloque externo de S3. Debe usar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y sea compatible CON la API DE restauración POSTERIOR a objetos de S3.

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 utilice la gestión del ciclo de vida del almacenamiento BLOB de Azure para el contenedor utilizado con un Cloud Storage Pool. 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

- S3: Especifique los detalles de autenticación para un pool de almacenamiento en cloud
- C2S S3: Especifique los detalles de la autenticación de un pool de almacenamiento en el cloud
- Azure: Especifique detalles de autenticación para un pool de almacenamiento en cloud

Comparación de 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?	Un pool de almacenamiento en cloud 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. Es decir, en lugar de conservar dos copias en las instalaciones, solo puede conservar una copia en StorageGRID y enviar una copia al Cloud Storage Pool.	El servicio de replicación de CloudMirror permite que un inquilino replique automáticamente objetos de un bloque en StorageGRID (origen) en un bloque de S3 externo (destino). La replicación de CloudMirror crea una copia independiente de un objeto en una infraestructura de S3 independiente.
¿Cómo se configura?	Los pools de almacenamiento en cloud se definen del mismo modo que los pools de almacenamiento, mediante Grid Manager o la API de gestión de grid. Puede seleccionar un Cloud Storage Pool 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	• Cualquier infraestructura compatible de S3 (incluido Amazon S3)

	Pool de almacenamiento en cloud	Servicio de replicación de CloudMirror
¿Qué hace que los objetos se muevan al destino?	Una o varias reglas de ILM en la política activa de ILM. Las reglas de ILM definen los objetos que StorageGRID se mueve al Cloud Storage Pool y cuándo se mueven los objetos.	La acción de incluir un nuevo objeto en un bloque de origen que se haya configurado con un extremo de CloudMirror.los objetos que existían en el bloque de origen antes de que se configurara el bloque con el extremo de CloudMirror no se replican, a menos que se modifiquen.
¿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 en el 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

Cuando crea un Cloud Storage Pool, debe especificar el nombre y la ubicación del bloque o contenedor externo que StorageGRID utilizará para almacenar objetos, el tipo de proveedor cloud (Amazon S3 o Azure Blob Storage) y la información que StorageGRID necesita para acceder a la bloque o el contenedor externo.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha revisado las directrices para configurar Cloud Storage Pools.
- El bloque o contenedor externo al que hace referencia el Cloud Storage Pool ya existe.
- Tiene toda la información de autenticación necesaria para acceder al bloque o contenedor.

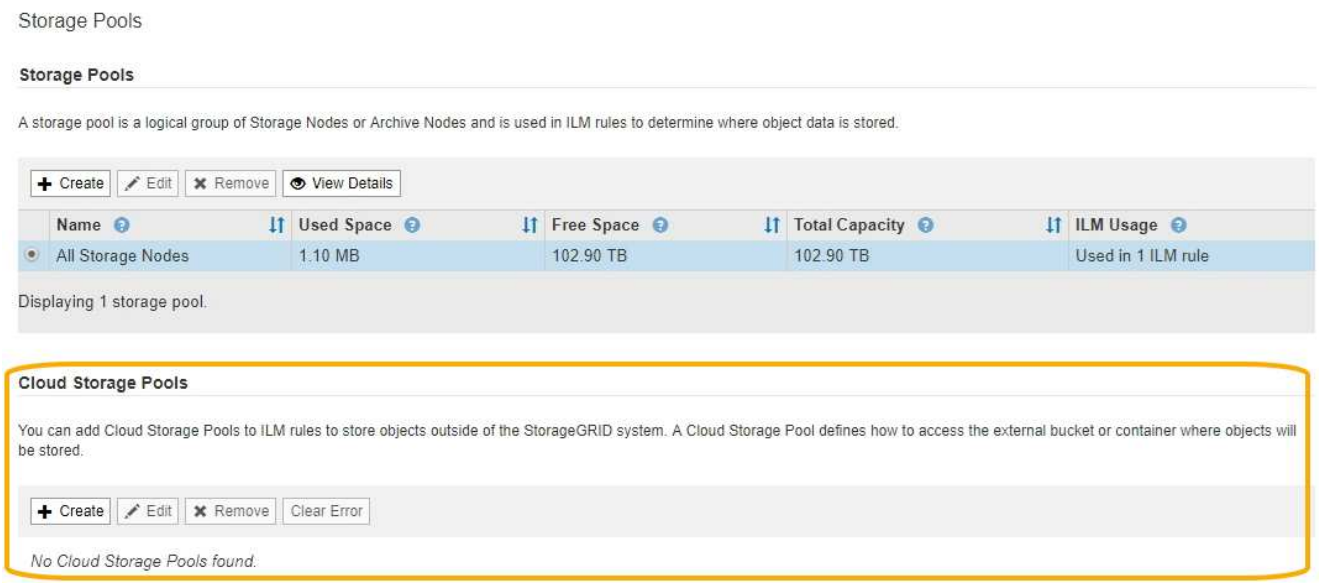
Acerca de esta tarea

Un Cloud Storage Pool especifica un único bloque de almacenamiento S3 externo o Azure Blob. 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.

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

   Aparece la página Storage Pools. Esta página incluye dos secciones: Pools de almacenamiento y pools de almacenamiento en cloud.



2. En la sección Cloud Storage Pools de la página, seleccione **Crear**.

   Se muestra el cuadro de diálogo Crear un pool de almacenamiento en cloud.

3. Introduzca la siguiente información:

Campo	Descripción
Nombre para mostrar	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**: Seleccione esta opción para un extremo S3, C2S S3 o Google Cloud Platform (GCP). • **Almacenamiento de Azure Blob** **Nota:** cuando selecciona un Tipo de proveedor, las secciones de extremo de servicio, autenticación y verificación de servidor aparecen en la parte inferior de la página.
Cucharón o contenedor	El nombre del bloque de S3 externo o del contenedor de Azure que se creó para el pool de almacenamiento en cloud. Se producirá un error en el nombre que especifique aquí para que coincida exactamente con el nombre del bloque o contenedor, o bien se producirá un error al crear el pool de almacenamiento en cloud. No se puede cambiar este valor después de guardar el pool de almacenamiento en cloud.

4. Complete las secciones Service Endpoint, Authentication and Server Verification de la página, según el tipo de proveedor seleccionado.
   - S3: Especifique los detalles de autenticación para un pool de almacenamiento en cloud
   - C2S S3: Especifique los detalles de la autenticación de un pool de almacenamiento en el cloud
   - Azure: Especifique detalles de autenticación para un pool de almacenamiento en cloud

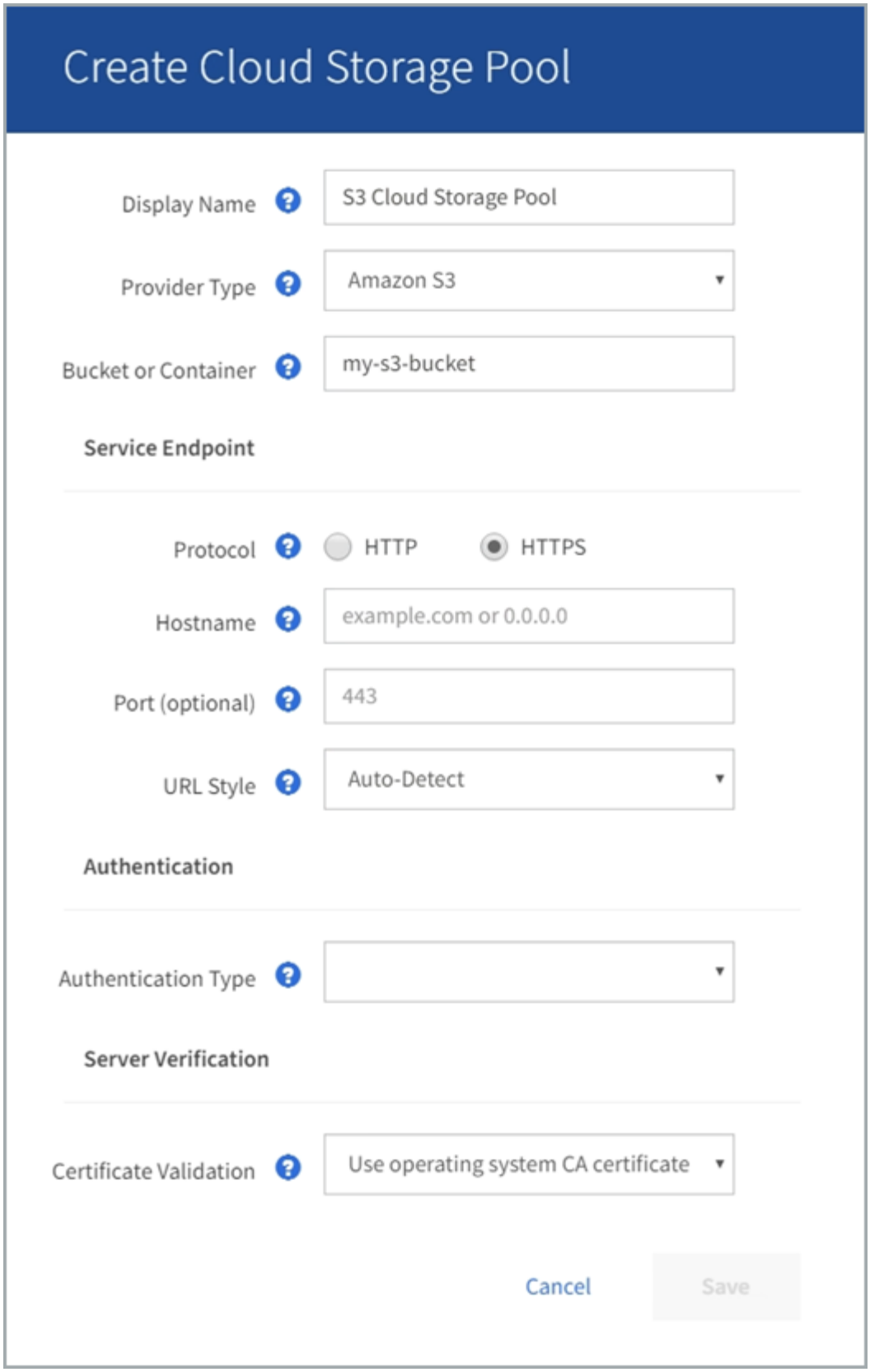
S3: Se especifican detalles de autenticación para un pool de almacenamiento en cloud

Al crear un Cloud Storage Pool para S3, debe seleccionar el tipo de autenticación

requerido para el extremo de Cloud Storage Pool. Puede especificar Anónimo o introducir un ID de clave de acceso y una clave de acceso secreta.

Lo que necesitará

- Ha introducido la información básica para Cloud Storage Pool y ha especificado **Amazon S3** como tipo de proveedor.



- Si utiliza la autenticación de clave de acceso, conoce el identificador de clave de acceso y la clave de acceso secreta del bloque S3 externo.

Pasos

1. En la sección **Service Endpoint**, proporcione la siguiente información:

a. Seleccione el protocolo que desea utilizar al conectarse al Cloud Storage Pool.

   El protocolo predeterminado es HTTPS.

b. Introduzca el nombre de host o la dirección IP del servidor del grupo de almacenamiento en cloud.

   Por ejemplo:

   `s3-aws-region.amazonaws.com`

   > No incluya el nombre del segmento en este campo. Incluye el nombre del segmento en el campo **cucharón o contenedor**.

a. Opcionalmente, especifique el puerto que se debe utilizar al conectarse al Cloud Storage Pool.

   Deje este campo vacío para utilizar el puerto predeterminado: Puerto 443 para HTTPS o puerto 80 para HTTP.

b. Seleccione el estilo de la URL para el bucket de Cloud Storage Pool:

Opción	Descripción
Estilo de alojamiento virtual	Utilice una URL de estilo alojado virtual para acceder al bloque. Las URL de estilo alojado virtual incluyen el nombre de bloque como parte del nombre de dominio, por ejemplo `https://bucket-name.s3.company.com/key-name`.
Estilo de trazado	Utilice una dirección URL de estilo de ruta para acceder al bloque. Las direcciones URL de estilo de ruta incluyen el nombre de bloque al final, por ejemplo `https://s3.company.com/bucket-name/key-name`. **Nota:** la dirección URL de estilo de ruta está en desuso.
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.

2. En la sección **autenticación**, seleccione el tipo de autenticación que se requiere para el extremo de Cloud Storage Pool.

Opción	Descripción
Clave de acceso	Se requiere un identificador de clave de acceso y una clave de acceso secreta para acceder al bloque del pool de almacenamiento en cloud.

Opción	Descripción
Anónimo	Todos tienen acceso al bloque de pools de almacenamiento en cloud. No se requieren un identificador de clave de acceso ni una clave de acceso secreta.
CAP (Portal de acceso C2S)	Se utiliza únicamente para C2S S3. Vaya a. C2S S3: Especificar detalles de autenticación de un pool de almacenamiento en el cloud.

3. Si seleccionó Access Key, introduzca la siguiente información:

Opción	Descripción
ID de clave de acceso	El ID de clave de acceso de la cuenta a la que pertenece el bloque externo.
Clave de acceso secreta	La clave de acceso secreta asociada.

4. En la sección Server Verification, seleccione el método que debe utilizarse para validar el certificado de conexiones TLS con el pool de almacenamiento de cloud:

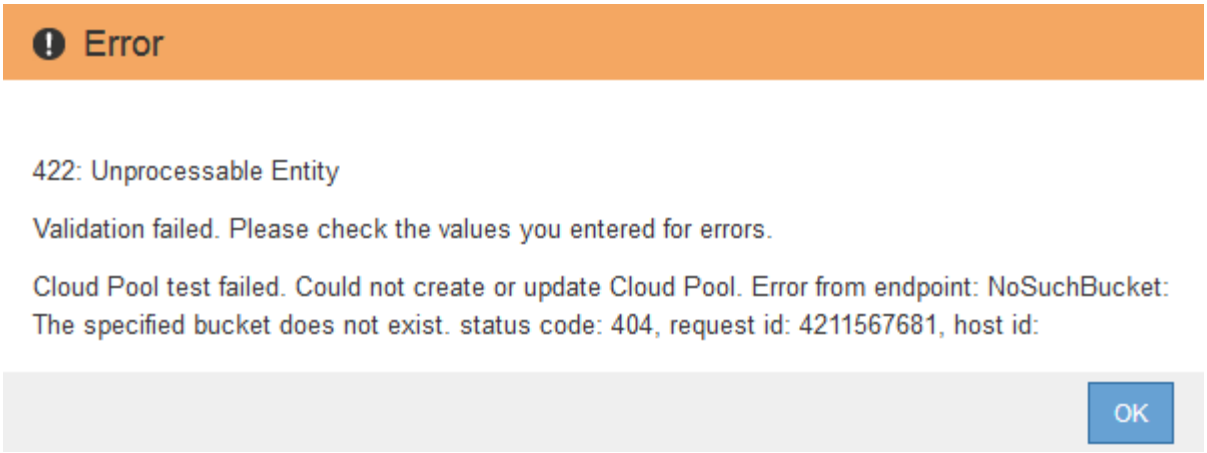
Opción	Descripción
Utilizar certificado de CA del sistema operativo	Utilice los certificados de CA de cuadrícula predeterminados instalados en el sistema operativo para asegurar las conexiones.
Utilizar certificado de CA personalizado	Usar un certificado de CA personalizado. Seleccione **Seleccionar nuevo** y cargue el certificado de CA codificado con PEM.
No verifique el certificado	El certificado utilizado para la conexión TLS no se verifica.

5. Seleccione **Guardar**.

Cuando guarda un pool de almacenamiento en cloud, StorageGRID hace lo siguiente:

- Valida que el bloque y el extremo de servicio existen y que se pueden alcanzar utilizando las credenciales especificadas.
- Escribe un archivo de marcador en el bloque para identificar el bloque como un pool de almacenamiento en el cloud. 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, se puede informar un error si existe un error de certificado o si el bloque especificado no existe todavía.



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.

C2S S3: Especifique los detalles de la autenticación de un pool de almacenamiento en el cloud

Para utilizar el servicio S3 de Commercial Cloud Services (C2S) como un Pool de almacenamiento en cloud, debe configurar C2S Access Portal (CAP) como el tipo de autenticación, de modo que StorageGRID pueda solicitar credenciales temporales para acceder al bloque de S3 de su cuenta C2S.

Lo que necesitará

- Introdujo la información básica de un pool de almacenamiento en cloud de Amazon S3, incluido el extremo de servicio.
- Conoce la dirección URL completa que StorageGRID utilizará para obtener credenciales temporales del servidor CAP, incluidos todos los parámetros API necesarios y opcionales asignados a su cuenta C2S.
- Tiene un certificado de CA de servidor emitido por una entidad de certificación gubernamental (CA) correspondiente. StorageGRID utiliza este certificado para comprobar la identidad del servidor CAP. El certificado de CA del servidor debe utilizar la codificación PEM.
- Tiene un certificado de cliente emitido por una autoridad de certificación gubernamental (CA) correspondiente. 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.
- Tiene una clave privada codificada en PEM para el certificado de cliente.
- Si la clave privada del certificado de cliente está cifrada, tendrá la frase de contraseña para descifrarla.

Pasos

1. En la sección **autenticación**, seleccione **CAP (Portal de acceso de C2S)** en el menú desplegable **Tipo de autenticación**.

   Aparecen los campos de autenticación CAP C2S.

Create Cloud Storage Pool

Display Name: C2S Cloud Storage Pool

Provider Type: Amazon S3

Bucket or Container: my-c2s-bucket

Service Endpoint

Protocol: HTTP HTTPS

Hostname: s3-aws-region.amazonaws.com

Port (optional): 443

URL Style: Auto-Detect

Authentication

Authentication Type: CAP (C2S Access Portal)

Temporary Credentials URL: https://example.com/CAP/api/v1/cred

Server CA Certificate: Select New

Client Certificate: Select New

Client Private Key: Select New

Client Private Key Passphrase (optional):

Server Verification

Certificate Validation: Use operating system CA certificate

Cancel Save

2. Proporcione la siguiente información:
   a. Para **URL de credenciales temporales**, introduzca la dirección URL completa que StorageGRID utilizará para obtener credenciales temporales del servidor CAP, incluidos todos los parámetros API necesarios y opcionales asignados a su cuenta C2S.
   b. Para **Certificado CA de servidor**, seleccione **Seleccionar nuevo** y cargue el certificado de CA codificado con PEM que StorageGRID utilizará para verificar el servidor CAP.
   c. Para **Certificado de cliente**, seleccione **Seleccionar nuevo** y cargue el certificado codificado con PEM que StorageGRID utilizará para identificarse al servidor CAP.
   d. Para **clave privada de cliente**, seleccione **Seleccionar nuevo** y cargue la clave privada codificada con PEM para el certificado de cliente.

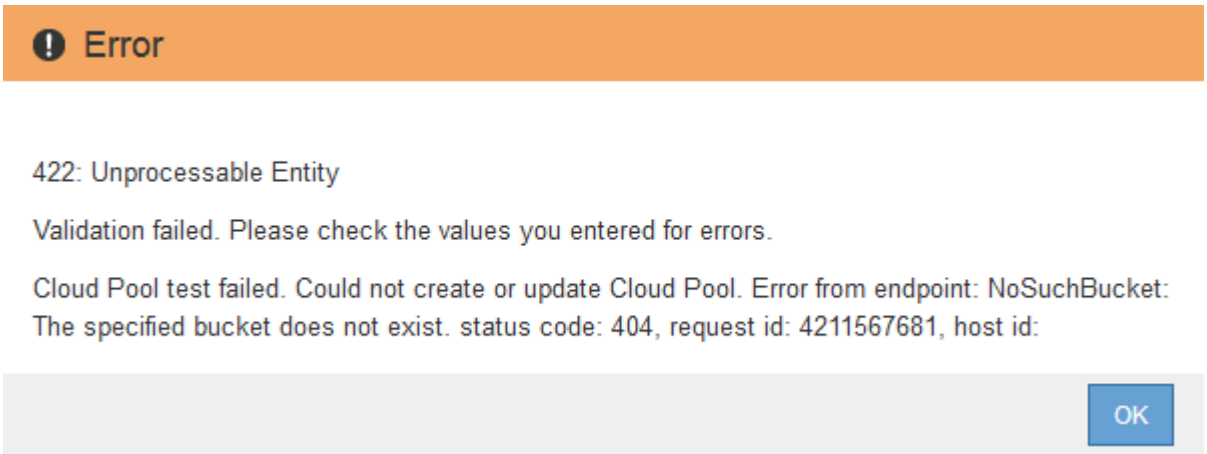
      Si la clave privada está cifrada, se debe utilizar el formato tradicional. (No se admite el formato cifrado PKCS #8).

   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 **frase de paso de clave privada cliente**.
3. En la sección Server Verification, introduzca la siguiente información:
   a. Para **validación de certificados**, seleccione **utilizar certificado de CA personalizado**.
   b. Seleccione **Seleccionar nuevo** y cargue el certificado de CA codificado con PEM.
4. Seleccione **Guardar**.

Cuando guarda un pool de almacenamiento en cloud, StorageGRID hace lo siguiente:

- Valida que el bloque y el extremo de servicio existen y que se pueden alcanzar utilizando las credenciales especificadas.
- Escribe un archivo de marcador en el bloque para identificar el bloque como un pool de almacenamiento en el cloud. 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, se puede informar un error si existe un error de certificado o si el bloque especificado no existe todavía.



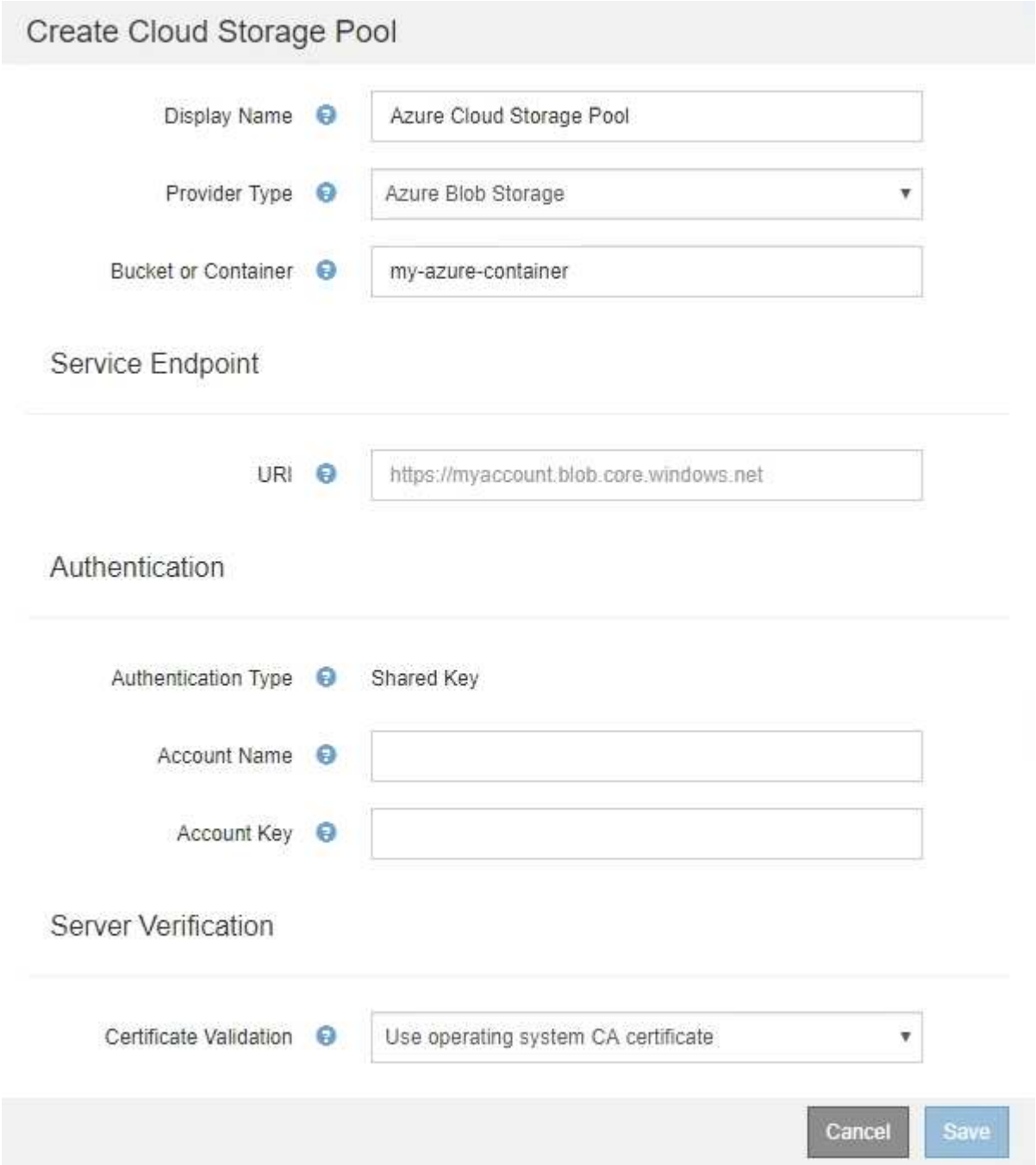
Consulte las instrucciones para Solución de problemas de Cloud Storage Pools, Resuelva el problema e intente volver a guardar el grupo de almacenamiento en la nube.

Azure: Especifique detalles de autenticación para un pool de almacenamiento en cloud

Cuando crea un Cloud Storage Pool para el almacenamiento BLOB de Azure, debe especificar un nombre de cuenta y una clave de cuenta para el contenedor externo que StorageGRID utilizará para almacenar objetos.

Lo que necesitará

- Ha introducido la información básica para Cloud Storage Pool y ha especificado **Azure Blob Storage** como tipo de proveedor. **Clave compartida** aparece en el campo **Tipo de autenticación**.



- Conoce el identificador uniforme de recursos (URI) que se utiliza para acceder al contenedor de almacenamiento BLOB que se utiliza para el pool de almacenamiento cloud.
- Conoce el nombre de la cuenta de almacenamiento y la clave secreta. Puede usar el portal de Azure para

encontrar estos valores.

Pasos

1. En la sección **Service Endpoint**, introduzca el Identificador uniforme de recursos (URI) que se utiliza para acceder al contenedor de almacenamiento BLOB utilizado para el Pool de almacenamiento en la nube.

   Especifique el URI en uno de los siguientes formatos:

   - `https://host:port`
   - `http://host:port`

   Si no especifica un puerto, el puerto 443 se utiliza de manera predeterminada para los URI HTTPS y el puerto 80 se utiliza para los URI HTTP. + + **ejemplo URI para el contenedor de almacenamiento Azure Blob**:
   `https://myaccount.blob.core.windows.net`

2. En la sección **autenticación**, proporcione la siguiente información:

   a. Para **Nombre de cuenta**, introduzca el nombre de la cuenta de almacenamiento Blob que posee el contenedor de servicios externo.

   b. Para **clave de cuenta**, introduzca la clave secreta de la cuenta de almacenamiento Blob.

   Para los extremos de Azure, se debe usar la autenticación de clave compartida.

3. En la sección **verificación del servidor**, seleccione el método que debe utilizarse para validar el certificado para las conexiones TLS con el grupo de almacenamiento en la nube:

Opción	Descripción
Utilizar certificado de CA del sistema operativo	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 **Seleccionar nuevo** y cargue el certificado codificado con PEM.
No verifique el certificado	El certificado utilizado para la conexión TLS no se verifica.

4. Seleccione **Guardar**.

Cuando guarda un pool de almacenamiento en cloud, StorageGRID hace lo siguiente:

- Valida que el contenedor y el URI existen y que se puede alcanzar utilizando las credenciales especificadas.
- Escribe un archivo marcador en el contenedor para identificarlo como un pool de almacenamiento en el cloud. 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, es posible que se notifique un error si existe un error de certificado o el contenedor especificado no existe todavía.

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.

Editar un pool de almacenamiento en el cloud

Puede editar un pool de almacenamiento en cloud para cambiar su nombre, extremo de servicio u otros detalles; sin embargo, no puede cambiar el bloque de S3 o el contenedor de Azure para un pool de almacenamiento en cloud.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha revisado el Consideraciones para Cloud Storage Pools.

Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

   Aparece la página Storage Pools. En la tabla Cloud Storage Pools, se enumera los pools de almacenamiento en el cloud.

   Cloud Storage Pools

   You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

   + Create | Edit | Remove | Clear Error

	Pool Name	URI	Pool Type	Container	Used in ILM Rule	Last Error
◉	azure-endpoint	https://storagegrid.blob.core.windows.net	azure	azure-3	✔	
○	s3-endpoint	https://s3.amazonaws.com	s3	s3-1	✔	

   Displaying 2 pools.

2. Seleccione el botón de opción del pool de almacenamiento en cloud que desea editar.
3. Seleccione **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, ni el bloque de S3 o el contenedor de Azure para un pool de almacenamiento en cloud.

   Si ha cargado previamente un certificado de servidor o cliente, puede seleccionar **Ver actual** para revisar el certificado que se está utilizando 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 que no se utilice en una regla de ILM y que no contenga datos de objetos.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- 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 se denomina `x-ntap-sgws-cloud-pool-uuid`.

- Ya ha quitado todas las reglas de ILM que pueden haber usado el pool.

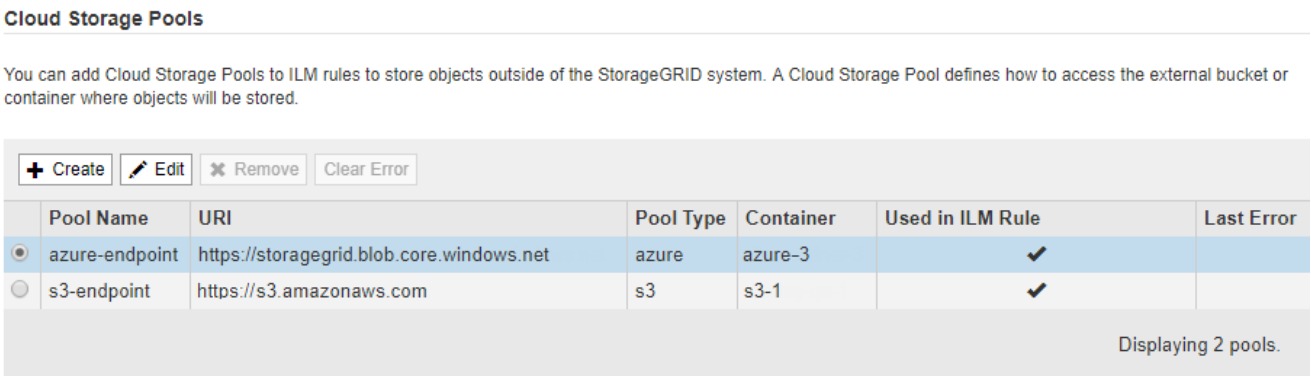
Pasos

1. Seleccione **ILM** > **agrupaciones de almacenamiento**.

   Aparece la página Storage Pools.

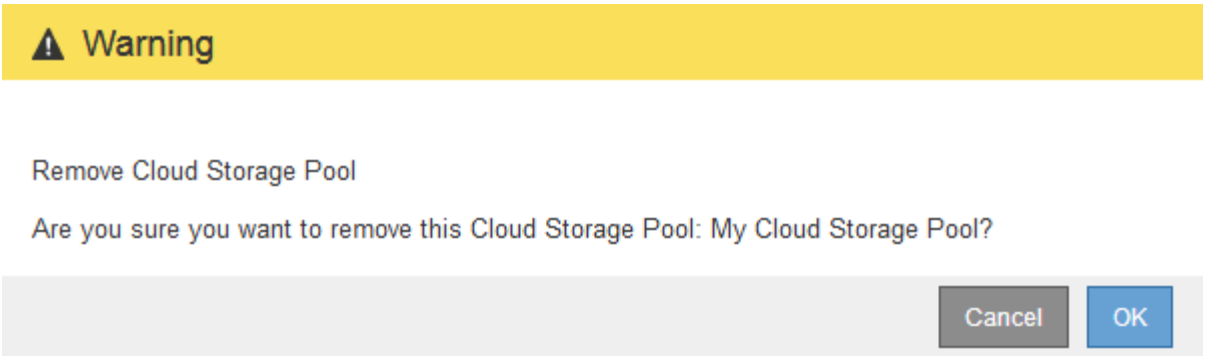
2. Seleccione el botón de opción de un pool de almacenamiento en cloud que no se utilice actualmente en una regla de ILM.

   No puede quitar un pool de almacenamiento en cloud si se utiliza en una regla de ILM. El botón **Quitar** está desactivado.



3. Seleccione **Quitar**.

   Aparecerá una advertencia de confirmación.



4. Seleccione **OK**.

   El pool de almacenamiento en cloud se elimina.

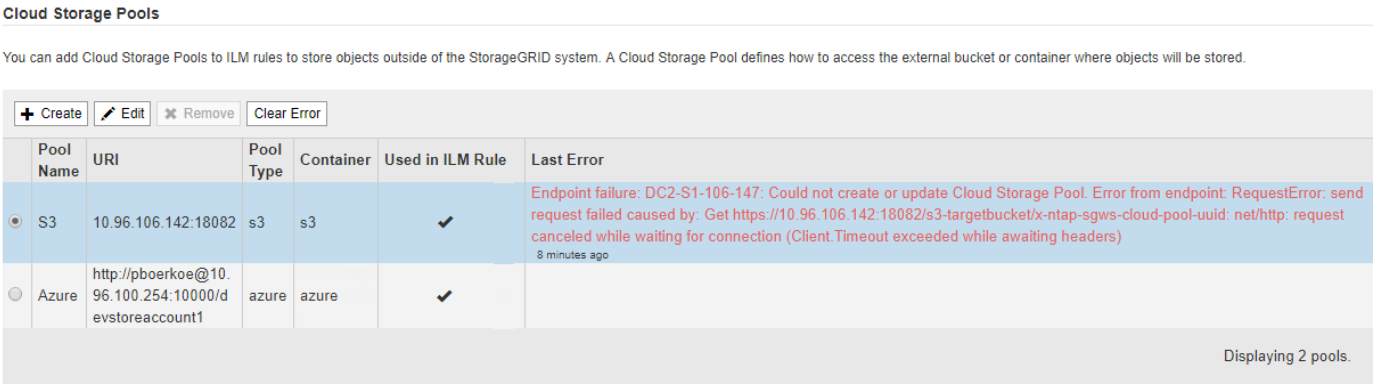
Solucione problemas de Cloud Storage Pools

Si se encuentran errores al crear, editar o eliminar un pool de almacenamiento en el cloud, siga estos pasos para resolver el problema.

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 columna Last error de la tabla Cloud Storage Pools en 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.

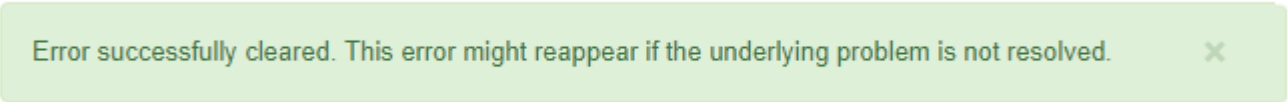


Además, se activa una alerta de error * de conectividad del grupo de almacenamiento en cloud* si la comprobación del estado detecta que se han producido uno o varios errores nuevos de Cloud Storage Pool en los últimos 5 minutos. Si recibe una notificación por correo electrónico para esta alerta, vaya a la página del grupo de almacenamiento (seleccione **ILM** > **agrupaciones de almacenamiento**), revise los mensajes de error en la columna último error y consulte las siguientes directrices para la solución de problemas.

Compruebe si se ha resuelto un error

Después de resolver cualquier problema subyacente, puede determinar si se ha resuelto el error. En la página agrupación de almacenamiento en la nube, seleccione el botón de opción para el extremo 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 aparecerá en la columna último error en unos 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 extremo de servicio utilizado para el grupo de almacenamiento en la nube no utiliza el protocolo HTTP para un contenedor o bloque 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 bloque.
- 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 a este punto por ILM, datos que estaban en el bloque antes de configurar el Cloud Storage Pool o datos que algún otro origen colocó en el bloque después de crear el Cloud Storage Pool.

Intente uno o más de estos pasos para corregir el problema:

- Siga las instrucciones para devolver objetos a StorageGRID en «"ciclo de vida de un objeto de agrupación 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 se configuró un proxy de almacenamiento no transparente entre los nodos de almacenamiento y el extremo externo de S3 utilizado para el pool de almacenamiento en el cloud. Este error ocurre si el servidor proxy externo no puede acceder al extremo 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 red del servidor proxy de almacenamiento.

Información relacionada

Ciclo de vida de un objeto de Cloud Storage Pool

Configure los perfiles de código de borrado

Cree un perfil de código de borrado

Para crear un perfil de código de borrado, debe asociar un pool de almacenamiento que contiene nodos de almacenamiento con un esquema de código de borrado. Esta asociación determina el número de fragmentos de datos y de paridad creados y el lugar en el que el sistema distribuye estos fragmentos.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha creado un grupo de almacenamiento que incluye exactamente un sitio o un grupo de almacenamiento que incluye tres o más sitios. No hay esquemas de codificación de borrado disponibles para un pool de almacenamiento que únicamente tenga dos ubicaciones.

Acerca de esta tarea

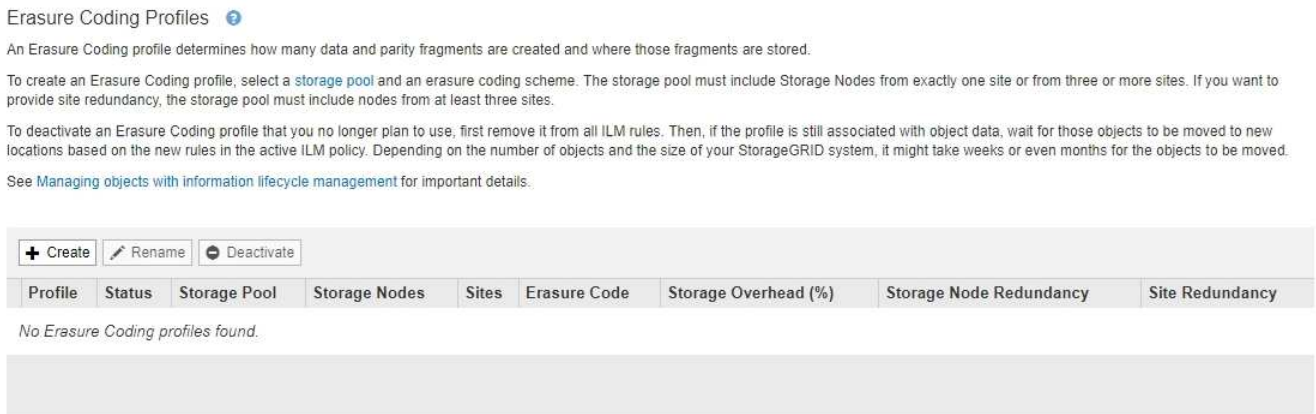
Los pools de almacenamiento utilizados en los perfiles de código de borrado deben incluir exactamente un sitio o tres o más. Si desea proporcionar redundancia del sitio, el pool de almacenamiento debe tener al menos tres sitios.

> Debe seleccionar un pool de almacenamiento que contenga nodos de almacenamiento. No se pueden usar nodos de archivado para los datos codificados mediante borrado.

Pasos

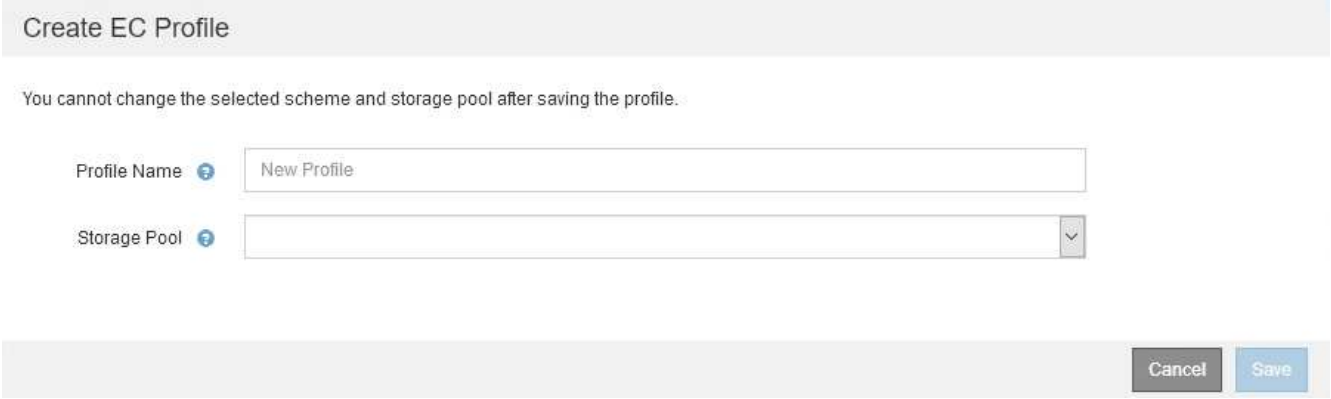
1. Seleccione **ILM** > **codificación de borrado**.

   Aparece la página Perfiles de código de borrado.



2. Seleccione **Crear**.

   Aparece el cuadro de diálogo Crear perfil de EC.



3. Introduzca un nombre único para el perfil de código de borrado.

   Los nombres de perfiles 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.

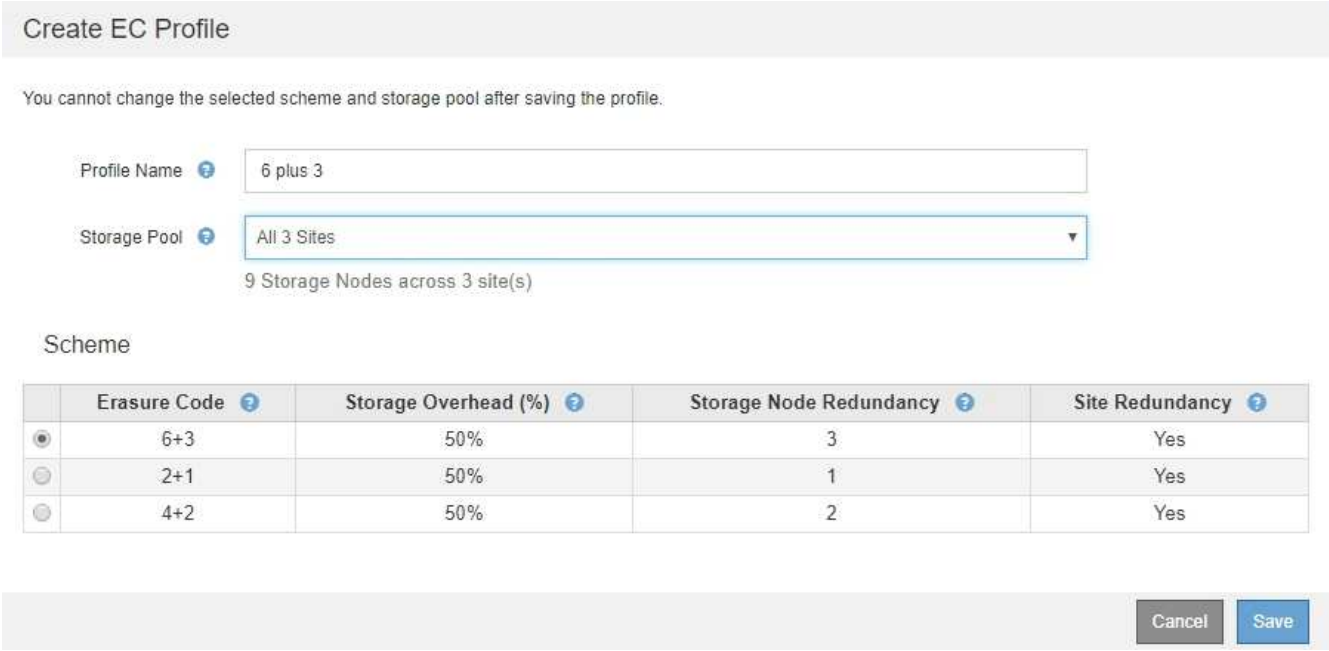
   > El nombre del perfil de código de borrado se anexa al nombre del pool de almacenamiento en la instrucción de ubicación de una regla de ILM.

4. Seleccione el pool de almacenamiento que ha creado para este perfil de código de borrado.

   > Si el grid incluye actualmente un solo sitio, no podrá utilizar el pool de almacenamiento predeterminado, todos los nodos de almacenamiento o cualquier pool de almacenamiento que incluya el sitio predeterminado, todos los sitios. Este comportamiento impide que el perfil de código de borrado no sea válido si se agrega un segundo sitio.

   > Si un pool de almacenamiento incluye exactamente dos sitios, no podrá utilizar ese pool de almacenamiento para codificar el borrado. No hay esquemas de codificación de borrado disponibles para un pool de almacenamiento que tenga dos ubicaciones.

   Cuando se selecciona un pool de almacenamiento, se muestra la lista de esquemas de codificación de borrado disponibles, según la cantidad de nodos de almacenamiento y sitios del pool.



La siguiente información se incluye para cada esquema de codificación de borrado disponible:

- **Código de borrado**: El nombre del esquema de código de borrado en el formato siguiente: Fragmentos de datos + fragmentos de paridad.
- **Gastos generales de almacenamiento (%)**: El almacenamiento adicional necesario para fragmentos de paridad en relación con el tamaño de los datos del objeto. Sobrecarga del almacenamiento = número total de fragmentos de paridad / número total de fragmentos de datos.
- **Redundancia del nodo de almacenamiento**: El número de nodos de almacenamiento que se pueden perder manteniendo la capacidad de recuperar datos del objeto.
- **Redundancia del sitio**: Si el código de borrado seleccionado permite recuperar los datos del objeto si se pierde un sitio.

  Para admitir la redundancia de sitios, el pool de almacenamiento seleccionado debe incluir varios sitios, cada uno con nodos de almacenamiento suficientes para permitir la pérdida de cualquier sitio. Por ejemplo, para admitir la redundancia del sitio con un esquema de codificación de borrado 6+3, el pool de almacenamiento seleccionado debe incluir al menos tres sitios con al menos tres nodos de almacenamiento en cada sitio.

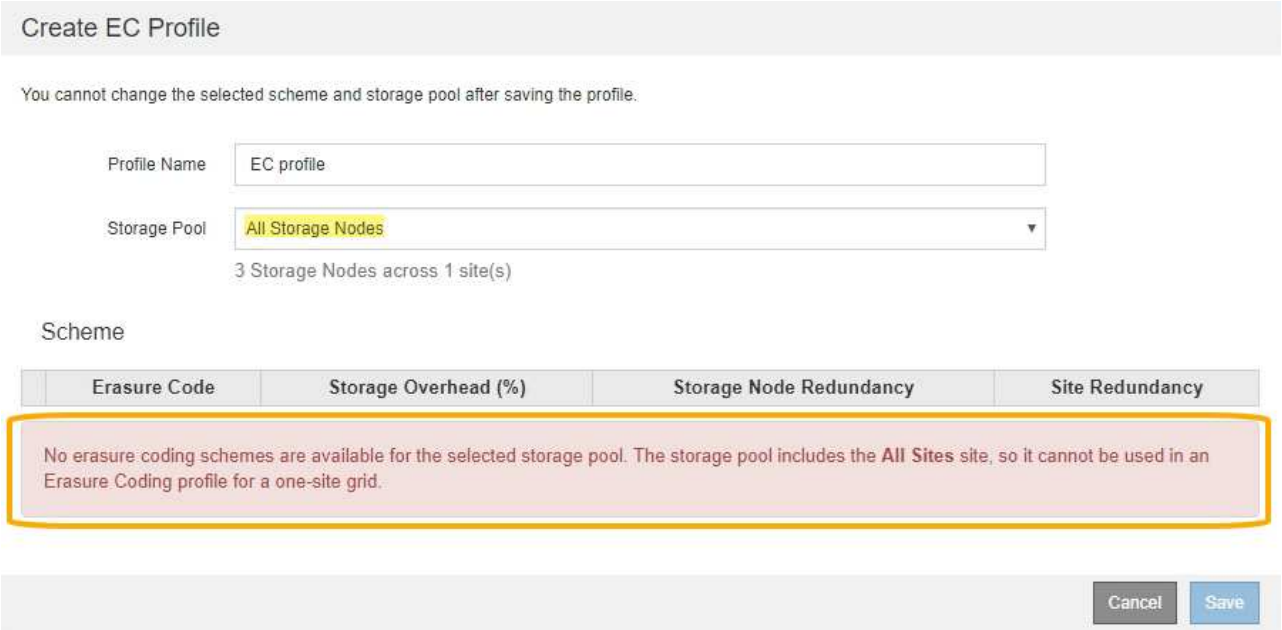
  Los mensajes se muestran en estos casos:

- El pool de almacenamiento seleccionado no proporciona redundancia de sitio. Se espera el siguiente mensaje cuando el grupo de almacenamiento seleccionado incluye sólo un sitio. Puede utilizar este perfil de código de borrado en reglas de ILM para protegerse contra fallos de nodos.

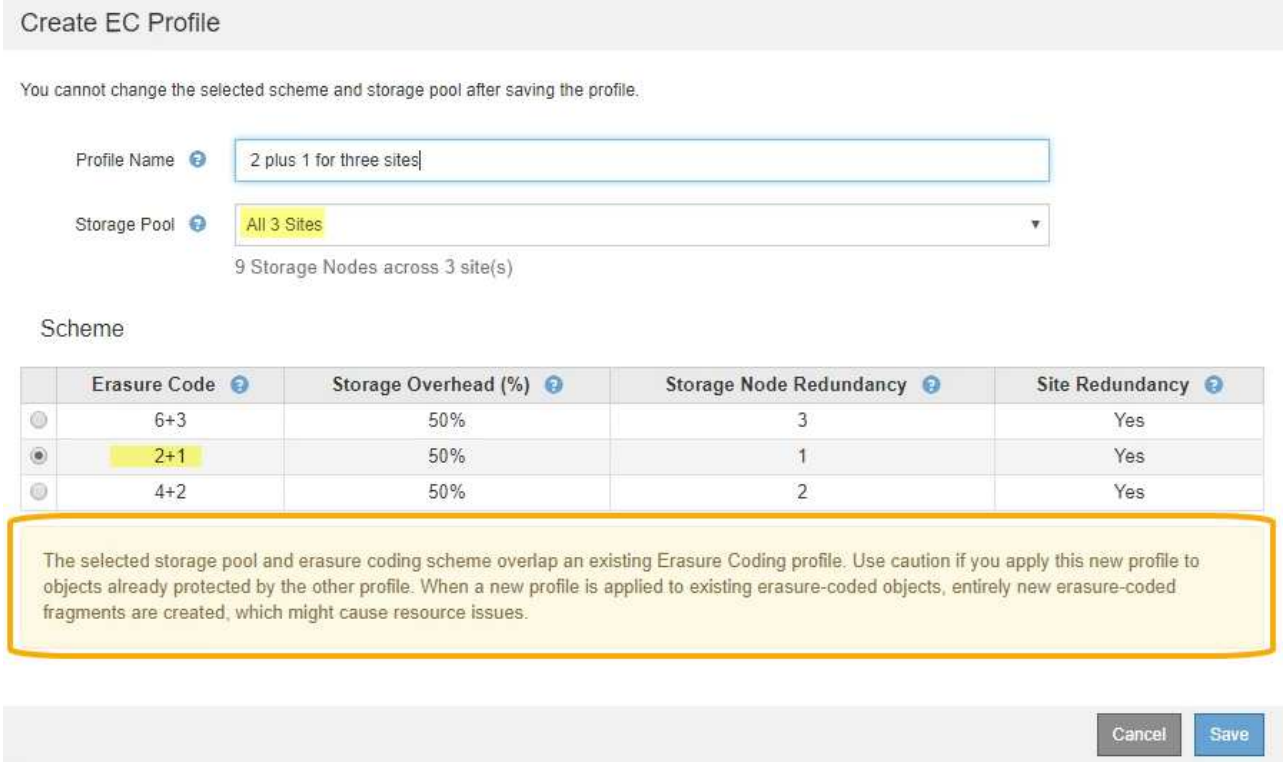
- El pool de almacenamiento seleccionado no cumple con los requisitos de ningún esquema de

codificación de borrado. Por ejemplo, se espera el siguiente mensaje cuando el grupo de almacenamiento seleccionado incluye exactamente dos sitios. Si desea utilizar la codificación de borrado para proteger los datos de los objetos, debe seleccionar un pool de almacenamiento con exactamente un sitio o un pool de almacenamiento con tres o más ubicaciones.

- El grid incluye un solo sitio y seleccionó el pool de almacenamiento predeterminado, todos los nodos de almacenamiento o cualquier pool de almacenamiento que incluya el sitio predeterminado, todos los sitios.



- El esquema de codificación de borrado y el pool de almacenamiento seleccionados se superponen con otro perfil de código de borrado.



En este ejemplo, aparece un mensaje de advertencia porque otro perfil de código de borrado está utilizando el esquema 2+1 y el grupo de almacenamiento del otro perfil también utiliza uno de los sitios del grupo de almacenamiento todos los 3 sitios.

Aunque no se le impide crear este nuevo perfil, debe tener mucho cuidado al empezar a utilizarlo en la política de ILM. Si este nuevo perfil se aplica a los objetos existentes con código de borrado ya protegidos por otro perfil, StorageGRID creará un conjunto de fragmentos de objeto completamente nuevo. No reutilizará los fragmentos 2+1 existentes. Los problemas de los recursos se pueden producir al migrar de un perfil de codificación de borrado a otro, aunque los esquemas de codificación de borrado sean los mismos.

5. Si se muestra más de un esquema de codificación de borrado, seleccione el que desee utilizar.

   Al decidir qué esquema de codificación de borrado utilizar, debe equilibrar la tolerancia a fallos (lograda mediante más segmentos de paridad) con los requisitos del tráfico de red en las reparaciones (más fragmentos equivale a más tráfico de red). Por ejemplo, al decidir entre un esquema 4+2 y un esquema 6+3, seleccione el esquema 6+3 si se requiere paridad adicional y tolerancia a fallos. Seleccione el esquema 4+2 si los recursos de red están limitados para reducir el uso de la red durante las reparaciones de nodo.

6. Seleccione **Guardar**.

Cambie el nombre de un perfil de código de borrado

Es posible que desee cambiar el nombre de un perfil de código de borrado para que sea más obvio lo que hace el perfil.

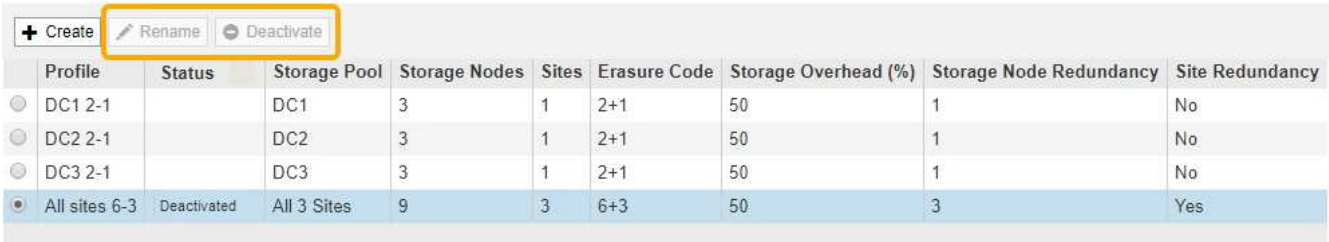
Lo que necesitará

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

Pasos

1. Seleccione **ILM** > **codificación de borrado**.

   Aparece la página Perfiles de código de borrado. Los botones **Renombrar** y **Desactivar** están desactivados.



Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
DC1 2-1		DC1	3	1	2+1	50	1	No
DC2 2-1		DC2	3	1	2+1	50	1	No
DC3 2-1		DC3	3	1	2+1	50	1	No
All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

2. Seleccione el perfil al que desea cambiar el nombre.

   Los botones **Renombrar** y **Desactivar** se activan.

3. Seleccione **Cambiar nombre**.

   Aparece el cuadro de diálogo Cambiar nombre de perfil EC.

4. Introduzca un nombre único para el perfil de código de borrado.

   El nombre del perfil de código de borrado se anexa al nombre del pool de almacenamiento en la instrucción de ubicación de una regla de ILM.

   Los nombres de perfiles 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

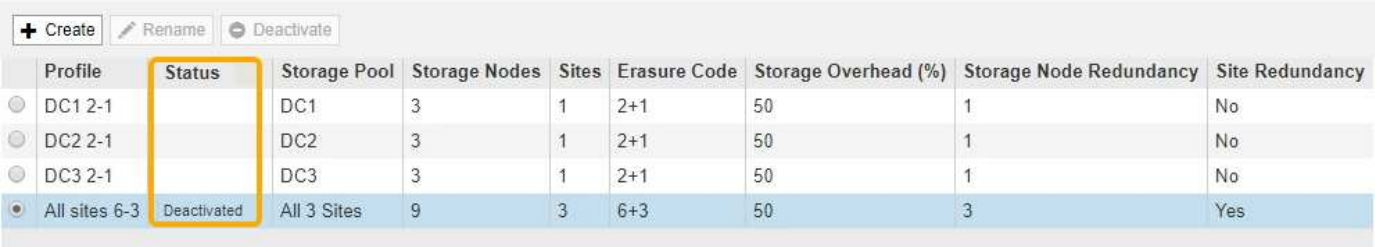
Puede desactivar un perfil de código de borrado si ya no tiene pensado utilizarlo y si el perfil no se utiliza actualmente en ninguna regla de ILM.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha confirmado que no hay operaciones de reparación de datos codificados para borrado ni procedimientos de retirada en curso. Se devuelve un mensaje de error si intenta desactivar un perfil de código de borrado mientras alguna de estas operaciones está en curso.

Acerca de esta tarea

Cuando desactiva un perfil de código de borrado, el perfil sigue apareciendo en la página Perfiles de código de borrado, pero su estado es **desactivado**.



+ Create | Rename | Deactivate

	Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
○	DC1 2-1		DC1	3	1	2+1	50	1	No
○	DC2 2-1		DC2	3	1	2+1	50	1	No
○	DC3 2-1		DC3	3	1	2+1	50	1	No
◉	All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

Ya no puede utilizar un perfil de código de borrado que se haya desactivado. No se muestra un perfil desactivado al crear las instrucciones de colocación para una regla de ILM. No puede reactivar un perfil desactivado.

StorageGRID evita la desactivación de 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 utiliza en ninguna regla de ILM, pero los datos de los objetos y los fragmentos de paridad para el perfil siguen existiendo.

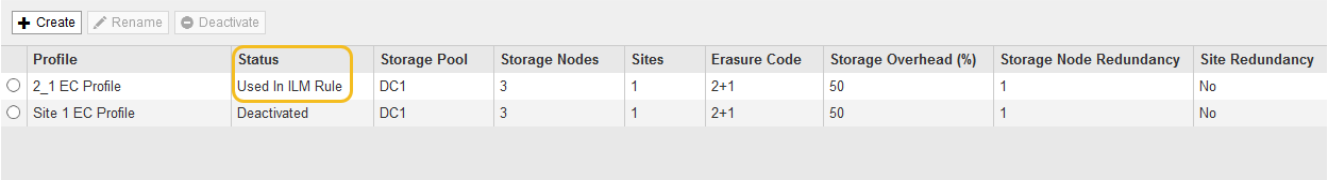
Pasos

1. Seleccione **ILM** > **código de borrado**.

   Aparece la página Perfiles de código de borrado. Los botones **Renombrar** y **Desactivar** están desactivados.

2. Revise la columna **Estado** para confirmar que el perfil de código de borrado que desea desactivar no se utiliza en ninguna regla de ILM.

   No puede desactivar un perfil de codificación de borrado si se utiliza en cualquier regla de ILM. En el ejemplo, el **2_1 EC Profile** se utiliza en al menos una regla ILM.



+ Create | Rename | Deactivate

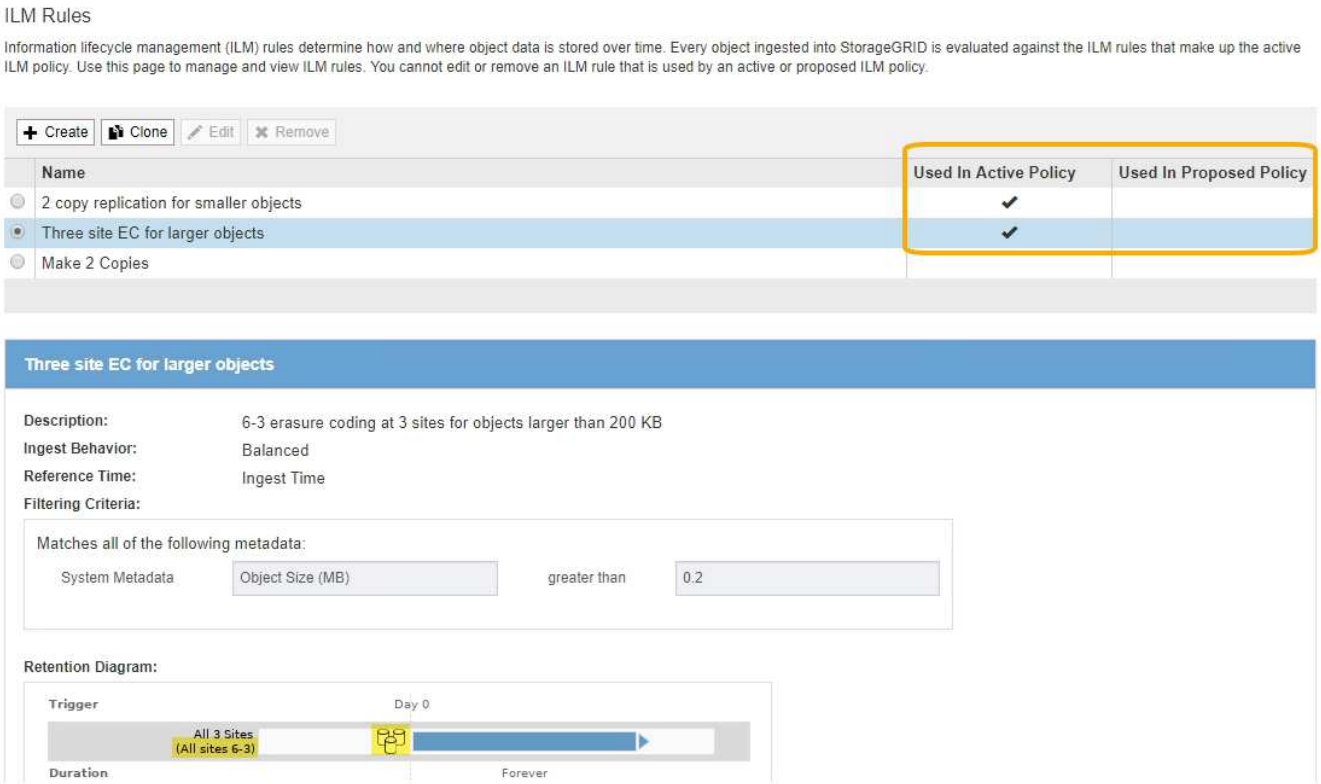
	Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
○	2_1 EC Profile	Used In ILM Rule	DC1	3	1	2+1	50	1	No
○	Site 1 EC Profile	Deactivated	DC1	3	1	2+1	50	1	No

3. Si el perfil se utiliza en una regla de ILM, siga estos pasos:

   a. Seleccione **ILM** > **Reglas**.

b. Para cada regla de la lista, seleccione el botón de opción y revise el diagrama de retención para determinar si la regla utiliza el perfil de código de borrado que desea desactivar.

   En el ejemplo, la regla **tres sitio EC para objetos más grandes** utiliza un grupo de almacenamiento denominado **todos los 3 sitios** y el perfil de código de borrado **todos los sitios 6-3**. Los perfiles de código de borrado se representan con este icono:



a. Si la regla de ILM utiliza el perfil de código de borrado que desea desactivar, determine si la regla se utiliza en la política de ILM activa o en una política propuesta.

   En el ejemplo, la regla **tres sitios EC para objetos más grandes** se utiliza en la política activa de ILM.

b. Complete los pasos adicionales de la tabla, según el lugar donde se utilice el perfil de código de borrado.

¿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

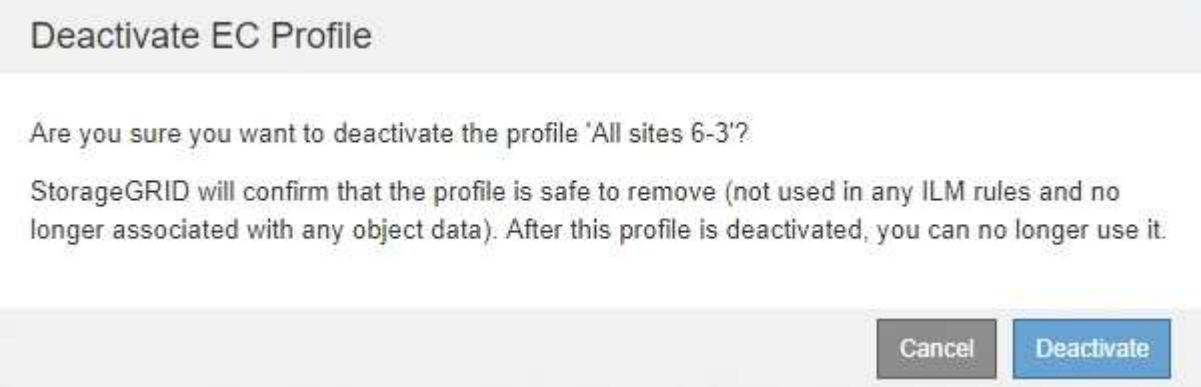
¿Dónde se ha utilizado el perfil?	Pasos adicionales que se deben realizar antes de desactivar el perfil	Consulte estas instrucciones adicionales
En una regla de ILM que esté actualmente en la política activa de ILM	i. Clonar la política activa. ii. Quite la regla de ILM que utiliza el perfil de código 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 código de borrado mientras sigue asociado con 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 se encuentra actualmente en una política de ILM propuesta	i. Edite la directiva propuesta. ii. Quite la regla de ILM que utiliza 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 directiva propuesta. 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

¿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 en una política histórica de ILM	i. Edite o elimine la regla. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de código de borrado. (La regla aparecerá ahora como una regla histórica en la política histórica.) ii. Continúe con este procedimiento.	Trabaje con las reglas de ILM y las políticas de ILM

c. Actualice la página Perfiles de código de borrado para asegurarse de que el perfil no se utilice 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 EC.



5. Si está seguro de que desea desactivar el perfil, seleccione **Desactivar**.
   - Si StorageGRID puede desactivar el perfil de código de borrado, su estado será **desactivado**. Ya no puede seleccionar este perfil para ninguna regla de ILM.
   - 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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 solo se aplique a los objetos en cubos S3 creados en la región US-West-2. 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 cucharones pertenecen a la región US-East-1.
- 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 mayúsculas de minúsculas y deben contener al menos 2 caracteres y no más de 32. Los caracteres válidos son números, letras y guiones.

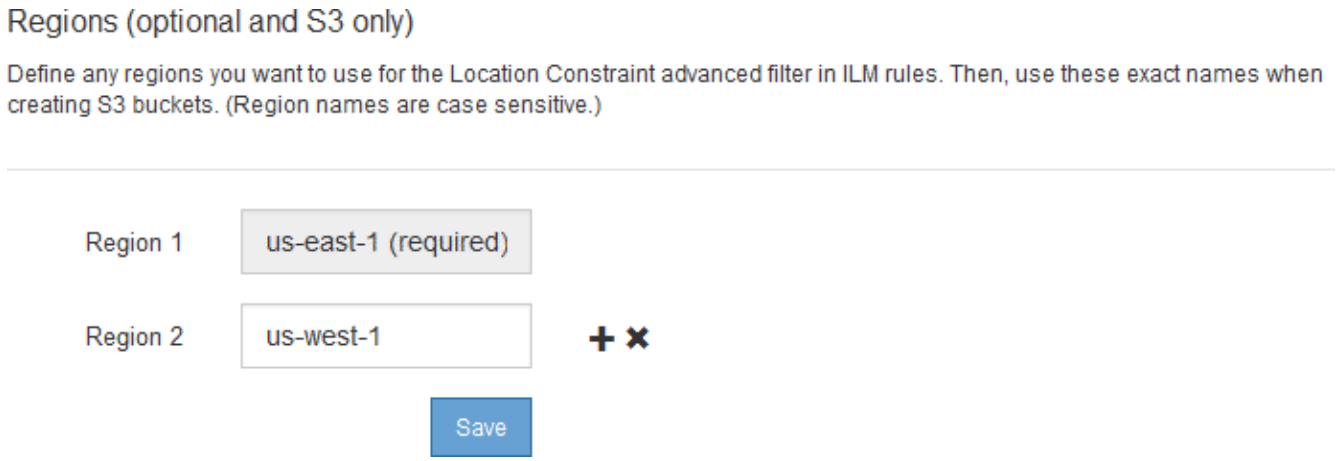
> No se considera que la UE sea un alias para la ue-oeste-1. Si desea utilizar la región UE o eu-West-1, debe usar el nombre exacto.

- No se puede eliminar ni modificar una región si actualmente se utiliza dentro de la política de ILM activa o la política de ILM propuesta.
- Si la región utilizada como filtro avanzado en una regla de ILM no es válida, todavía es posible agregar esa regla a la directiva propuesta. Sin embargo, se produce un error si intenta guardar o activar la directiva propuesta. (Una región no válida puede resultar si utiliza una región como filtro avanzado en una regla de ILM, pero después 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 ni eliminar.

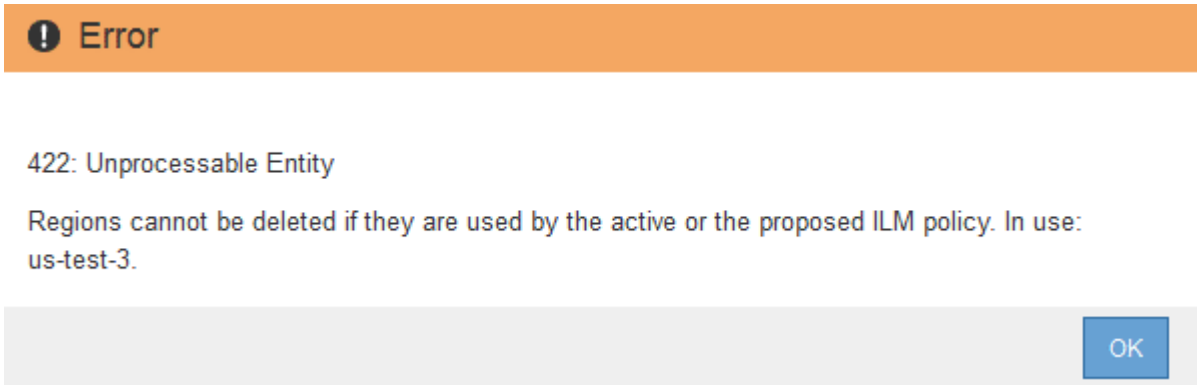
   

2. Para agregar una región:
   a. Seleccione el icono de inserción ➕ a la derecha de la última entrada.
   b. Introduzca el nombre de una región que desea utilizar al crear bloques de S3.

      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 la directiva activa o la directiva propuesta.



4. Cuando haya terminado de realizar los cambios, seleccione **Guardar**.

   Ahora puede seleccionar estas regiones en la lista **restricción de ubicaciones** de la página filtro avanzado del asistente Crear regla ILM. ConsulteUsar filtros avanzados en las reglas de ILM.

Cree la regla de ILM

Acceda al asistente Create 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 ILM Rule.

> ⓘ Si crea la regla de ILM predeterminada para una política, utilice este procedimiento en su lugar: Cree una regla de ILM predeterminada.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Si desea especificar a qué cuentas de arrendatario se aplica esta regla, tiene el permiso Cuentas de arrendatario o conoce el ID de cuenta de cada cuenta.
- Si desea que la regla filtre objetos en los metadatos del último acceso, las actualizaciones de la hora del último acceso deben habilitarse en bloque para S3 o mediante contenedor para Swift.
- Si crea copias replicadas, debe configurar todos los pools de almacenamiento o los pools de almacenamiento en el cloud que planea utilizar. Consulte Cree el pool de almacenamiento y.. Cree el pool de almacenamiento en el cloud.

- Si crea copias con código de borrado, configuró un perfil de código de borrado. Consulte Cree un perfil de código de borrado.
- Usted está familiarizado con el opciones de protección de datos para consumo.
- 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 ILM para StorageGRID: Introducción".

Acerca de esta tarea

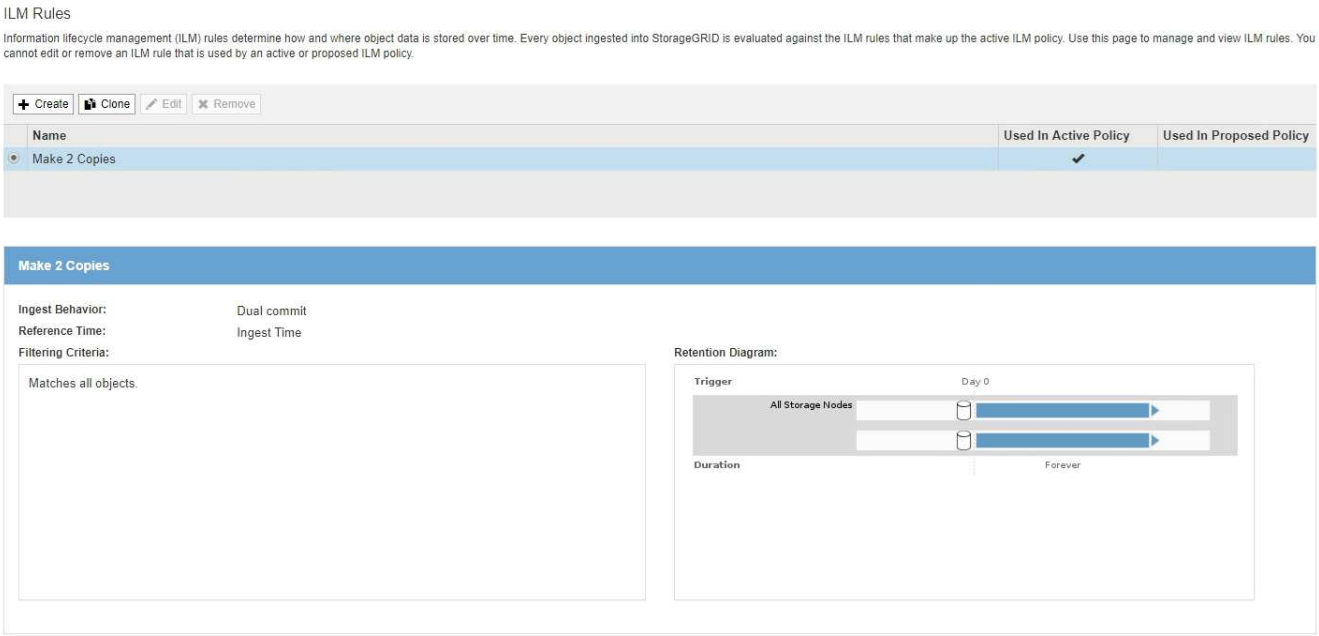
Al crear reglas de ILM:

- Considere la topología y las configuraciones de almacenamiento del sistema StorageGRID.
- Considere qué tipos de copias de objetos desea hacer (replicadas o codificadas por 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 se debe usar para la opción de protección de datos durante el procesamiento (equilibrado, estricto o Dual Commit).

Pasos

1. Seleccione **ILM** > **Reglas**.

   Aparece la página ILM Rules, con la regla general, haga 2 copias, seleccionada.



> La página ILM Rules tiene un aspecto ligeramente diferente si se habilitó la configuración global de bloqueo de objetos S3 para el sistema StorageGRID. La tabla de resumen incluye una columna **compatible** y los detalles de la regla seleccionada incluyen un campo **compatible**.

2. Seleccione **Crear**.

   Aparece el paso 1 (definir datos básicos) del asistente Crear regla de ILM. Utilice la página definir conceptos básicos para definir a qué objetos se aplica la regla.

Paso 1 de 3: Definir lo básico

El paso 1 (definir datos básicos) del asistente Crear regla de ILM permite definir los filtros básicos y avanzados de la regla.

Acerca de esta tarea

Al evaluar un objeto con una 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**.

   Debe introducir entre 1 y 64 caracteres.

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.

Name	Make 3 Copies
Description	Save 1 copy at 3 sites for 1 year. Then, save EC copy forever

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 dispone del permiso acceso raíz o de las cuentas de arrendatario, no podrá seleccionar arrendatarios en 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 **coincide con All** (valor predeterminado), la regla se aplica a todos los bloques S3 o contenedores Swift.

5. Opcionalmente, seleccione **filtrado 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.

   Si esta regla crea copias con código de borrado, agregue el filtro avanzado **Tamaño de objeto (MB)** y configúrelo en **mayor que 1**. El filtro de tamaño garantiza que los objetos de 1 MB o menos no se recodifiquen.

   > El código de borrado se adapta mejor a los objetos de más de 1 MB. No utilice la codificación de borrado para objetos de menos de 200 KB con el fin de evitar la sobrecarga de gestión de fragmentos codificados con borrado de muy pequeño tamaño.

6. Seleccione **Siguiente**.

   Aparece el paso 2 (definir ubicaciones).

Información relacionada

- Qué es una regla de ILM
- Usar filtros avanzados en las reglas de ILM
- Paso 2 de 3: Definir colocaciones

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.

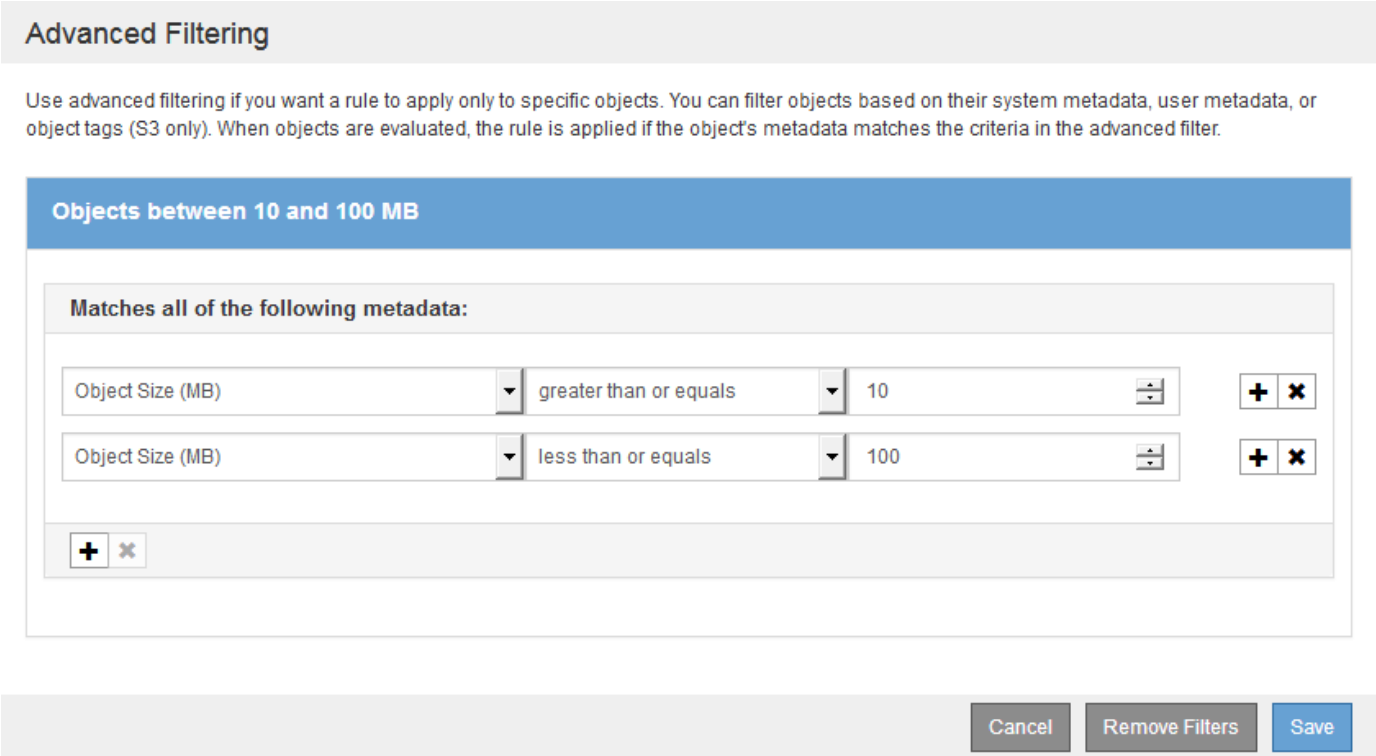
Tipo de metadatos	Operadores compatibles	Valor de los metadatos
Tiempo de consumo (microsegundos)	• es igual a • no es igual • menor que • menor que o igual • mayor que • mayor o igual que	Hora y fecha en la que se ingirió el objeto. **Nota:** para evitar problemas de recursos al activar una nueva política de ILM, puede utilizar 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 ingesta como 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.
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 (microsegundos)	• es igual a • no es igual • menor que • menor que o igual • mayor que • mayor o igual que • existe • no existe	Hora y fecha en la que se recuperó por última vez el objeto (leído o visualizado). **Nota:** Si planea utilizar la última hora de acceso como filtro avanzado, las actualizaciones de la última hora de acceso deben estar habilitadas para el contenedor S3 bucket o Swift. Utilice la hora del último acceso en las reglas de ILM
Limitación de ubicaciones (solo 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. Configurar regiones (opcional solo S3)

Tipo de metadatos	Operadores compatibles	Valor de los metadatos
Tamaño del objeto (MB)	• es igual a • no es igual • menor que • menor que o igual • mayor que • mayor o igual que	Tamaño del objeto en MB. El código de borrado se adapta mejor a los objetos de más de 1 MB. No utilice la codificación de borrado para objetos de menos de 200 KB con el fin de evitar la sobrecarga de gestión de fragmentos codificados con borrado de muy pequeño tamaño. **Nota:** para filtrar en tamaños de objeto menores de 1 MB, escriba un valor decimal. El tipo de navegador y la configuración regional controlan si necesita utilizar un punto o una coma como separador decimal.
Metadatos del usuario	• contiene • termina con • es igual a • existe • no contiene • no termina con • no es igual • no existe • no empieza por • comienza con	Par clave-valor, donde **Nombre de metadatos de usuario** es la clave y **valor de metadatos de usuario** 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 de usuario**. **Nota:** los nombres de metadatos del usuario no distinguen entre mayúsculas y minúsculas; los valores de metadatos del usuario distinguen entre mayúsculas y minúsculas.
Etiqueta de objeto (solo S3)	• contiene • termina con • es igual a • existe • no contiene • no termina con • no es igual • no existe • no empieza por • comienza con	Par clave-valor, donde **Nombre de etiqueta de objeto** es la clave y **valor de etiqueta de objeto** 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 **valor de etiqueta de objeto**. **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.

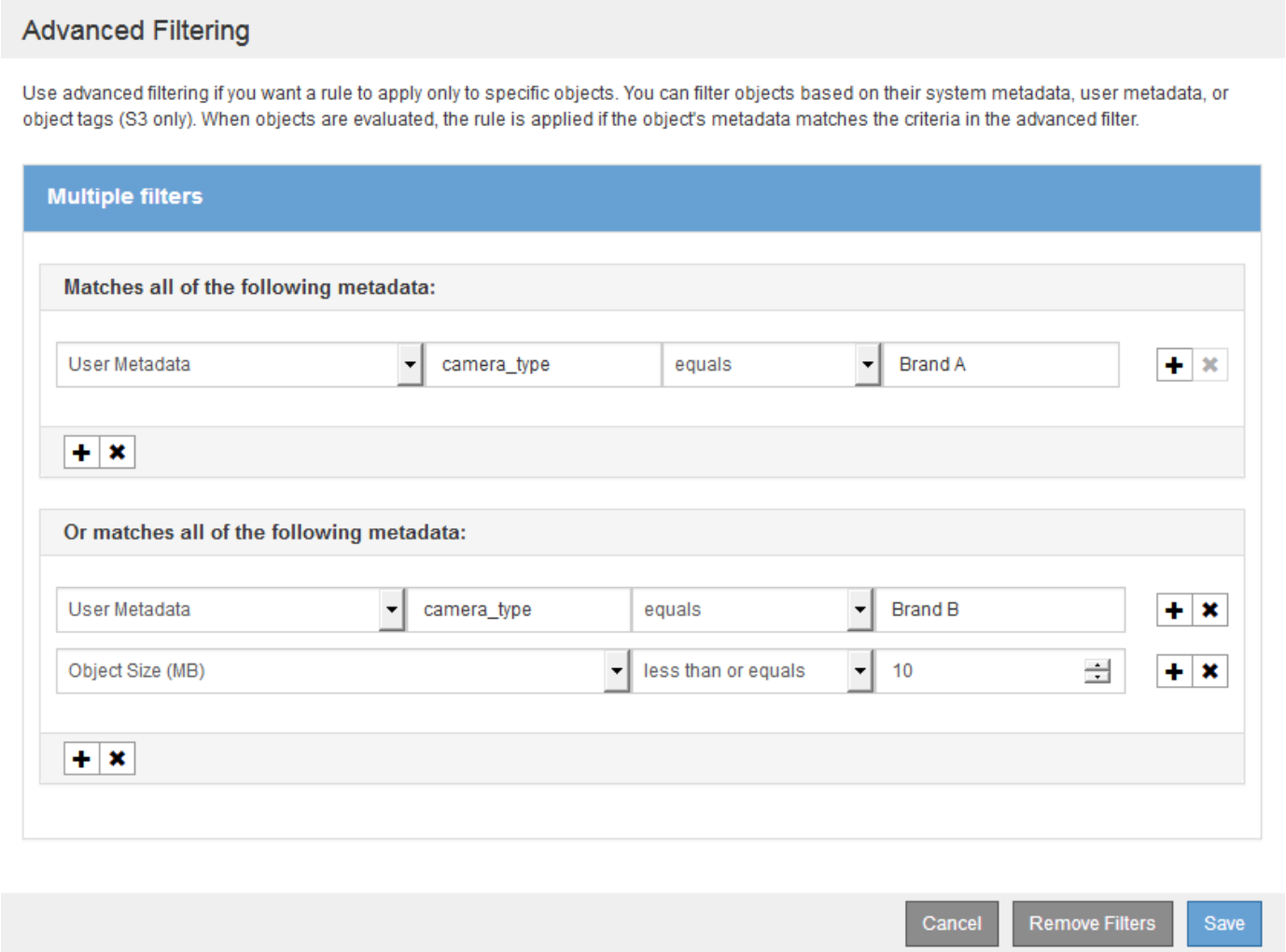
Especifique varios tipos de metadatos y valores

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 ejemplo siguiente, la regla se aplica a los objetos que tienen una Marca A o una 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

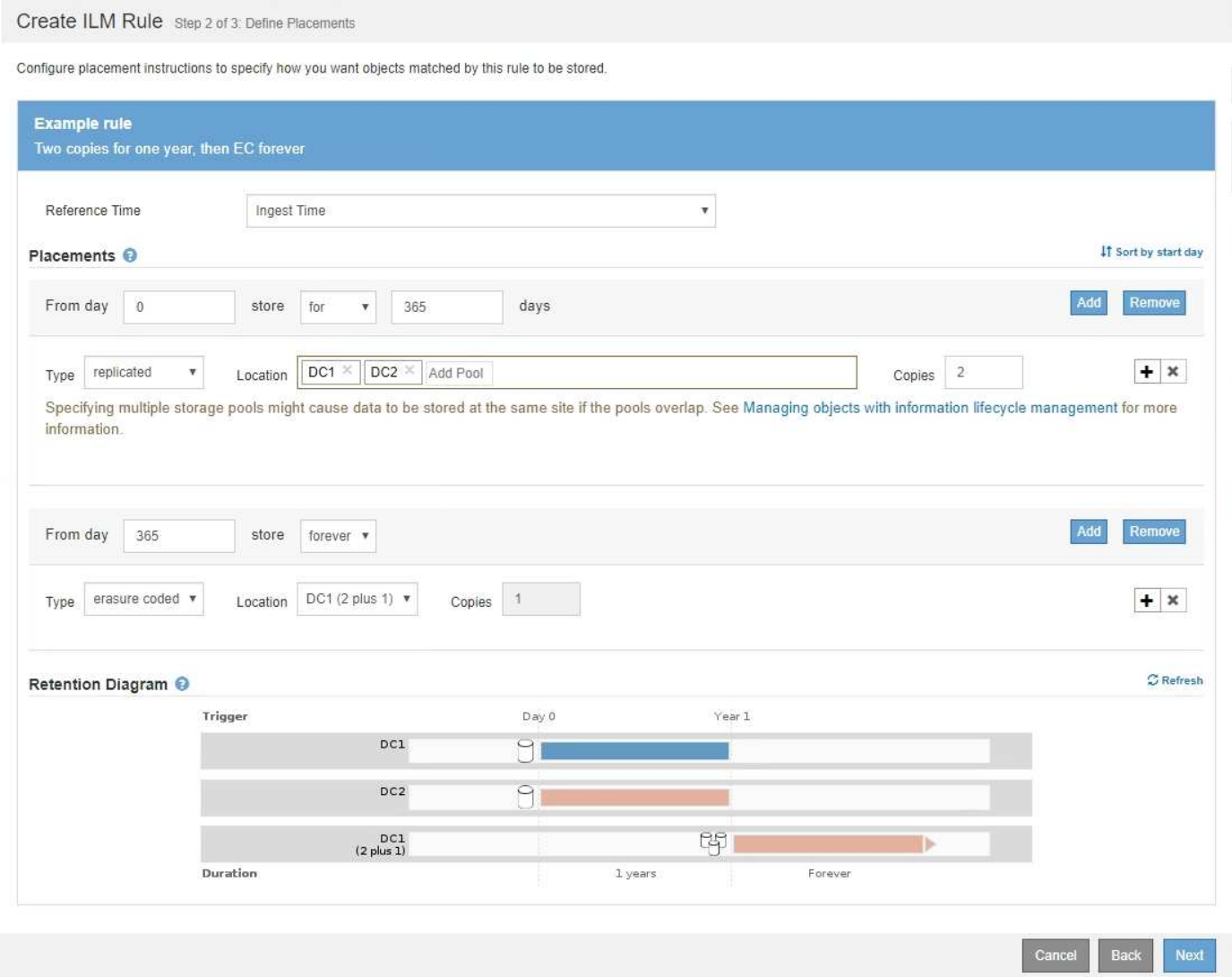
El paso 2 (definir ubicaciones) del asistente para crear regla de ILM permite definir las instrucciones de ubicación que determinan la cantidad de objetos que se almacenan, el tipo de copias (replicadas o codificadas para borrado), la ubicación del almacenamiento y el número de copias.

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.

Esta regla de ILM de ejemplo crea dos copias replicadas para el primer año. Cada copia se guarda en una agrupación de almacenamiento de un sitio diferente. Después de un año, se realiza y se guarda una copia con código de borrado al 2+1 en una sola instalación.



Pasos

1. En **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 utilizar esta opción, las actualizaciones de la hora de último acceso deben estar habilitadas para el contenedor S3 bucket o Swift. Consulte Utilice la hora del último acceso en las reglas de ILM.

Opción	Descripción
Hora no actual	El tiempo que una versión de objeto se volvió no actual porque se ingirió una nueva versión y la reemplazó como la versión actual. **Nota:** el tiempo no corriente se aplica sólo a los objetos S3 en bloques habilitados para versionado. 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.
Hora de creación definida por el usuario	Hora especificada en los metadatos definidos por el usuario.

> Si desea crear una regla compatible, debe seleccionar **tiempo de procesamiento**.

2. En la sección **colocaciones**, seleccione un tiempo de inicio y una duración para el primer período de tiempo.

   Por ejemplo, es posible que desee especificar dónde almacenar los objetos durante el primer año ("días 0 durante 365 días"). Al menos una instrucción debe comenzar en el día 0.

3. Si desea crear copias replicadas:
   a. En la lista desplegable **Tipo**, seleccione **replicado**.
   b. En el campo **ubicación**, seleccione **Agregar pool** para cada pool de almacenamiento que desee 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 su grid incluye tres nodos de almacenamiento y selecciona 4 como el número de copias, solo se realizarán tres copias: Una copia para cada nodo de almacenamiento.

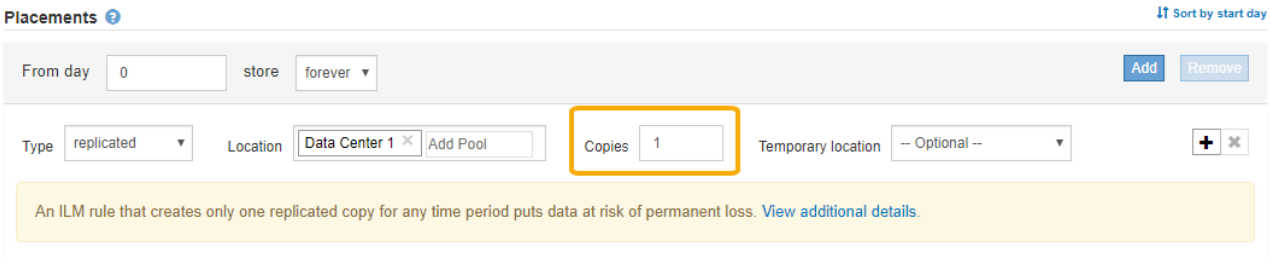
      > Se activa la alerta **colocación de ILM inalcanzable** para indicar que la regla ILM no se pudo aplicar completamente.

      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 especifique el pool de almacenamiento predeterminado todos los nodos de almacenamiento y otro pool de almacenamiento.

c. 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 estos riesgos, siga uno o varios de estos procedimientos:

   - Aumentar el número de copias durante el período de tiempo.
   - Seleccione el icono de signo más ➕ para crear copias adicionales durante el período de tiempo. A continuación, seleccione un pool de almacenamiento diferente o un pool de almacenamiento cloud.
   - Seleccione **Código de borrado** para Tipo, en lugar de **replicado**. Puede ignorar con toda tranquilidad esta advertencia si esta regla ya crea varias copias para todos los períodos de tiempo.

d. Si ha especificado sólo una agrupación de almacenamiento, ignore el campo **ubicación temporal**.

   > ⓘ Las ubicaciones temporales están obsoletas y se eliminarán en un lanzamiento futuro. Consulte Usar un pool de almacenamiento como ubicación temporal (obsoleto).

4. Si desea crear una copia con código de borrado:

   a. En la lista desplegable **Tipo**, seleccione **Código de borrado**.

      El número de copias cambia a 1. Aparece una advertencia si la regla no tiene un filtro avanzado para ignorar objetos de 200 KB o menos.

      > Erasure coding is best suited for objects greater than 1 MB. Do not use erasure coding for objects that are 200 KB or smaller. Select **Back** to return to Step 1. Then, use **Advanced filtering** to set the Object Size (MB) filter to any value greater than 0.2.

      > ⓘ El código de borrado se adapta mejor a los objetos de más de 1 MB. No utilice la codificación de borrado para objetos de menos de 200 KB con el fin de evitar la sobrecarga de gestión de fragmentos codificados con borrado de muy pequeño tamaño.

   b. Si aparece la advertencia de tamaño de objeto, seleccione **Atrás** para volver al paso 1. A continuación, seleccione **filtrado avanzado** y establezca el filtro Tamaño del objeto (MB) en cualquier valor superior a 0.2.

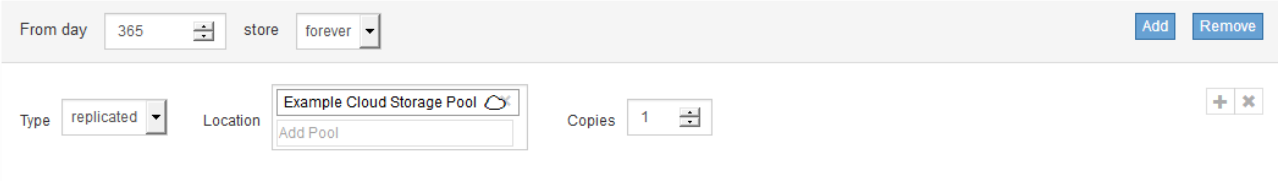
c. Seleccione la ubicación de almacenamiento.

La ubicación de almacenamiento de una copia codificada con borrado incluye el nombre del pool de almacenamiento seguido del nombre del perfil de la codificación de borrado.

5. Si lo desea, puede agregar periodos de tiempo diferentes o crear copias adicionales en diferentes ubicaciones:
   - Seleccione el icono más para crear copias adicionales en una ubicación diferente durante el mismo período de tiempo.
   - Seleccione **Agregar** para agregar un período de tiempo diferente a las instrucciones de colocación.

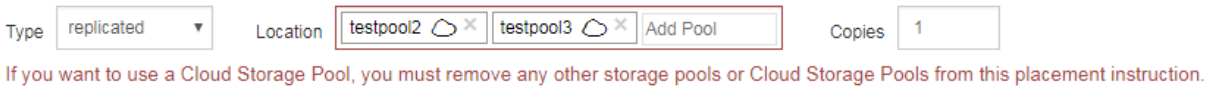
> Los objetos se eliminan automáticamente al final del período de tiempo final, a menos que el período de tiempo final finalice con **para siempre**.

6. Si desea almacenar objetos en un pool de almacenamiento en cloud:
   a. En la lista desplegable **Tipo**, seleccione **replicado**.
   b. En el campo **ubicación**, seleccione **Agregar grupo**. A continuación, seleccione un pool de almacenamiento en el cloud.

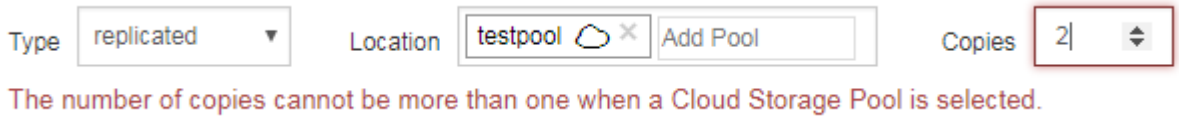


Cuando utilice Cloud Storage Pools, tenga en cuenta estas reglas:

- No puede seleccionar más de un pool de almacenamiento en cloud mediante una única instrucción de colocación. De forma similar, no puede seleccionar un pool de almacenamiento en cloud ni un pool de almacenamiento en la misma instrucción de ubicación.

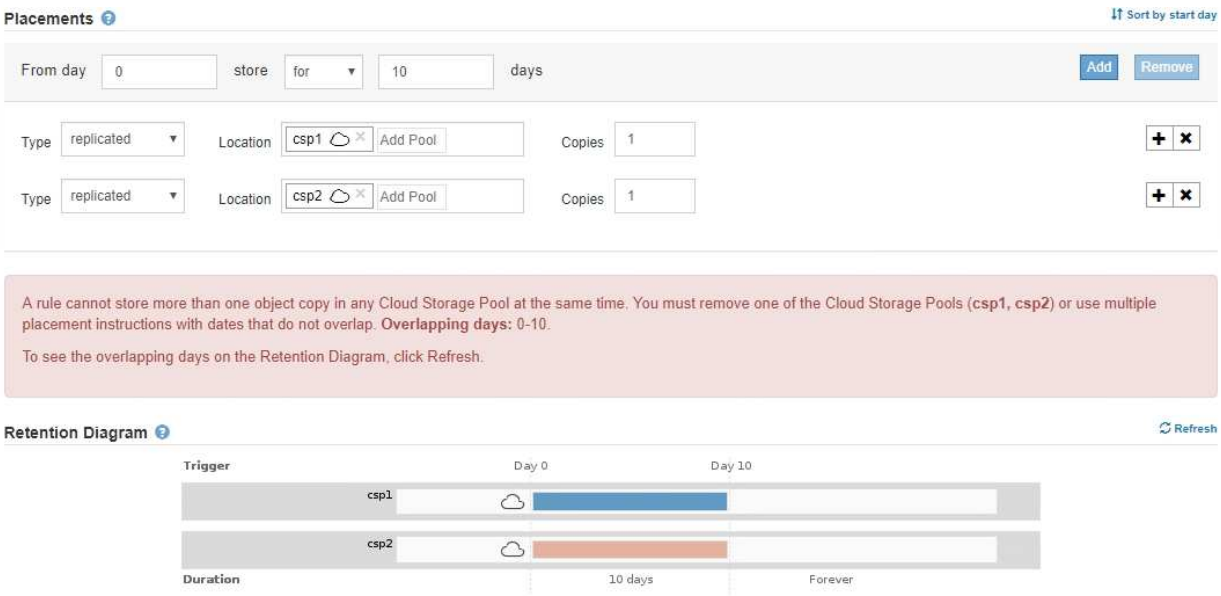


- Solo puede almacenar una copia de un objeto en cualquier Cloud Storage Pool en concreto. Aparece un mensaje de error si configura **copias** en 2 o más.

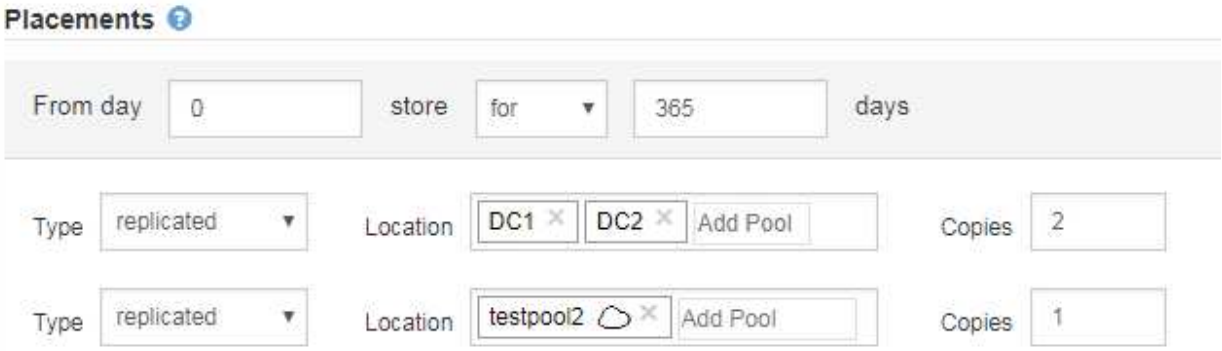


- No puede almacenar más de una copia de objetos en ningún pool de almacenamiento en cloud al mismo tiempo. Aparecerá un mensaje de error si varias ubicaciones que utilizan un Cloud Storage

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 al mismo tiempo que el objeto se almacena como copias replicadas o codificadas de borrado en StorageGRID. Sin embargo, como se muestra en este ejemplo, 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.



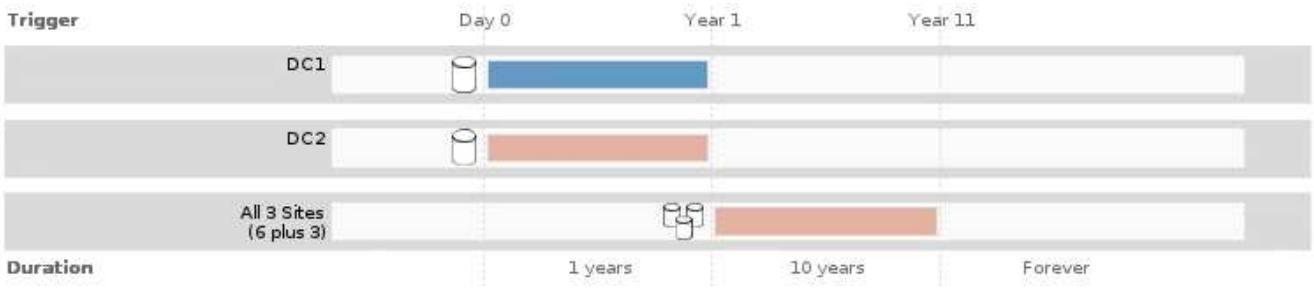
7. Seleccione **Actualizar** para actualizar el Diagrama de retención y confirmar las instrucciones de colocación.

   Cada línea del diagrama muestra dónde y cuándo se colocarán las copias de objeto. El tipo de copia está representado por uno de los siguientes iconos:

	Copia replicada
	Copia con código de borrado
	Copia de Cloud Storage Pool

   En este ejemplo, se guardarán dos copias replicadas en dos agrupaciones de almacenamiento (DC1 y DC2) durante un año. A continuación, se guardará una copia codificada con borrado durante 10 años

adicionales utilizando un esquema de codificación de borrado de 6+3 en tres ubicaciones. Transcurridos 11 años, los objetos se eliminarán de StorageGRID.



8. Seleccione **Siguiente**.

   Aparece el paso 3 (definir comportamiento de procesamiento).

Información relacionada

- Qué es una regla de ILM
- Gestione objetos con S3 Object Lock
- Paso 3 de 3: Definir el comportamiento de la ingesta

Utilice la hora del último acceso en las reglas de ILM

Puede usar la hora de Last Access 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 hora de última acceso como filtro avanzado si desea que una regla de ILM se aplique sólo a los objetos a los que se accedió por última vez en una fecha determinada.

Acerca de esta tarea

Antes de utilizar la hora del último acceso en una regla de ILM, revise las siguientes consideraciones:

- Cuando utilice la hora de última acceso como hora de referencia, tenga en cuenta que al cambiar la hora de último acceso de un objeto no se desencadena una evaluación de ILM inmediata. 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 tiempo del último acceso y evite ubicaciones que usan breves periodos de tiempo (menos de un mes).

- Cuando se utiliza la hora de última acceso como filtro avanzado o como hora de referencia, debe habilitar actualizaciones del último tiempo de acceso para bloques S3. Se puede usar 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 tabla siguiente se resume si se actualiza la hora del último acceso para todos los objetos del bloque para los diferentes tipos de peticiones.

Tipo de solicitud	Si la hora de último acceso se actualiza cuando se desactivan las actualizaciones de la última hora de acceso	Si la hora de último acceso se actualiza 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

Información relacionada

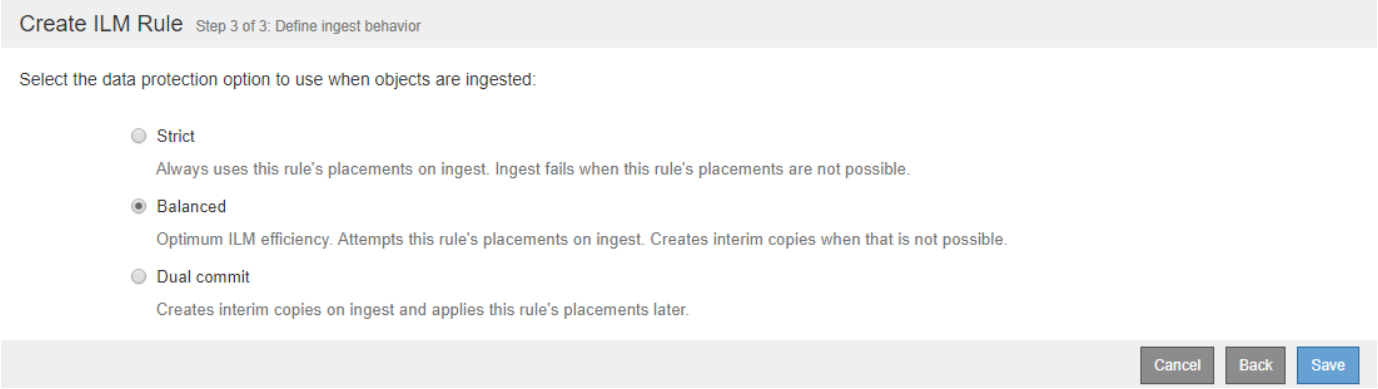
- Use S3
- Usar una cuenta de inquilino

Paso 3 de 3: Definir el comportamiento de la ingesta

El paso 3 (definir comportamiento de la ingesta) del asistente Crear regla de ILM permite elegir cómo se protegen los objetos filtrados por esta regla mientras 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 opción de protección de datos que se va a utilizar cuando se ingieren los objetos:

Opción	Descripción
Estricto	Siempre utiliza las colocaciones de esta regla durante el procesamiento. La ingesta falla cuando las colocaciones de esta regla no son posibles.
Equilibrado	Eficiencia óptima de ILM. Intenta colocar esta regla en el procesamiento. Crea copias provisionales cuando eso no es posible.
Registro doble	Crea copias provisionales en el procesamiento y aplica las colocaciones de esta regla más adelante.

   Balance ofrece una combinación de seguridad de datos y eficiencia que es adecuada en la mayoría de los casos. La confirmación estricta o doble se utiliza generalmente para satisfacer requisitos específicos.

   Consulte Opciones de protección de datos para consumo y.. Ventajas, inconvenientes y limitaciones de las opciones de protección de datos si quiere más información.

   > Aparece un mensaje de error si selecciona la opción estricta o equilibrada y 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 cloud o un nodo de archivado cuando la regla utiliza un tiempo de creación definido por el usuario como tiempo de referencia

2. Seleccione **Guardar**.

   Se guarda la regla ILM. La regla no estará activa hasta que se agregue a una política de ILM y esa política se active.

Información relacionada

- Ejemplo 5: Reglas de ILM y política para el comportamiento de consumo estricto
- Cree una política 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.

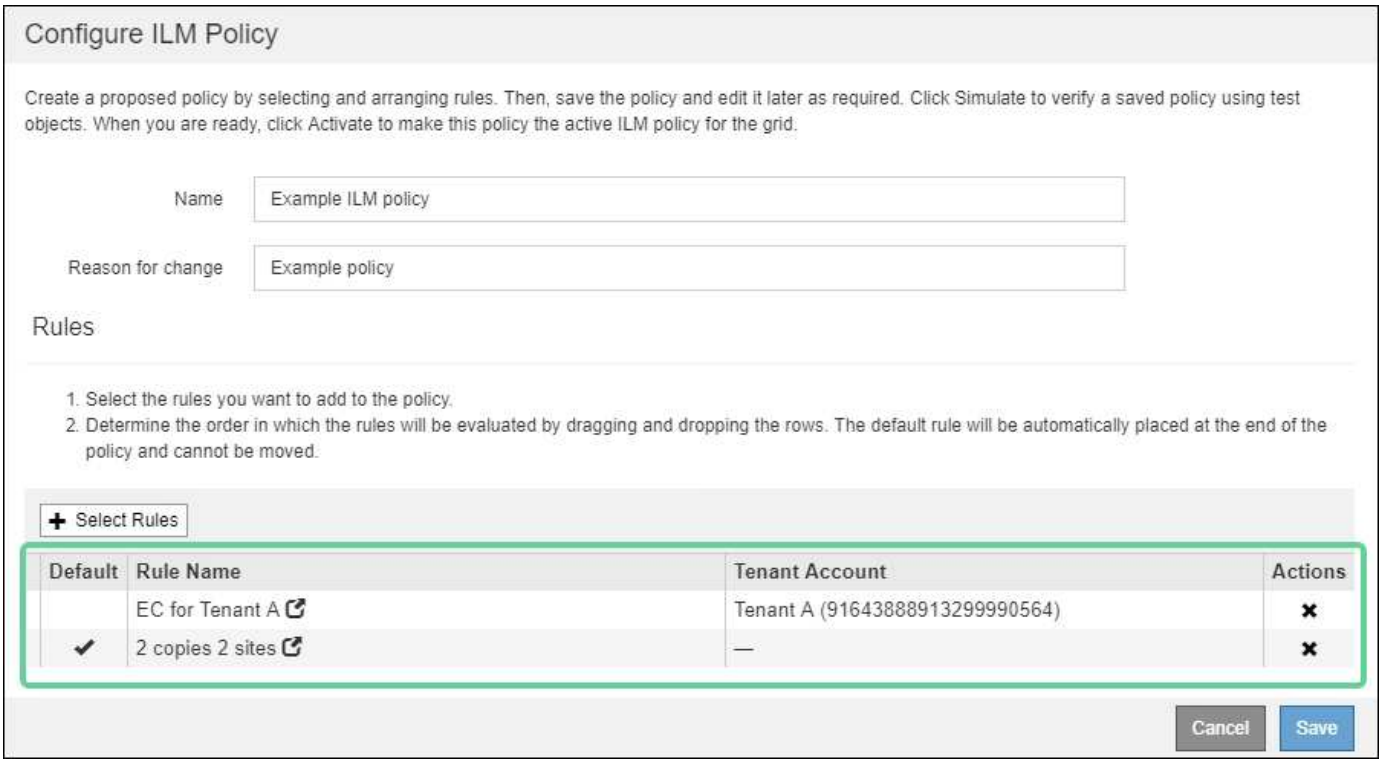
Lo que necesitará

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

Acerca de esta tarea

La regla predeterminada es la última regla que se evalúa en una política de ILM, por lo que no puede usar ningún filtro ni el tiempo de referencia no actual. Las instrucciones de colocación de la regla predeterminada se aplican a cualquier objeto que no coincida con otra regla de la directiva.

En esta política de ejemplo, la primera regla se aplica sólo a los objetos que pertenecen al arrendatario A. 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 coloca automáticamente como última regla en la directiva.
- La regla predeterminada no puede utilizar ningún filtro básico o avanzado.
- La regla predeterminada debe aplicarse a todas las versiones de objeto, por lo que no puede utilizar la hora de referencia no corriente.
- 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 deberían utilizar un filtro avanzado para evitar que los objetos más pequeños se codificen con el borrado.

- En general, la regla predeterminada debería retener objetos para siempre.
- Si está utilizando (o tiene previsto habilitar) la configuración de bloqueo de objetos global S3, la regla predeterminada para la directiva activa o propuesta debe ser compatible.

Pasos

1. Seleccione **ILM** > **Reglas**.

   Aparece la página ILM Rules.

2. Seleccione **Crear**.

   Aparece el paso 1 (definir datos básicos) del asistente Crear regla de ILM.

3. Introduzca un nombre único para la regla en el campo **Nombre**.
4. Si lo desea, introduzca una breve descripción de la regla en el campo **Descripción**.
5. Deje el campo **Cuentas de inquilino** en blanco.

   La regla predeterminada debe aplicarse a todas las cuentas de arrendatario.

6. Deje en blanco el campo **Nombre de bloque**.

   La regla predeterminada debe aplicarse a todos los bloques de S3 y contenedores Swift.

7. No seleccione **filtrado avanzado**

   La regla predeterminada no puede especificar ningún filtro.

8. Seleccione **Siguiente**.

   Aparece el paso 2 (definir ubicaciones).

9. Para tiempo de referencia, seleccione cualquier opción excepto **tiempo no corriente**.

   La regla predeterminada debe aplicar todas las versiones del objeto.

10. 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 **Tamaño de objeto (MB) superior al 0.2** avanzado para evitar que los objetos más pequeños se codifican con el 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 cloud.
- 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 procesamiento como tiempo de referencia.
- Al menos una línea de las instrucciones de colocación deberá ser «'para siempre».

11. Seleccione **Actualizar** para actualizar el Diagrama de retención y confirmar las instrucciones de colocación.
12. Seleccione **Siguiente**.

    Aparece el paso 3 (definir comportamiento de procesamiento).

13. Seleccione la opción de protección de datos que se va a utilizar cuando se ingieren objetos y seleccione **Guardar**.

Cree una política de ILM

Cree una política de ILM: Descripción general

Al crear una política de ILM, para comenzar, debe seleccionar y organizar las reglas de ILM. A continuación, se comprueba el comportamiento de la directiva propuesta simulándola de objetos ingeridos previamente. Cuando esté satisfecho de que la directiva propuesta funcione según lo previsto, puede activarla para crear la directiva activa.

> 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.

Consideraciones que tener en cuenta para crear una política de ILM

- Utilice la política integrada del sistema, la directiva de copias base 2, sólo en sistemas de prueba. La regla hacer 2 copias 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.
- 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, dicha regla no será evaluada por ninguna otra regla.

- La última regla de todas las políticas de ILM es la regla predeterminada de ILM, 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.

Cree una política de ILM propuesta

Puede crear una política de ILM propuesta desde cero o clonar la política activa actual si desea empezar con el mismo conjunto de reglas.

> Si se habilitó el ajuste global de bloqueo de objetos S3, utilice este procedimiento en su lugar: Cree una política de ILM después de habilitar el bloqueo de objetos de S3.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha creado las reglas de ILM que desea añadir a la política propuesta. Según sea necesario, puede guardar una directiva propuesta, crear reglas adicionales y, a continuación, editar la directiva propuesta para agregar las nuevas reglas.
- Ya tienes Se ha creado una regla de ILM predeterminada para la directiva que no contiene ningún filtro.
- Opcionalmente, ha visto el vídeo: "Vídeo: Políticas de ILM de StorageGRID"

Acerca de esta tarea

Algunos de los motivos típicos para crear una política de ILM propuesta son:

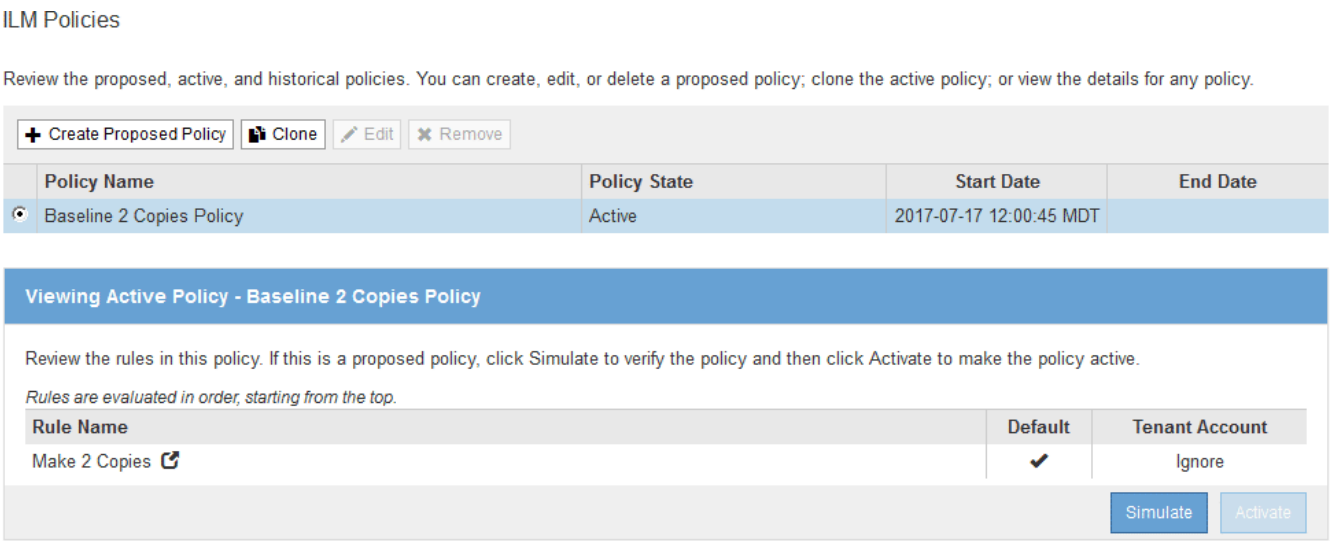
- Ha añadido un sitio nuevo y debe utilizar nuevas reglas de ILM para colocar objetos en dicho sitio.
- Se está decomisionando un sitio y es necesario eliminar todas las reglas que hacen referencia al sitio.
- Se ha agregado un nuevo inquilino que tiene requisitos especiales de protección de datos.
- Comenzó a utilizar un pool de almacenamiento en el cloud.

Utilice la política integrada del sistema, la directiva de copias base 2, sólo en sistemas de prueba. La regla hacer 2 copias 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.

Pasos

1. Seleccione **ILM** > **políticas**.

   Aparece la página ILM Policies. En esta página puede revisar la lista de políticas propuestas, activas e históricas; crear, editar, o elimine una política propuesta; clone la política activa o vea los detalles de cualquier política.

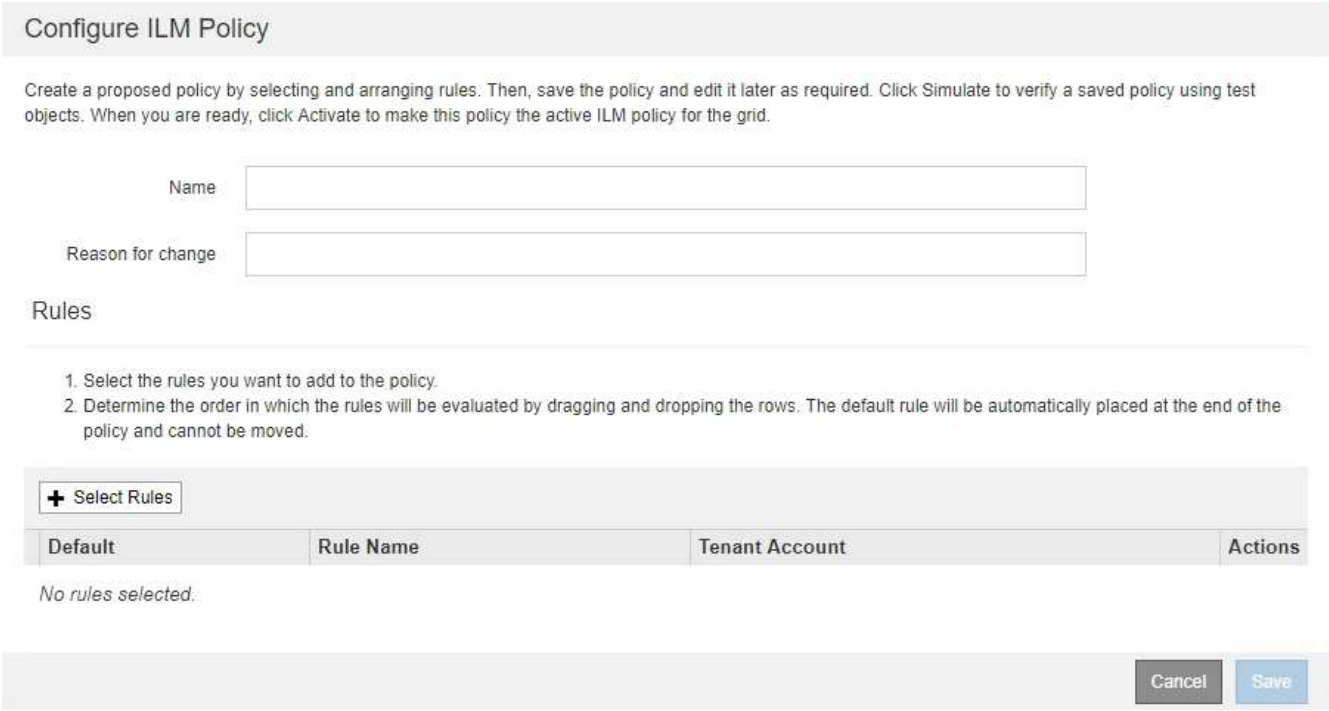


2. Determine cómo desea crear la política de ILM propuesta.

Opción	Pasos
Cree una nueva directiva propuesta que no tenga reglas ya seleccionadas	a. Si actualmente existe una política ILM propuesta, seleccione esa política y seleccione **Quitar**. No puede crear una nueva directiva propuesta si ya existe una propuesta. b. Seleccione **Crear directiva propuesta**.
Crear una directiva propuesta basada en la política activa	a. Si actualmente existe una política ILM propuesta, seleccione esa política y seleccione **Quitar**. No puede clonar la política activa si ya existe una política propuesta. b. Seleccione la directiva activa de la tabla. c. Seleccione **Clonar**.
Edite la directiva propuesta existente	a. Seleccione la directiva propuesta en la tabla. b. Seleccione **Editar**.

Se muestra el cuadro de diálogo Configurar política de ILM.

Si va a crear una nueva directiva propuesta, todos los campos estarán en blanco y no se seleccionará ninguna regla.



Si va a clonar la directiva activa, el campo **Nombre** muestra el nombre de la directiva activa, adjunto por un número de versión ("'v2'" en el ejemplo). Las reglas utilizadas en la directiva activa se seleccionan y se muestran en su orden actual.

3. Introduzca un nombre único para la directiva propuesta en el campo **Nombre**.

   Debe introducir al menos 1 y no más de 64 caracteres. Si clona la política activa, puede utilizar el nombre actual con el número de versión añadido o puede introducir un nuevo nombre.

4. Introduzca el motivo por el que está creando una nueva directiva propuesta en el campo **motivo del cambio**.

   Debe introducir al menos 1 y no más de 128 caracteres.

5. Para agregar reglas a la directiva, seleccione **Seleccionar reglas**.

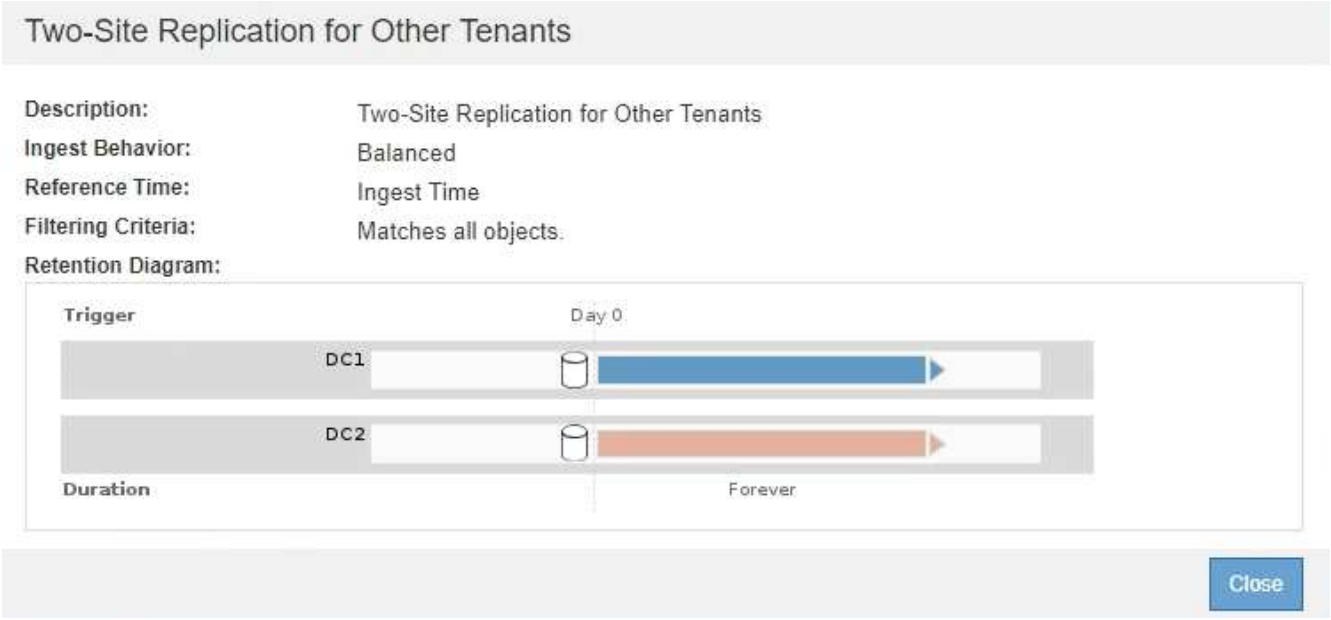
   Aparece el cuadro de diálogo Seleccionar reglas para la directiva, con todas las reglas definidas en la lista. Si está clonando una política:

   - 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 utiliza un filtro o la hora de referencia no corriente, se le solicitará que seleccione una nueva regla predeterminada.
- Si la regla predeterminada no era la última regla, un botón le permite mover la regla al final de la nueva directiva.

6. Seleccione un nombre de regla o el icono más detalles para ver la configuración de esa regla.

   Este ejemplo muestra los detalles de una regla de ILM que realiza dos copias replicadas en dos sitios.



7. En la sección **Seleccionar regla predeterminada**, seleccione una regla predeterminada para la directiva propuesta.

   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.

> Si no aparece ninguna regla en la sección Select Default Rule, debe salir de la página de la política de ILM y. Cree una regla de ILM predeterminada.

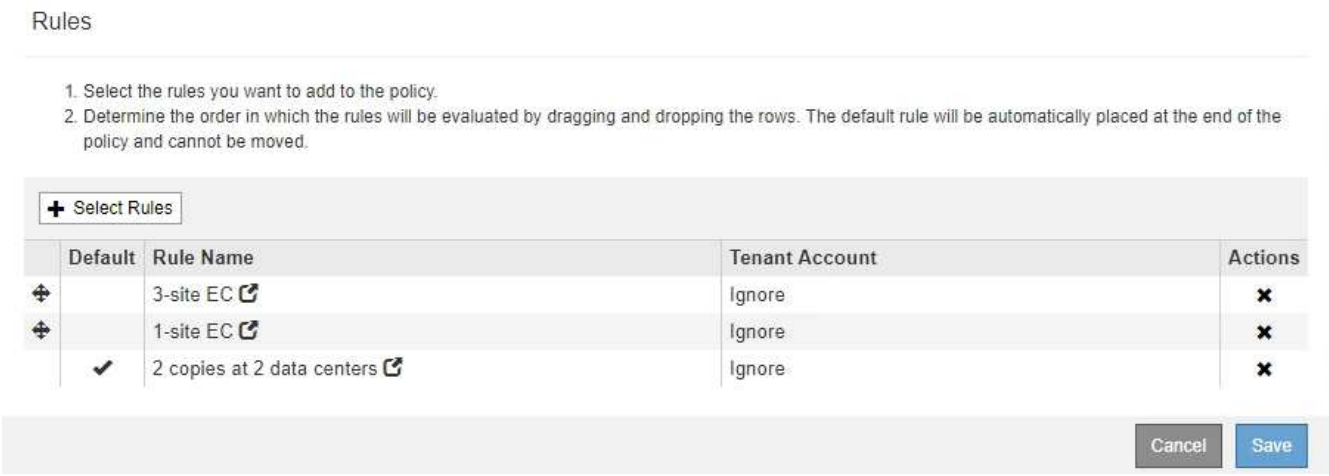
> No utilice la regla convertir 2 copias en stock como regla predeterminada para una directiva. La regla make 2 copies utiliza un único pool de almacenamiento, todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.

8. En la sección **Seleccionar otras reglas**, seleccione cualquier otra regla que desee incluir en la directiva.

   Las demás reglas se evalúan antes de la regla predeterminada y deben utilizar al menos un filtro (cuenta de inquilino, nombre de bloque, filtro avanzado o tiempo de referencia no corriente).

9. Cuando haya terminado de seleccionar reglas, seleccione **aplicar**.

   Se muestran las reglas seleccionadas. La regla predeterminada está al final, con las demás reglas encima.



> Aparece una advertencia si la regla predeterminada no conserva objetos para siempre. Al activar esta política, debe confirmar que desea que StorageGRID elimine objetos cuando transcurra las instrucciones de colocación de la regla predeterminada (a menos que un ciclo de vida de bloque mantenga los objetos durante más tiempo).

10. Arrastre y suelte las filas de las reglas no predeterminadas para determinar el orden en el que se evaluarán estas reglas.

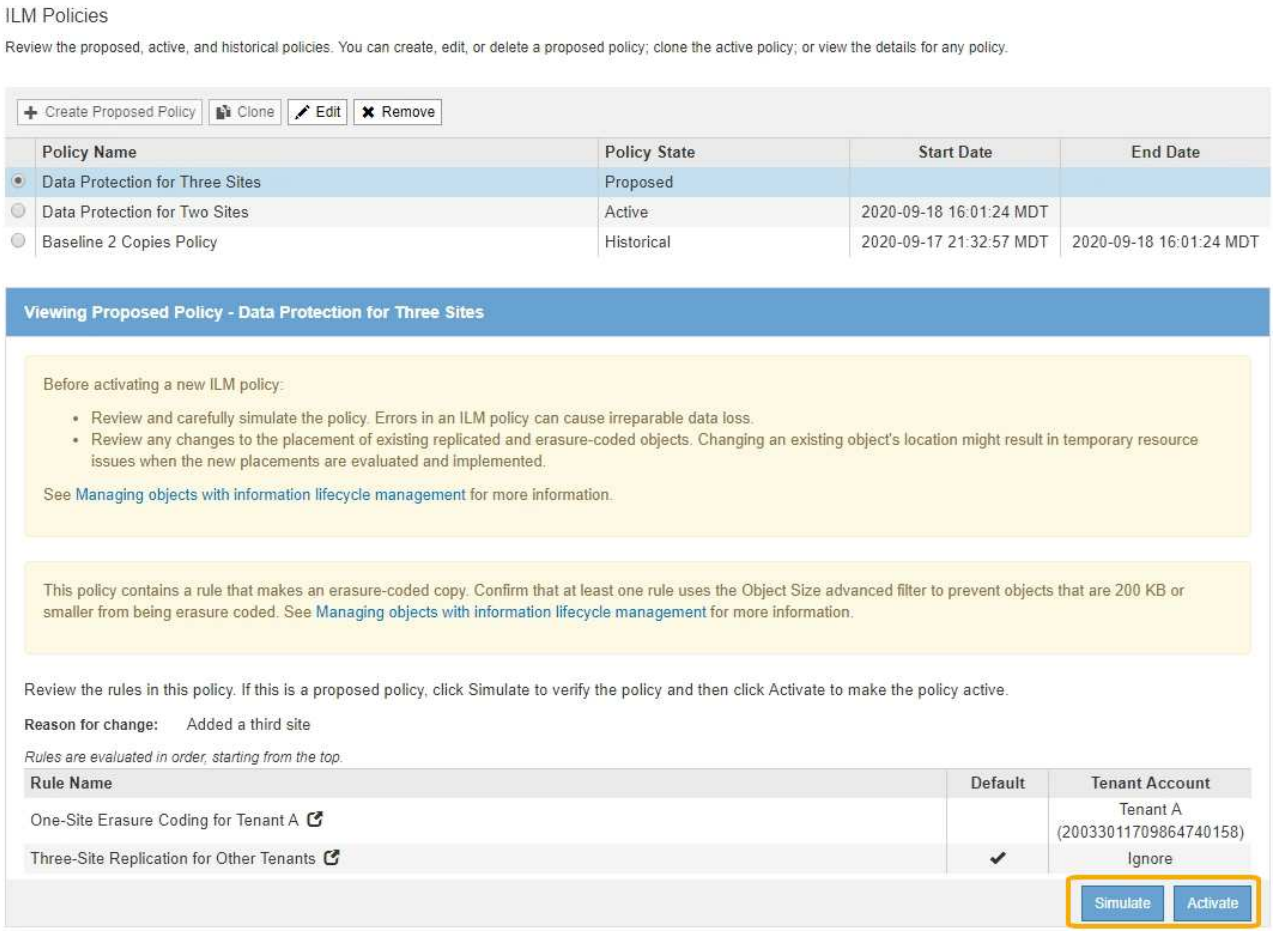
    No se puede mover la regla predeterminada.

> 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.

11. Según sea necesario, seleccione el icono de eliminación ✖ Para eliminar cualquier regla que no desee en la directiva o seleccione **Seleccionar reglas** para agregar más reglas.
12. Cuando haya terminado, seleccione **Guardar**.

    La página ILM Policies se actualiza:

    - La política que ha guardado se muestra como propuesta. Las políticas propuestas no tienen fechas de inicio y finalización.
    - Los botones **Simulate** y **Activate** están activados.



13. Vaya a. Simule una política de gestión de la vida útil.

Información relacionada

- Qué es una política de ILM
- Gestione objetos con S3 Object Lock

Cree una política de ILM después de habilitar el bloqueo de objetos de S3

Si la configuración global de bloqueo de objetos S3 está habilitada, los pasos para crear una política son ligeramente diferentes. Debe asegurarse de que la política de ILM

cumpla con los requisitos de los bloques con S3 Object Lock habilitado.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- La configuración global de bloqueo de objetos S3 ya está habilitada para el sistema StorageGRID.

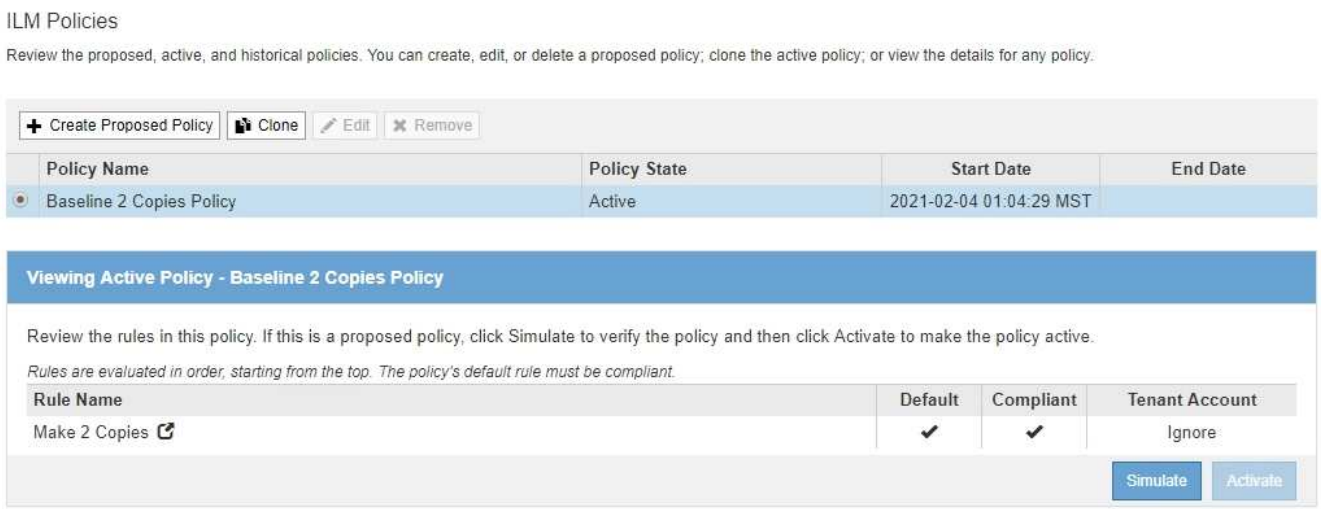
> Si la opción de bloqueo de objetos global de S3 no se ha habilitado, utilice las instrucciones generales para Creación de una política de ILM propuesta.

- Ha creado las reglas de ILM que cumplen y no cumplen con las normativas que desea agregar a la política propuesta. Según sea necesario, puede guardar una directiva propuesta, crear reglas adicionales y, a continuación, editar la directiva propuesta para agregar las nuevas reglas. ConsulteEjemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3.
- 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 ILM de StorageGRID"

Pasos

1. Seleccione **ILM** > **políticas**.

   Aparece la página ILM Policies. Si la configuración de bloqueo de objetos global de S3 está habilitada, la página ILM Policies indica qué reglas de ILM son compatibles.



2. Introduzca un nombre único para la directiva propuesta en el campo **Nombre**.

   Debe introducir al menos 1 y no más de 64 caracteres.

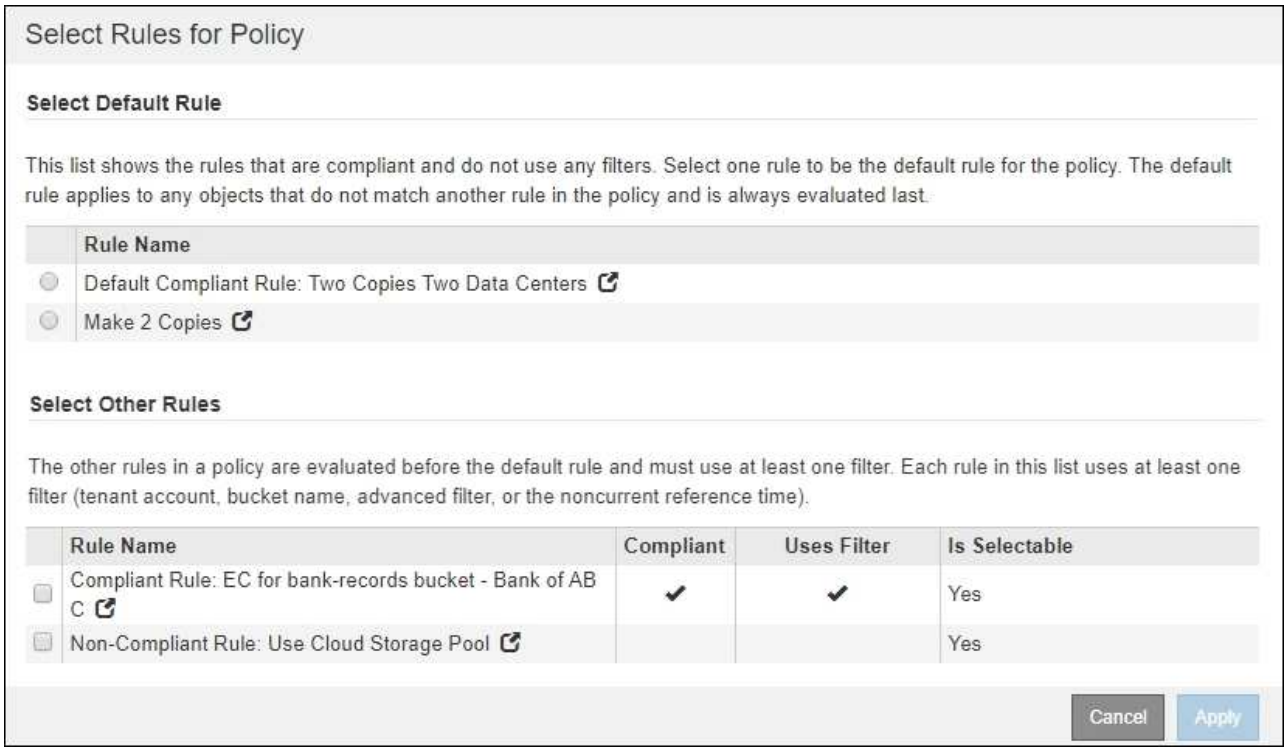
3. Introduzca el motivo por el que está creando una nueva directiva propuesta en el campo **motivo del cambio**.

   Debe introducir al menos 1 y no más de 128 caracteres.

4. Para agregar reglas a la directiva, seleccione **Seleccionar reglas**.

   Aparece el cuadro de diálogo Seleccionar reglas para la directiva, con todas las reglas definidas en la lista.

   - La sección Seleccionar regla predeterminada enumera las reglas que pueden ser predeterminadas para una directiva compatible. Incluye reglas compatibles que no utilizan filtros ni el tiempo de referencia no corriente.
   - La sección Seleccionar otras reglas enumera las demás reglas compatibles y no compatibles que se pueden seleccionar para esta directiva.



5. Seleccione un nombre de regla o el icono más detalles para ver la configuración de esa regla.
6. En la sección **Seleccionar regla predeterminada**, seleccione una regla predeterminada para la directiva propuesta.

   En la tabla de esta sección sólo se enumeran las reglas que cumplen y no utilizan ningún filtro.

   > Si no aparece ninguna regla en la sección Select Default Rule, debe salir de la página de la política de ILM y. Cree una regla de ILM predeterminada eso es conforme.

   > No utilice la regla convertir 2 copias en stock como regla predeterminada para una directiva. 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.

7. En la sección **Seleccionar otras reglas**, seleccione cualquier otra regla que desee incluir en la directiva.

   a. Si necesita una regla «predeterminada» distinta para los objetos de bloques S3 que no cumplen las normativas, seleccione opcionalmente una regla no conforme a la normativa que no utilice un filtro.

      Por ejemplo, se recomienda usar un pool de almacenamiento en cloud o un nodo de archivado para almacenar objetos en bloques que no tienen el bloqueo de objetos de S3 habilitado.

      > Sólo puede seleccionar una regla no compatible que no utilice un filtro. Tan pronto como seleccione una regla, la columna **is Selectable** muestra **no** para cualquier otra regla no compatible sin filtros.

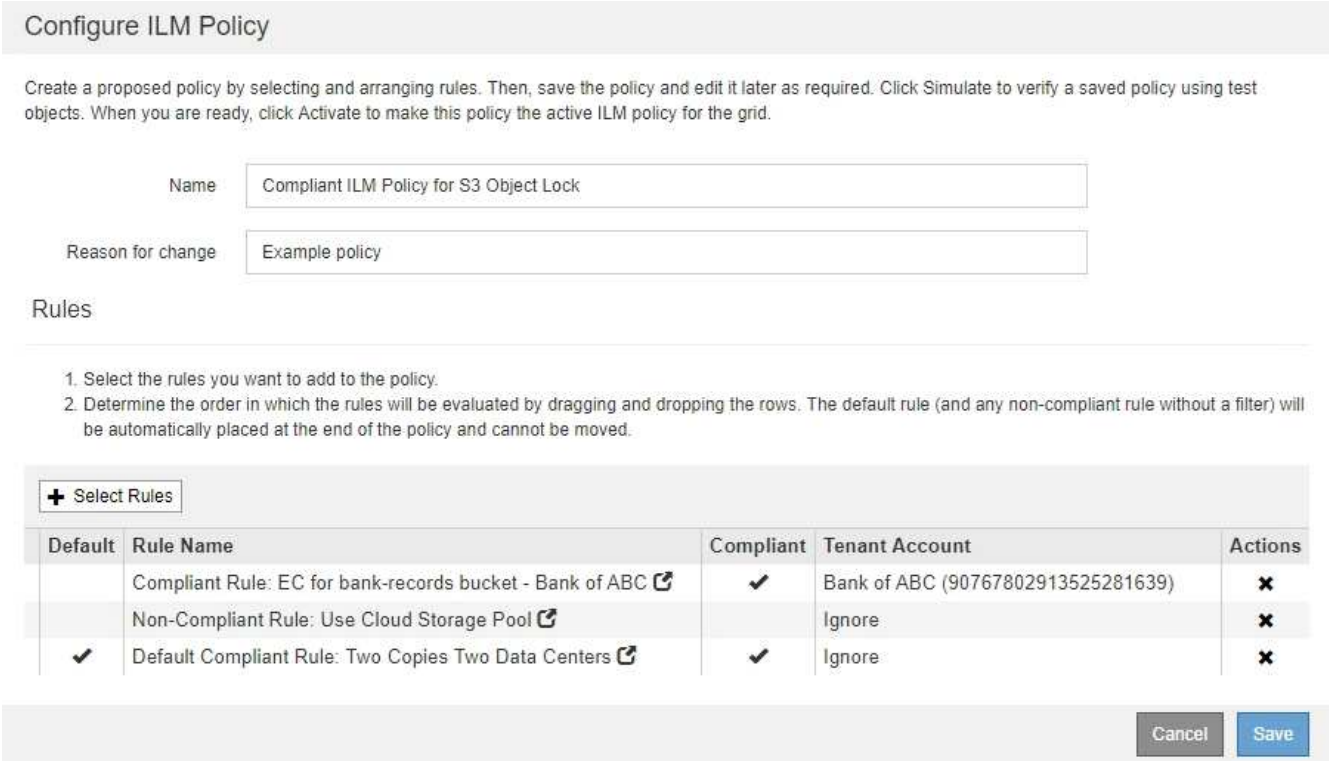
   a. Seleccione cualquier otra regla compatible o no compatible que desee utilizar en la directiva.

      Las otras reglas deben utilizar al menos un filtro (cuenta de inquilino, nombre de bloque o filtro avanzado, como el tamaño del objeto).

8. Cuando haya terminado de seleccionar las reglas, seleccione **aplicar**.

   Se muestran las reglas seleccionadas. La regla predeterminada está al final, con las demás reglas encima. Si también ha seleccionado una regla de «default» no conforme, esa regla se añade como la regla de segundo a último en la política.

   En este ejemplo, la última regla, 2 copias 2 centros de datos, es la regla predeterminada: Es compatible y no tiene filtros. La segunda regla, Cloud Storage Pool, también no tiene filtros pero no es conforme.



9. Arrastre y suelte las filas de las reglas no predeterminadas para determinar el orden en el que se evaluarán estas reglas.

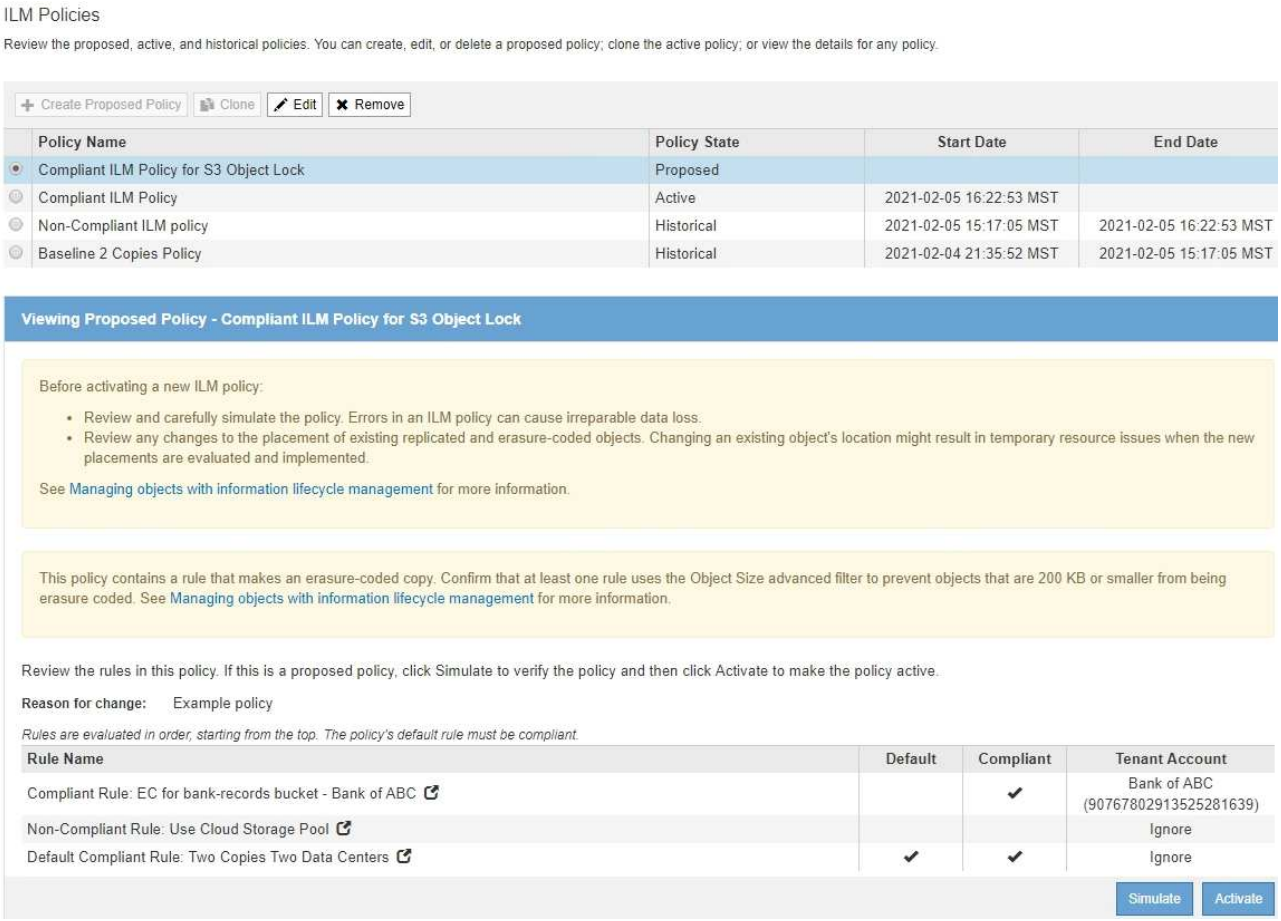
   No se puede mover la regla predeterminada ni la regla de «incumplimiento».

   > 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.

10. Según sea necesario, seleccione el icono de eliminación ✖ Para eliminar cualquier regla que no desee en la directiva, o **Seleccionar reglas** para agregar más reglas.
11. Cuando haya terminado, seleccione **Guardar**.

    La página ILM Policies se actualiza:

    - La política que ha guardado se muestra como propuesta. Las políticas propuestas no tienen fechas de inicio y finalización.
    - Los botones **Simulate** y **Activate** están activados.



12. Vaya a. Simule una política de gestión de la vida útil.

Simule una política de gestión de la vida útil

Debe simular una directiva propuesta en objetos de prueba antes de activar la directiva y aplicarla a los datos de producción. La ventana de simulación proporciona un entorno independiente que es seguro para las políticas de prueba antes de que se activen y apliquen a los datos en el entorno de producción.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Conoce el bucket/object-key o el contenedor/nombre de objeto de Swift para cada objeto que desea probar y ya ha ingerido esos objetos.

Acerca de esta tarea

Debe seleccionar cuidadosamente los objetos que desea que pruebe la directiva propuesta. Para simular una política completamente, debe probar al menos un objeto para cada filtro en cada regla.

Por ejemplo, si una política incluye una regla para que coincida con los objetos del bloque A y otra regla para que coincidan con los objetos del bloque B, debe seleccionar al menos un objeto del bloque A y un objeto del bloque B para probar la política a fondo. También debe seleccionar al menos un objeto de otro bloque para probar la regla predeterminada.

Al simular una directiva, se aplican las siguientes consideraciones:

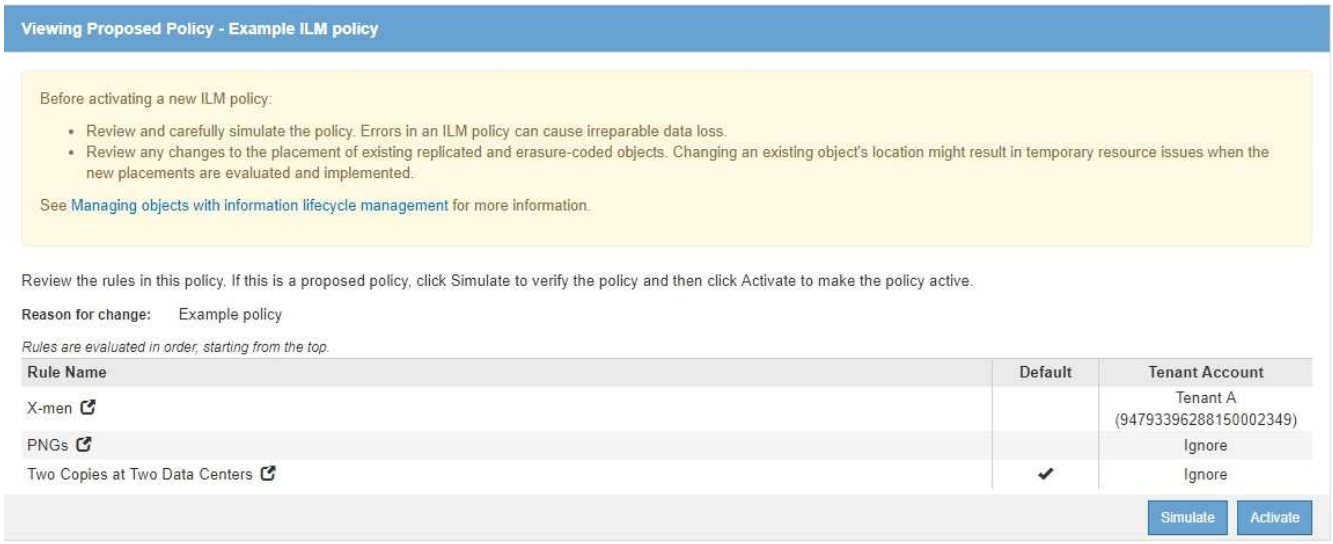
- Después de realizar cambios en una directiva, guarde la directiva propuesta. A continuación, simule el comportamiento de la directiva propuesta guardada.
- Cuando se simula una política, las reglas de ILM en la política filtran los objetos de prueba, de modo que se puede ver qué regla se aplicó a cada objeto. Sin embargo, no se crean copias de objeto y no se coloca ningún objeto. Al ejecutar una simulación no se modifican los datos, las reglas ni la política de ningún modo.
- La página Simulation conserva los objetos probados hasta que se cierra, se aleja o se actualiza la página políticas de ILM.
- Simulation devuelve el nombre de la regla coincidente. Para determinar qué pool de almacenamiento o perfil de código de borrado está activo, puede ver el diagrama de retención seleccionando el nombre de la regla o el icono más detalles .
- Si está habilitada la versión de S3, la política solo se simula con respecto a la versión actual del objeto.

Pasos

1. Seleccione y organice las reglas y guarde la política propuesta.

   La directiva de este ejemplo tiene tres reglas:

Nombre de regla	Filtro	Tipo de copias	Retención
Hombres-X.	• Inquilinoa • Metadatos del usuario (series=x-men)	2 copias en dos centros de datos	2 años
PNs	La clave termina con .png	2 copias en dos centros de datos	5 años
Dos copias dos centros de datos	*Ninguno*	2 copias en dos centros de datos	Para siempre



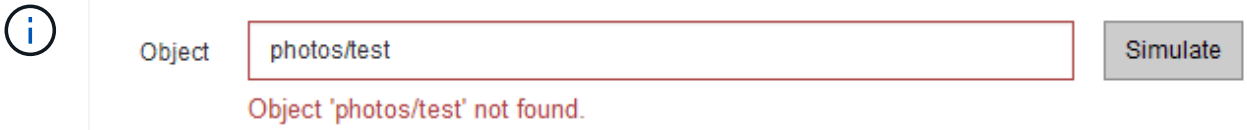
2. Use un cliente S3 o Swift o el Consola de S3 de experimental, Que está disponible en el Administrador de arrendatarios para cada arrendatario, procese los objetos necesarios para probar cada regla.

3. Seleccione **simular**.

   Aparecerá el cuadro de diálogo Directiva de gestión de la vida útil de Simulation.

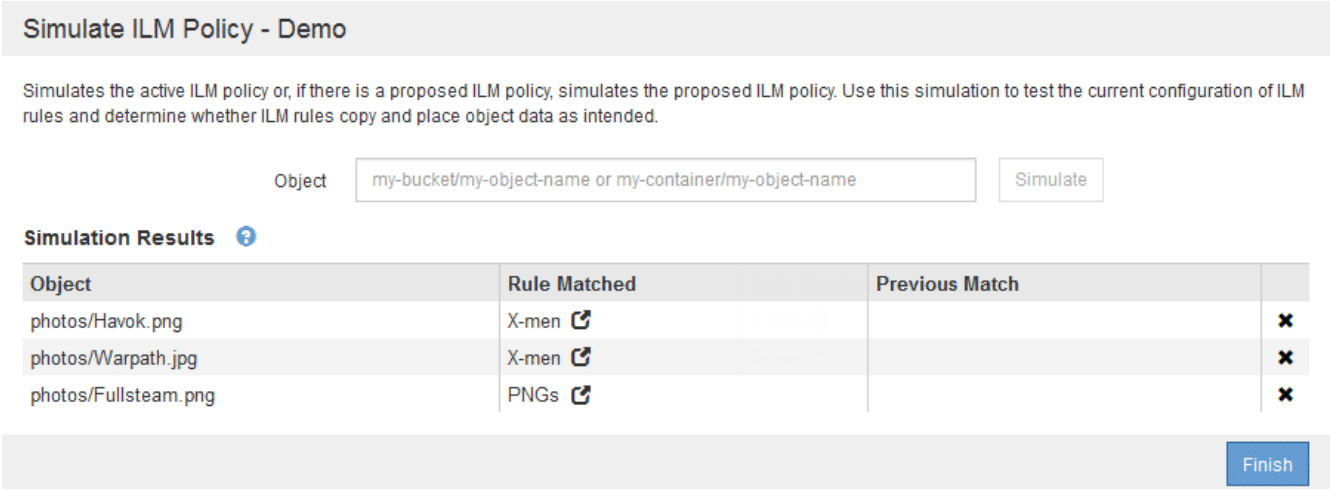
4. En el campo **Object**, introduzca el bucket/object-key de S3 o el nombre de objeto/contenedor de Swift para un objeto de prueba y seleccione **Simulate**.

   Aparece un mensaje si especifica un objeto que no se ha ingerido.

5. En **resultados de Simulation**, confirme que cada objeto estaba coincidente con la regla correcta.

   En el ejemplo, la `Havok.png` y.. `Warpath.jpg` Los objetos estaban correctamente emparejados con la regla X-men. La `Fullsteam.png` objeto, que no incluye `series=x-men` Los metadatos del usuario no se corresponden con la regla X-men, pero se emparejaron correctamente con la regla PNG. La regla predeterminada no se ha utilizado porque los tres objetos coinciden con otras reglas.

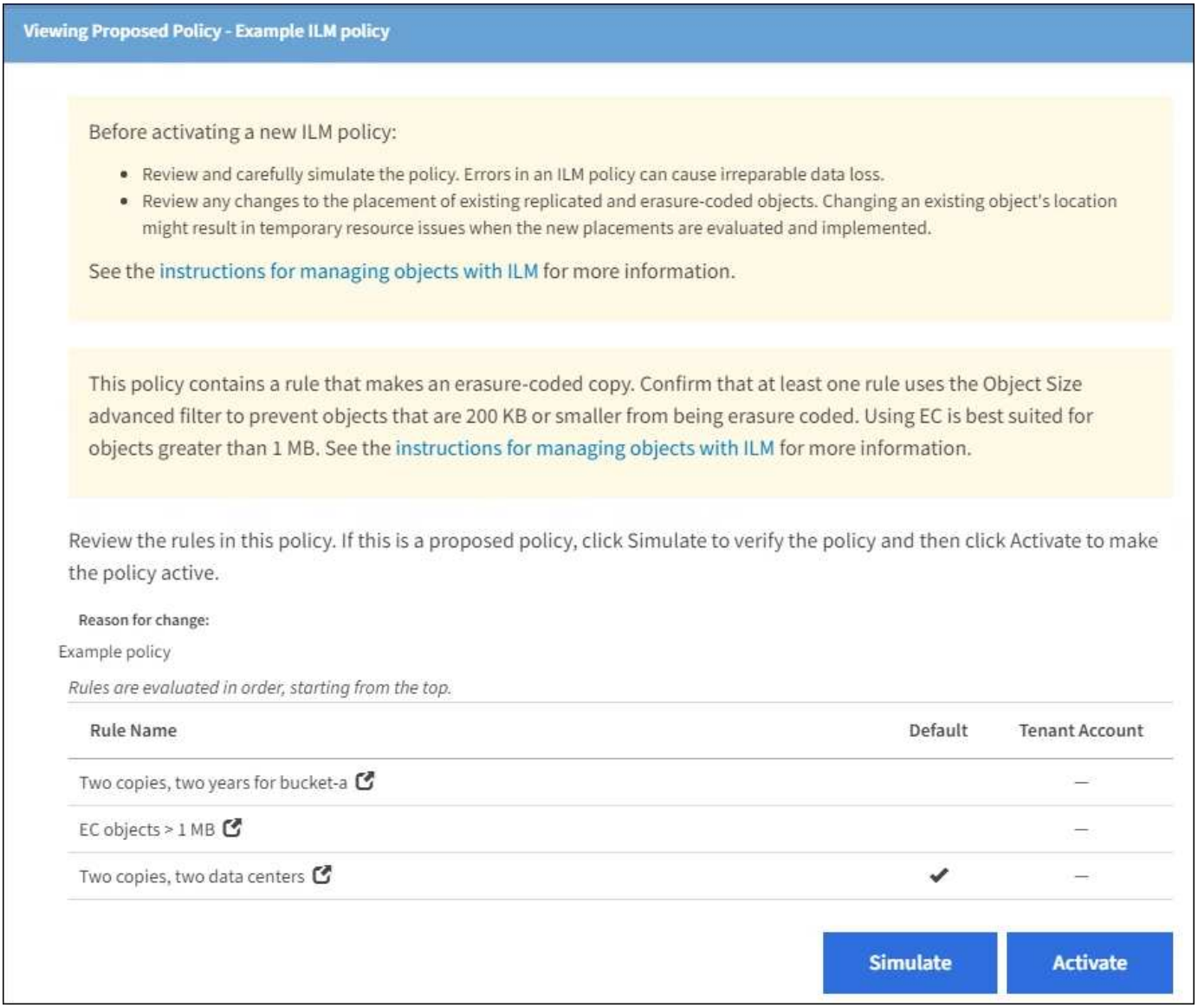
   

Ejemplo 1: Verifique las reglas al simular una política de ILM propuesta

En este ejemplo se muestra cómo comprobar las reglas al simular una directiva propuesta.

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.



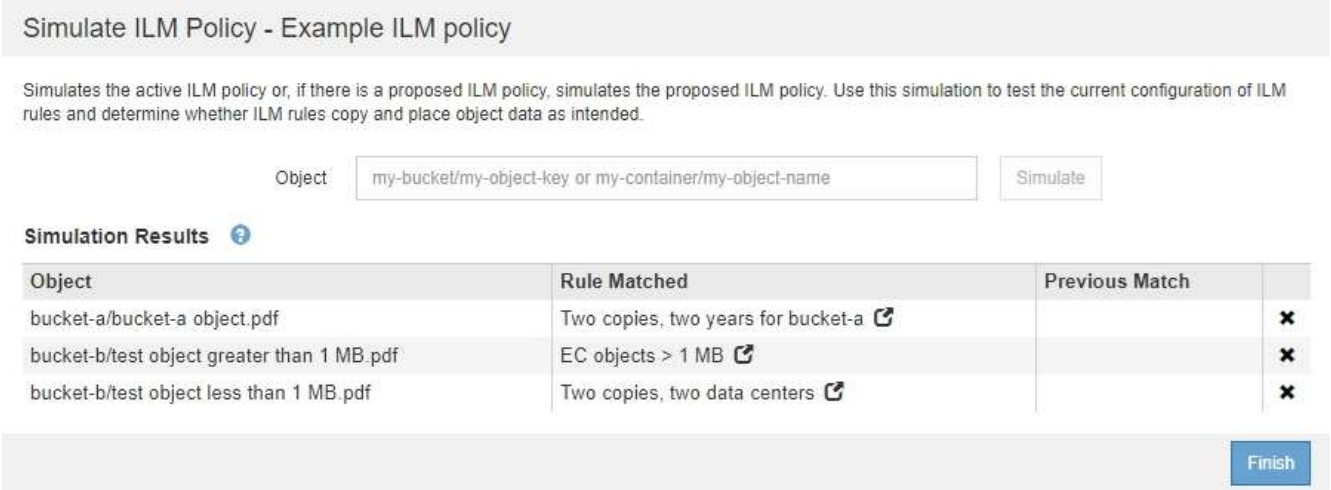
Pasos

1. Después de agregar las reglas y guardar la directiva, seleccione **simular**.

   Se muestra el cuadro de diálogo Simulate ILM Policy.

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, mostrando qué regla de la directiva coincide con cada objeto probado.



3. Confirme que cada objeto se ha coincidido con la regla correcta.

   En este ejemplo:

   a. `bucket-a/bucket-a object.pdf` coincide correctamente con la primera regla, que filtra los objetos de `bucket-a`.

   b. `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.

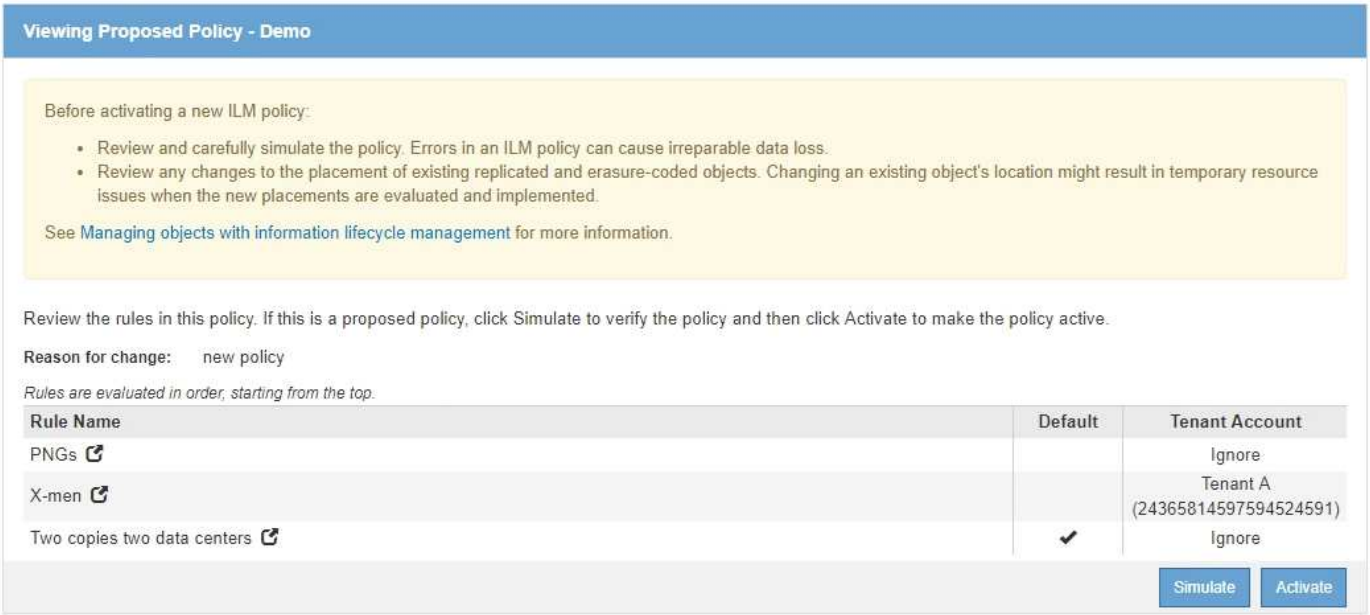
   c. `bucket-b/test object less than 1 MB.pdf` no coincide con los filtros de las dos primeras reglas, por lo que se colocará por la regla predeterminada, que no incluye ningún filtro.

Ejemplo 2: Reordenación de reglas al simular una política de ILM propuesta

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:

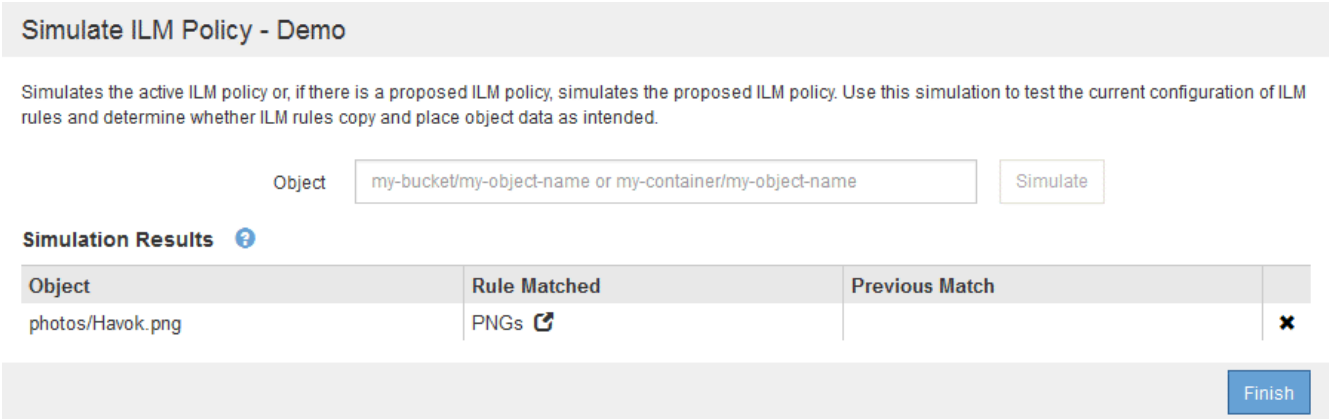
- La primera regla, **PNgs**, filtra los nombres de clave que terminan en `.png`.
- La segunda regla, **X-men**, se aplica sólo a los objetos para el arrendatario A y filtros para `series=x-men` metadatos del usuario.
- La última regla, **dos copias dos centros de datos**, es la regla predeterminada, que coincide con cualquier objeto que no coincida con las dos primeras reglas.



Pasos

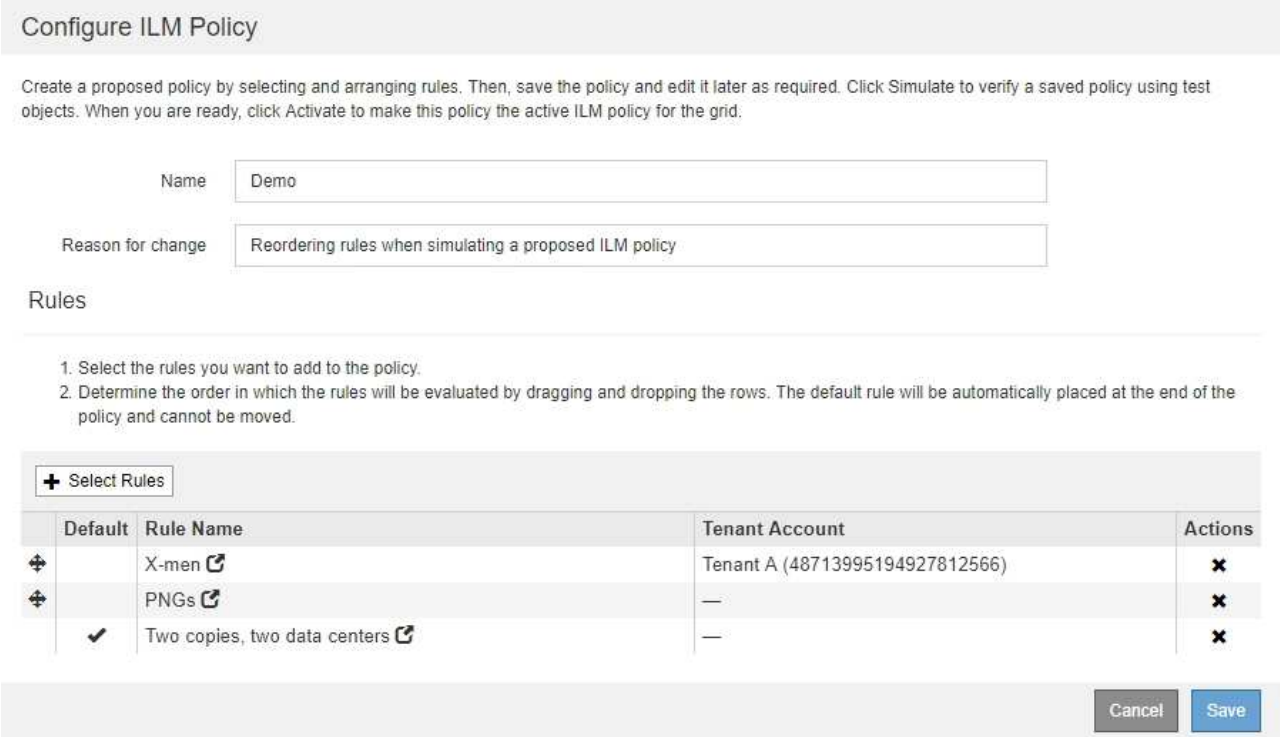
1. Después de agregar las reglas y guardar la directiva, seleccione **simular**.
2. En el campo **Object**, introduzca el bucket/object-key de S3 o el nombre de objeto/contenedor de Swift para un objeto de prueba y seleccione **Simulate**.

   Aparecen los resultados de Simulation, mostrando que `Havok.png` El objeto coincide con la regla **PNgs**.



   Sin embargo, la regla que el `Havok.png` El objeto fue ideado para probar la regla **X-men**.

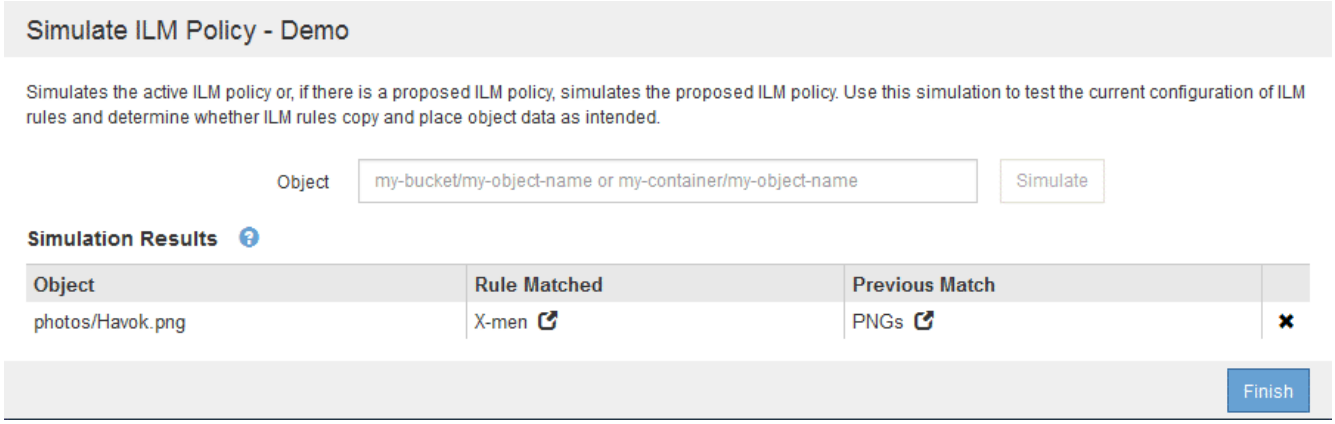
3. Para resolver el problema, vuelva a ordenar las reglas.
   a. Seleccione **Finalizar** para cerrar la página simular política de ILM.
   b. Seleccione **Editar** para editar la directiva.
   c. Arrastre la regla **X-men** hasta la parte superior de la lista.



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 conciliada muestra que `Havok.png` Ahora Object coincide con la regla de metadatos X-men, según lo esperado. La columna coincidencia anterior muestra que la regla PNG coincide con el objeto de la simulación anterior.



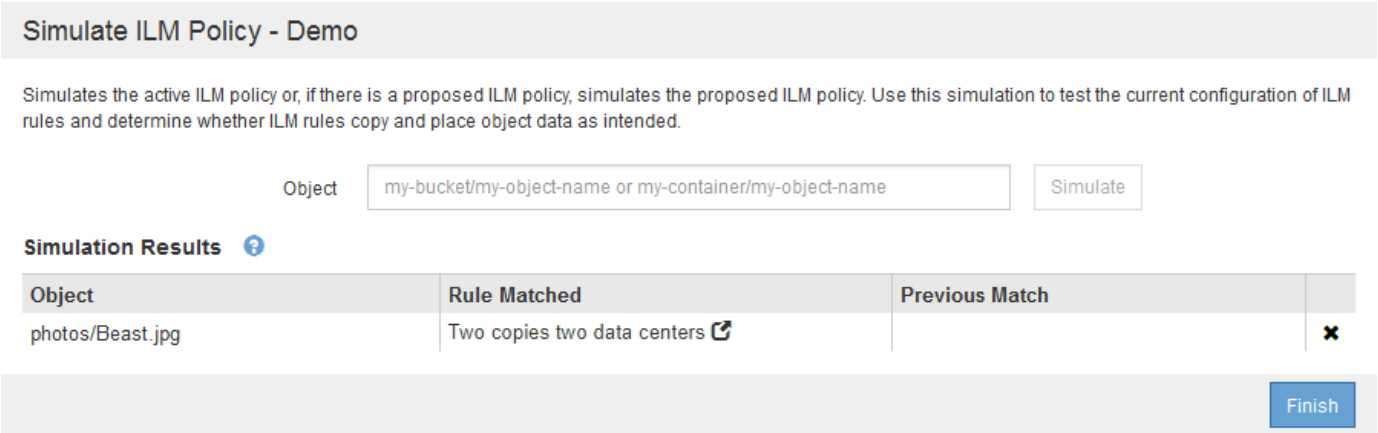
> Si permanece en la página Configure Policies, puede volver a simular una política después de realizar cambios sin tener que volver a introducir los nombres de los objetos de prueba.

Ejemplo 3: Corrección de una regla al simular una política de ILM propuesta

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.

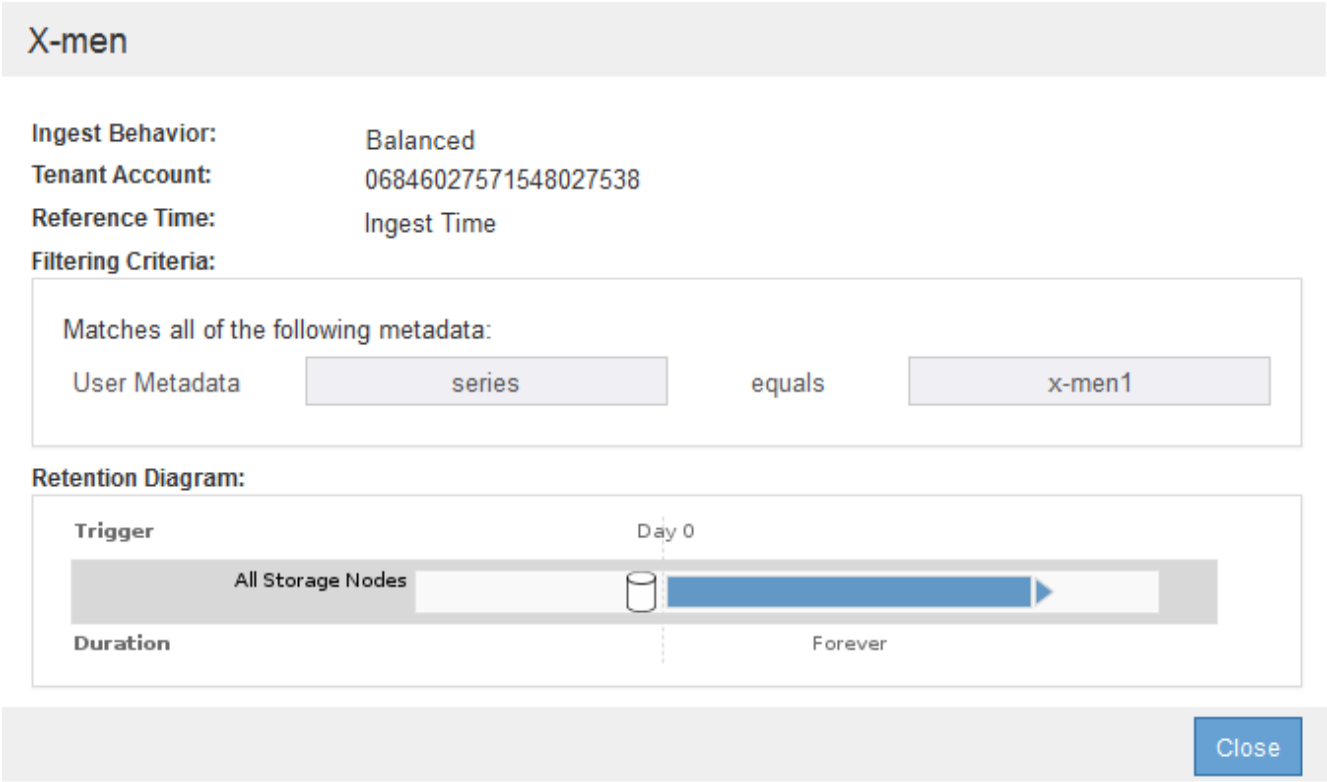


Cuando un objeto de prueba no coincide con la regla esperada de la directiva, debe examinar cada regla de la directiva y corregir cualquier error.

Pasos

1. Para cada regla de la política, consulte la configuración de reglas seleccionando el nombre de la regla o el icono más detalles en cualquier cuadro de diálogo en el que se muestre la regla.
2. Revise la cuenta de arrendatario de la regla, el tiempo de referencia y los criterios de filtrado.

   En este ejemplo, los metadatos de la regla X-men incluyen un error. El valor de los metadatos se introdujo como «'x-men1'» en lugar de «'x-men'».



3. Para resolver el error, corrija la regla de la siguiente manera:

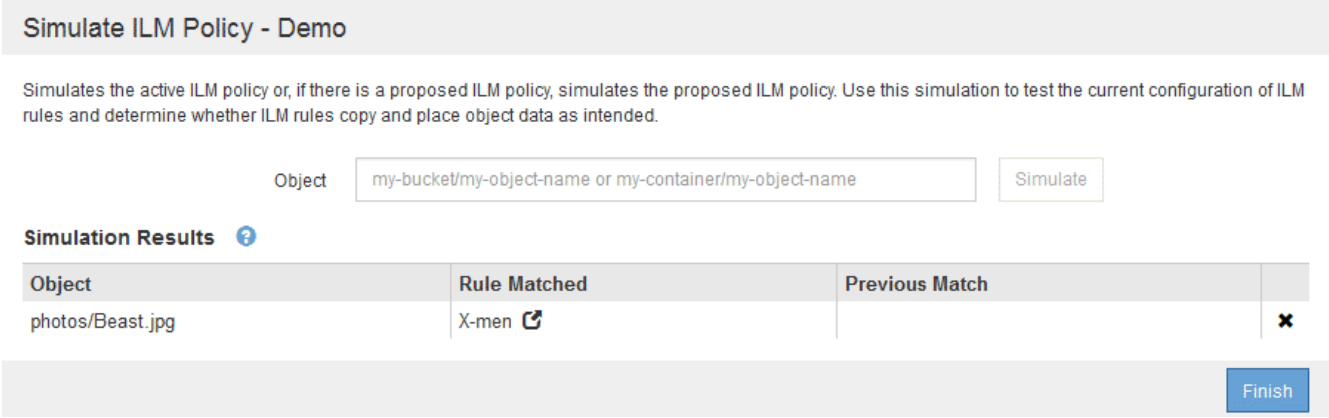
- Si la regla forma parte de la política propuesta, puede clonar la regla o quitar la regla de la política y editarla.
- Si la regla forma parte de la política activa, debe clonar esa regla. No puede editar ni eliminar una regla de la directiva activa.

Opción	Descripción
Clone la regla	i. Seleccione **ILM** > **Reglas**. ii. Seleccione la regla incorrecta y seleccione **Clonar**. iii. Cambie la información incorrecta y seleccione **Guardar**. iv. Seleccione **ILM** > **políticas**. v. Seleccione la directiva propuesta y seleccione **Editar**. vi. Seleccione **Seleccionar reglas**. vii. Active la casilla de verificación de la nueva regla, desactive la casilla de verificación de la regla original y seleccione **aplicar**. viii. Seleccione **Guardar**.
Edite la regla	i. Seleccione la directiva propuesta y seleccione **Editar**. ii. Seleccione el icono de eliminar ✖ Para eliminar la regla incorrecta y seleccione **Guardar**. iii. Seleccione **ILM** > **Reglas**. iv. Seleccione la regla incorrecta y seleccione **Editar**. v. Cambie la información incorrecta y seleccione **Guardar**. vi. Seleccione **ILM** > **políticas**. vii. Seleccione la directiva propuesta y seleccione **Editar**. viii. Seleccione la regla corregida, seleccione **aplicar** y seleccione **Guardar**.

4. Vuelva a ejecutar la simulación.

> Dado que aleja de la página ILM Policies para editar la regla, los objetos que introdujo anteriormente para la simulación ya no se muestran. Debe volver a introducir los nombres de los objetos.

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.



Active la política de ILM

Después de añadir reglas de ILM a una política de ILM propuesta, simular la política y confirmar que se comporta como esperaba, está listo para activar la política propuesta.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Ha guardado y simulado la política de ILM propuesta.

> 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.

Acerca de esta tarea

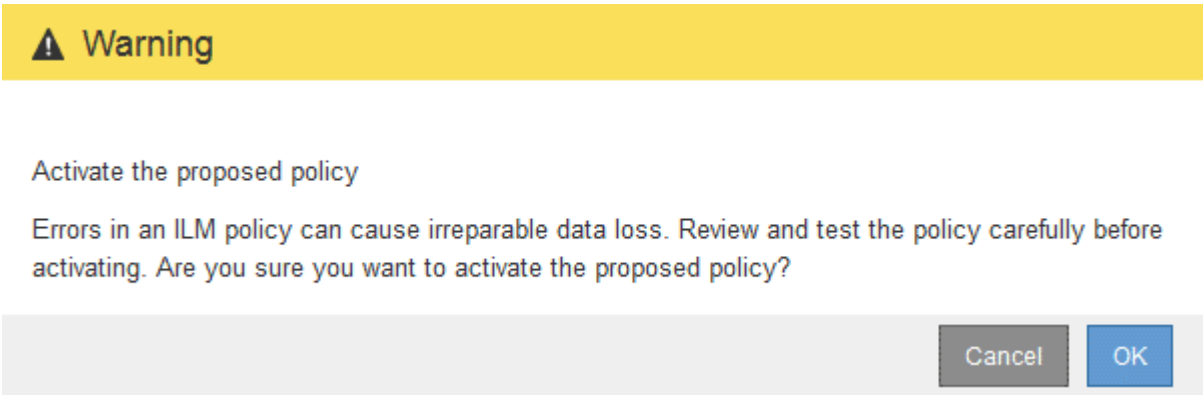
Cuando activa una política de ILM, el sistema distribuye la nueva política a todos los nodos. Sin embargo, es posible que la nueva directiva activa no surta efecto hasta que todos los nodos de grid estén disponibles para recibir la nueva directiva. En algunos casos, el sistema espera a implementar una nueva directiva activa para garantizar que los objetos de la cuadrícula no se eliminen accidentalmente.

- Si realiza cambios en las políticas que aumentan la redundancia o la durabilidad de los datos, estos cambios se implementan de inmediato. 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 en las políticas que podrían reducir la redundancia o la durabilidad de los datos, dichos cambios no se implementarán hasta que todos los nodos de grid estén disponibles. Por ejemplo, si activa una nueva directiva que utiliza una regla de dos copias en lugar de una regla de tres copias, la nueva directiva se marcará como "'activo'", pero no entrará en vigor hasta que todos los nodos estén en línea y disponibles.

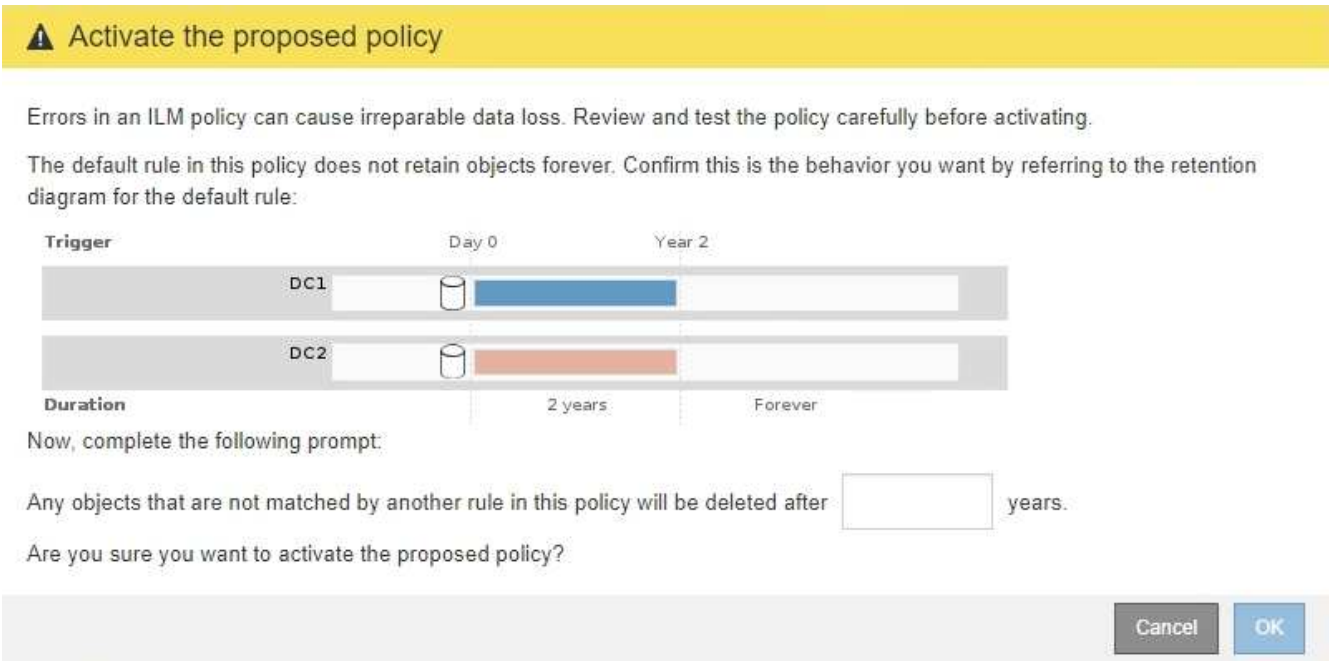
Pasos

1. Cuando esté listo para activar una directiva propuesta, seleccione la directiva en la página políticas de ILM y seleccione **Activar**.

   Aparecerá un mensaje de advertencia en el que se le pedirá que confirme que desea activar la directiva propuesta.



   Aparece un mensaje en el mensaje de advertencia si la regla predeterminada de la directiva no conserva objetos para siempre. En este ejemplo, el diagrama de retención muestra que la regla predeterminada eliminará objetos después de 2 años. Debe escribir **2** en el cuadro de texto para reconocer que cualquier objeto que no coincida con otra regla de la política se eliminará de StorageGRID después de 2 años.



2. Seleccione **OK**.

Resultado

Cuando se activa una nueva política de ILM:

- La política se muestra con un estado de política activo en la tabla de la página ILM Policies. La entrada Fecha de inicio indica la fecha y la hora en que se activó la directiva.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy | Clone | Edit | Remove

	Policy Name	Policy State	Start Date	End Date
◉	New Policy	Active	2017-07-20 18:49:53 MDT	
○	Baseline 2 Copies Policy	Historical	2017-07-19 21:24:30 MDT	2017-07-20 18:49:53 MDT

- La directiva anteriormente activa se muestra con un estado de directiva histórico. Las entradas Fecha de inicio y Fecha de finalización indican cuándo se ha activado la directiva y cuándo ha dejado de estar en vigor.

Información relacionada

Ejemplo 6: Cambiar una política de ILM

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.

Lo que necesitará

- 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 el ID de objeto (UUID), el nombre del objeto, el nombre del contenedor, el ID o el nombre de la cuenta de inquilino, el tamaño lógico del objeto, la fecha y hora en que se creó el objeto por primera vez, y la fecha y hora en que se modificó por última vez el objeto.
   - Todos los pares de valor de clave de metadatos de usuario personalizados asociados con el objeto.
   - Para los objetos S3, cualquier par de etiqueta de objeto clave-valor asociado al objeto.
   - Para las copias de objetos replicadas, la ubicación de almacenamiento actual de cada copia.
   - Para las copias de objetos codificados de borrado, la ubicación actual de almacenamiento de cada fragmento.
   - Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluido el nombre del bloque externo y el identificador único del objeto.
   - Para objetos segmentados y objetos multipartes, una lista de segmentos de objetos que incluyen identificadores de segmentos y tamaños de datos. Para objetos con más de 100 segmentos, sólo se muestran los primeros 100 segmentos.
   - Todos los metadatos del objeto en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen los metadatos internos del sistema que no se garantiza que continúen del lanzamiento al lanzamiento.

     En el ejemplo siguiente se muestran los resultados de búsqueda de metadatos de objetos para un objeto de prueba S3 almacenado como dos copias replicadas.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "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 de ORLM puede proporcionarle más información sobre el estado del proceso de evaluación de ILM, pero no puede proporcionarle información sobre la corrección de la ubicación de los datos del objeto ni sobre 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 S3
- Use Swift

Trabaje con las reglas de ILM y las políticas de ILM

Una vez creadas las reglas de ILM y una política de ILM, puede seguir trabajando con

ellas, modificando su configuración a medida que cambian sus requisitos de almacenamiento.

Lo que necesitará

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

Elimine una regla de ILM

Para que la lista de reglas de ILM actuales pueda ser manejable, elimine las reglas de ILM que no pueda usar.

No puede eliminar una regla de ILM si actualmente se encuentra en uso en la política activa o en la política propuesta. Si necesita eliminar una regla de ILM que utilice una política, primero debe realizar estos pasos:

1. Clone la política activa o edite la política propuesta.
2. Quite la regla de ILM de la política.
3. Guarde, simule y active la nueva directiva para asegurarse de que los objetos están protegidos como se espera.

Pasos

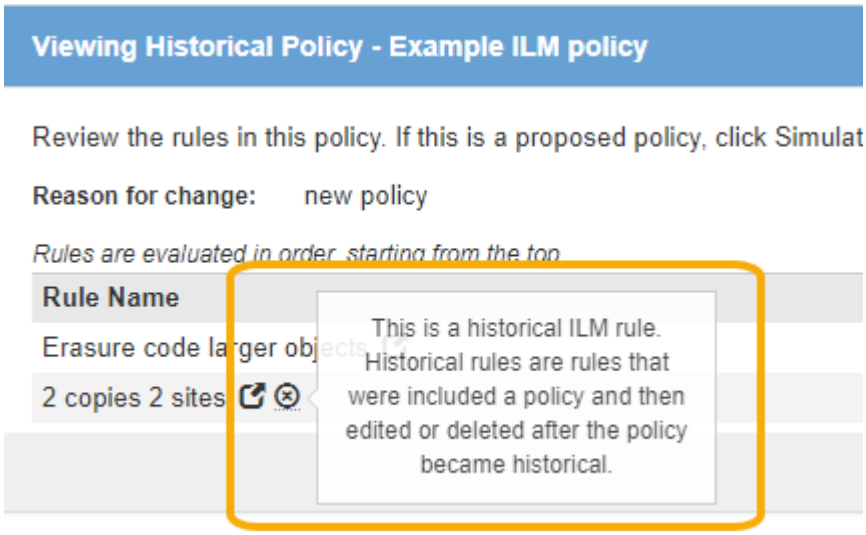
1. Seleccione **ILM** > **Reglas**.
2. Revise la entrada de tabla de la regla que desea quitar.

   Confirme que la regla no se utiliza en la política de ILM activa o en la política de ILM propuesta.

3. Si la regla que desea eliminar no está en uso, seleccione el botón de opción y seleccione **Quitar**.
4. Seleccione **Aceptar** para confirmar que desea eliminar la regla ILM.

   La regla de ILM se elimina.

Si elimina una regla que se utiliza en una política histórica, a. ⊗ aparece un icono para la regla cuando se visualiza la política, lo que indica que la regla se ha convertido en una regla histórica.



Editar una regla de ILM

Es posible que deba editar una regla de ILM para cambiar un filtro o una instrucción de ubicación.

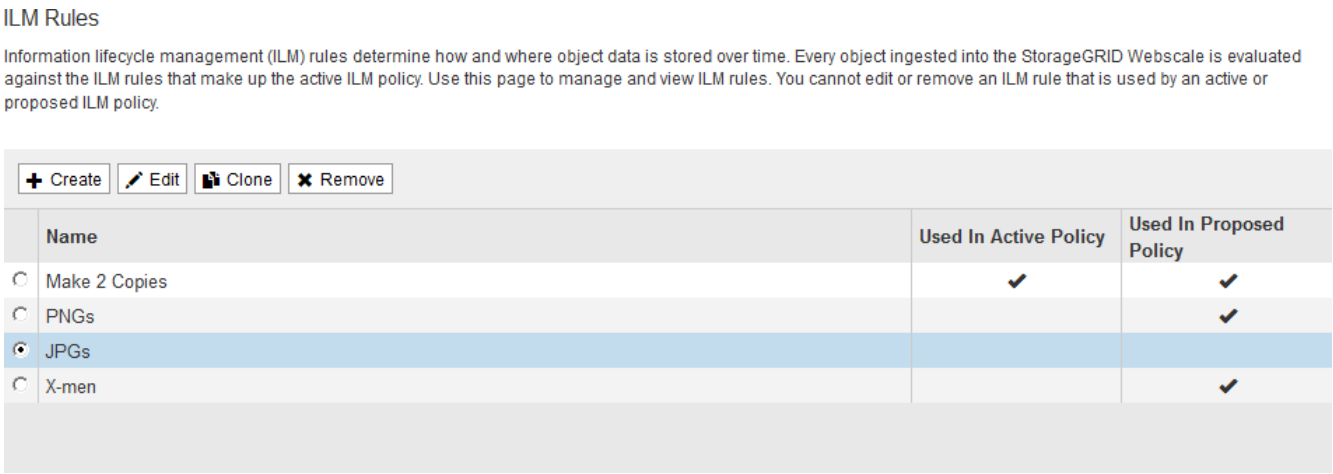
No se puede editar una regla si se está utilizando en la política de ILM propuesta o en la política de ILM activa. En su lugar, puede clonar estas reglas y hacer los cambios necesarios en la copia clonada. Tampoco puede editar la regla de gestión del ciclo de vida de la información (hacer 2 copias) o las reglas de gestión del ciclo de vida de la información creadas antes de la versión 10.3 de StorageGRID.

> Antes de agregar una regla editada a la política de ILM activa, tenga en cuenta que un cambio en las instrucciones de ubicación de un objeto puede provocar un aumento de la carga en el sistema.

Pasos

1. Seleccione **ILM** > **Reglas**.

   Aparece la página ILM Rules. Esta página muestra todas las reglas disponibles e indica qué reglas se están utilizando en la directiva activa o en la directiva propuesta.

2. Seleccione una regla que no se esté utilizando y seleccione **Editar**.

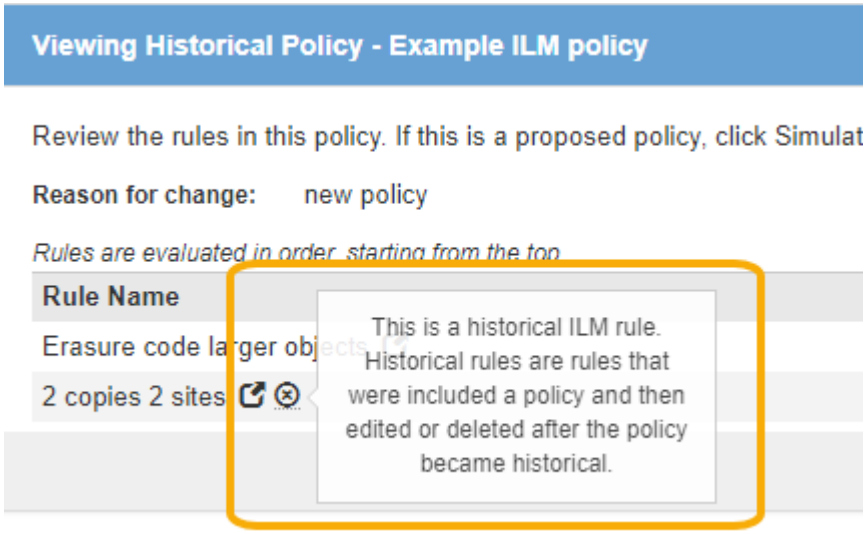
   Se abrirá el asistente Editar regla de ILM.

3. Complete las páginas del asistente Edit ILM Rule, siguiendo los pasos de Creación de una regla de ILM y.. uso de filtros avanzados, según sea necesario.

Al editar una regla de ILM, no puede cambiar su nombre.

4. Seleccione **Guardar**.

Si edita una regla que se utiliza en una política histórica, una aparece un icono para la regla cuando se visualiza la política, lo que indica que la regla se ha convertido en una regla histórica.



Clonar una regla de ILM

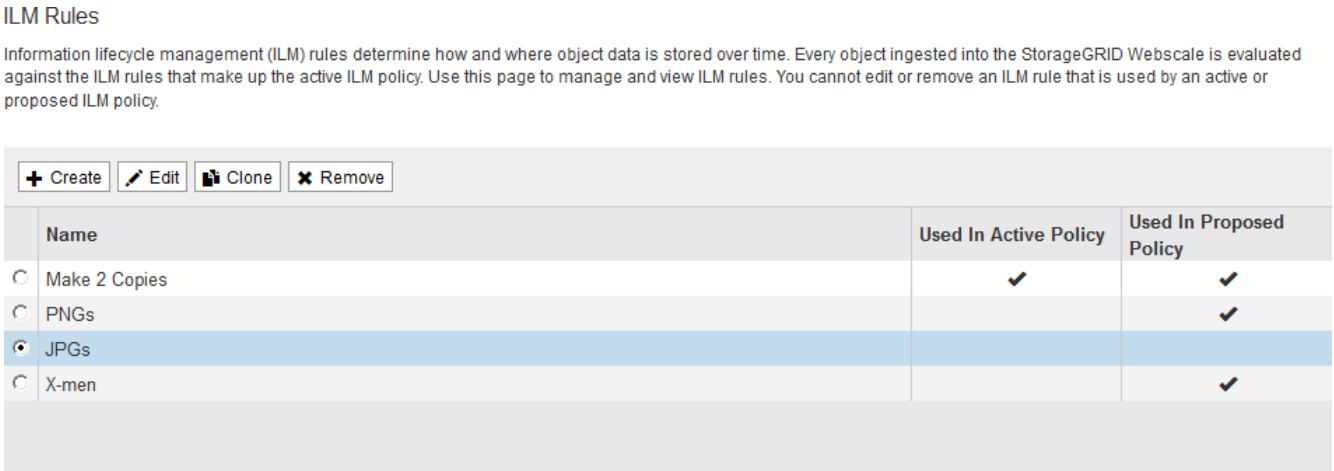
No se puede editar una regla si se está utilizando en la política de ILM propuesta o en la política de ILM activa. En su lugar, puede clonar una regla y hacer los cambios necesarios en la copia clonada. A continuación, si es necesario, puede eliminar la regla original de la directiva propuesta y sustituirla por la versión modificada. No puede clonar una regla de ILM si se creó con StorageGRID versión 10.2 o anterior.

Antes de añadir una regla clonada a la política de ILM activa, tenga en cuenta que un cambio en las instrucciones de ubicación de un objeto puede provocar un aumento de la carga en el sistema.

Pasos

1. Seleccione **ILM** > **Reglas**.

   Aparece la página ILM Rules.



2. Seleccione la regla ILM que desea clonar y seleccione **Clonar**.

   Se abrirá el asistente Crear regla de ILM.

3. Actualice la regla clonada siguiendo los pasos para editar una regla de ILM y usando filtros avanzados.

   Al clonar una regla de ILM, debe introducir un nombre nuevo.

4. Seleccione **Guardar**.

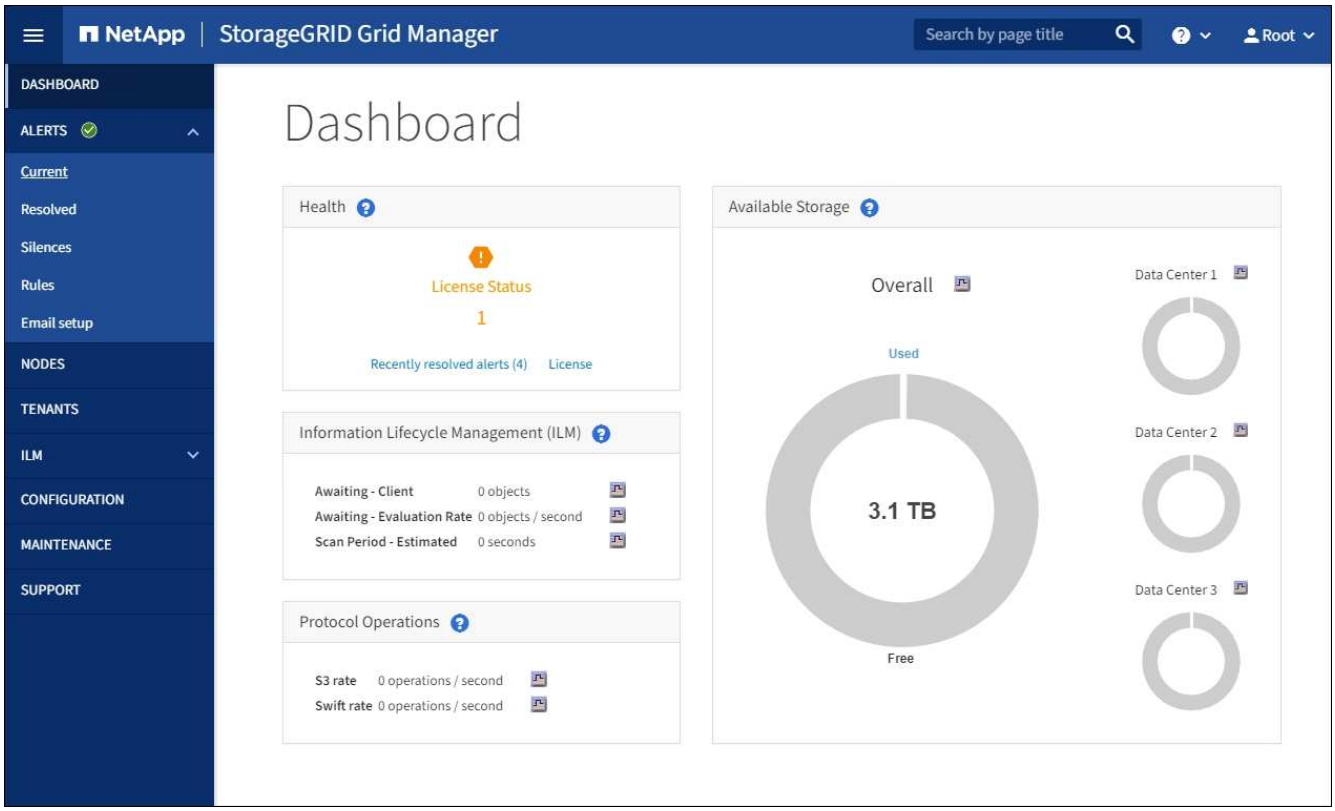
   Se crea la nueva regla de ILM.

Ver la cola de actividades de la política de ILM

Puede ver el número de objetos que hay en la cola que se van a evaluar en comparación con la política de ILM en cualquier momento. Puede ser conveniente supervisar la cola de procesamiento de ILM para determinar el rendimiento del sistema. Una cola grande puede indicar que el sistema no puede seguir el ritmo de la tasa de ingesta, la carga de las aplicaciones cliente es demasiado alta o que existe alguna condición anormal.

Pasos

1. Seleccione **Panel**.



2. Supervise la sección Information Lifecycle Management (ILM).

   Puede seleccionar el signo de interrogación ? para ver una descripción de los elementos de esta sección.

Utilice la bloqueo de objetos de S3 con ILM

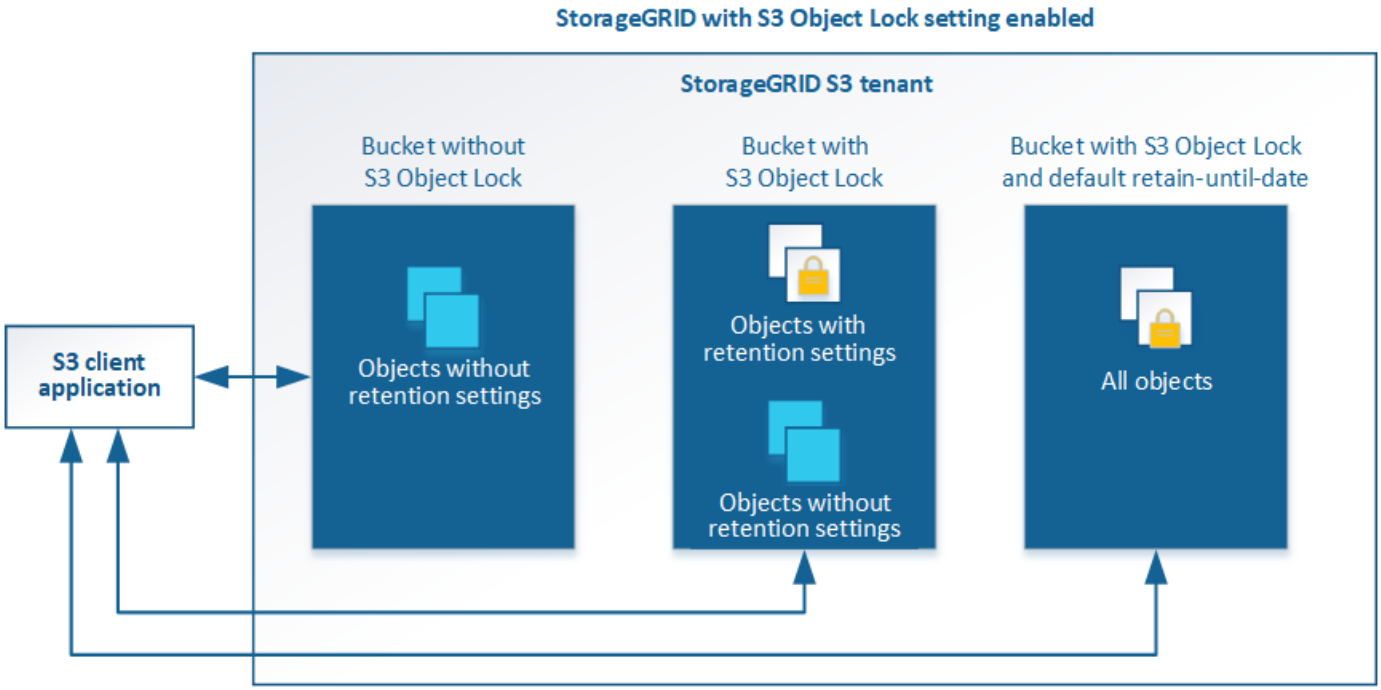
Gestione objetos con S3 Object Lock

Como administrador de grid, puede habilitar S3 Object Lock para el sistema StorageGRID e implementar una política de ILM compatible para ayudar a garantizar que los objetos de bloques S3 específicos no se eliminen ni se sobrescriban por un periodo 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 bloque tiene habilitada la función S3 Object Lock, las aplicaciones cliente S3 pueden especificar, opcionalmente, la configuración de retención para cualquier versión del objeto en ese bloque. Una versión de objeto debe tener la configuración de retención especificada para estar protegida por S3 Object Lock. Además, cada bloque con el bloqueo de objetos S3 habilitado puede tener, de manera opcional, un modo de retención y un período de retención predeterminados, lo que se aplica si se agregan objetos al bloque sin su propia configuración de retención.



La función de bloqueo de objetos StorageGRID S3 ofrece un único modo de retención equivalente al modo de cumplimiento de normativas Amazon S3. De forma predeterminada, cualquier usuario no puede sobrescribir ni eliminar una versión de objeto protegido. La función de bloqueo de objetos StorageGRID S3 no es compatible con un modo de gobierno y no permite a los usuarios con permisos especiales omitir la configuración de retención o eliminar objetos protegidos.

Si un bloque tiene habilitado el bloqueo de objetos S3, la aplicación cliente S3 puede especificar, de manera opcional, la siguiente configuración de retención a nivel de objeto al crear o actualizar un objeto:

- **Retener-hasta-fecha**: Si la fecha retener-hasta-fecha de una versión de objeto es en el futuro, el objeto puede ser recuperado, pero no puede ser modificado o eliminado. Según sea necesario, se puede aumentar la fecha de retención hasta de un objeto, pero esta fecha no se puede disminuir.
- **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.

Para obtener detalles sobre la configuración de retención de objetos, vaya a. Utilice el bloqueo de objetos de S3.

Para obtener más información acerca de la configuración de retención de bloque predeterminada, vaya a. Use la retención de bloque predeterminada de Object Lock de S3.

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 de bloqueo de objetos S3 cumple los requisitos de Amazon S3, deja obsoleto la función propia de cumplimiento de StorageGRID, que ahora se conoce como "'Legacy Compliance".

Si anteriormente habilitó la configuración de cumplimiento global, la opción global de bloqueo de objetos S3 se habilitó automáticamente. Los usuarios inquilinos ya no pueden crear nuevos bloques con el servicio de cumplimiento de normativas; sin embargo, según sea necesario, los usuarios inquilinos pueden seguir usando y gestionando cualquier parte existente compatible, lo que incluye realizar las siguientes tareas:

- Incorporación de objetos nuevos en un bloque existente con cumplimiento de normativas heredado habilitado.
- Aumento del período de retención de un bloque existente que tiene activada la normativa heredada.
- Cambio de la configuración de eliminación automática para un bloque existente que tiene activada la conformidad heredada.
- Colocar una retención legal en un bloque existente que tenga activada la conformidad heredada.
- Levantar una retención legal.

Consulte "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5" si desea obtener instrucciones.

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.

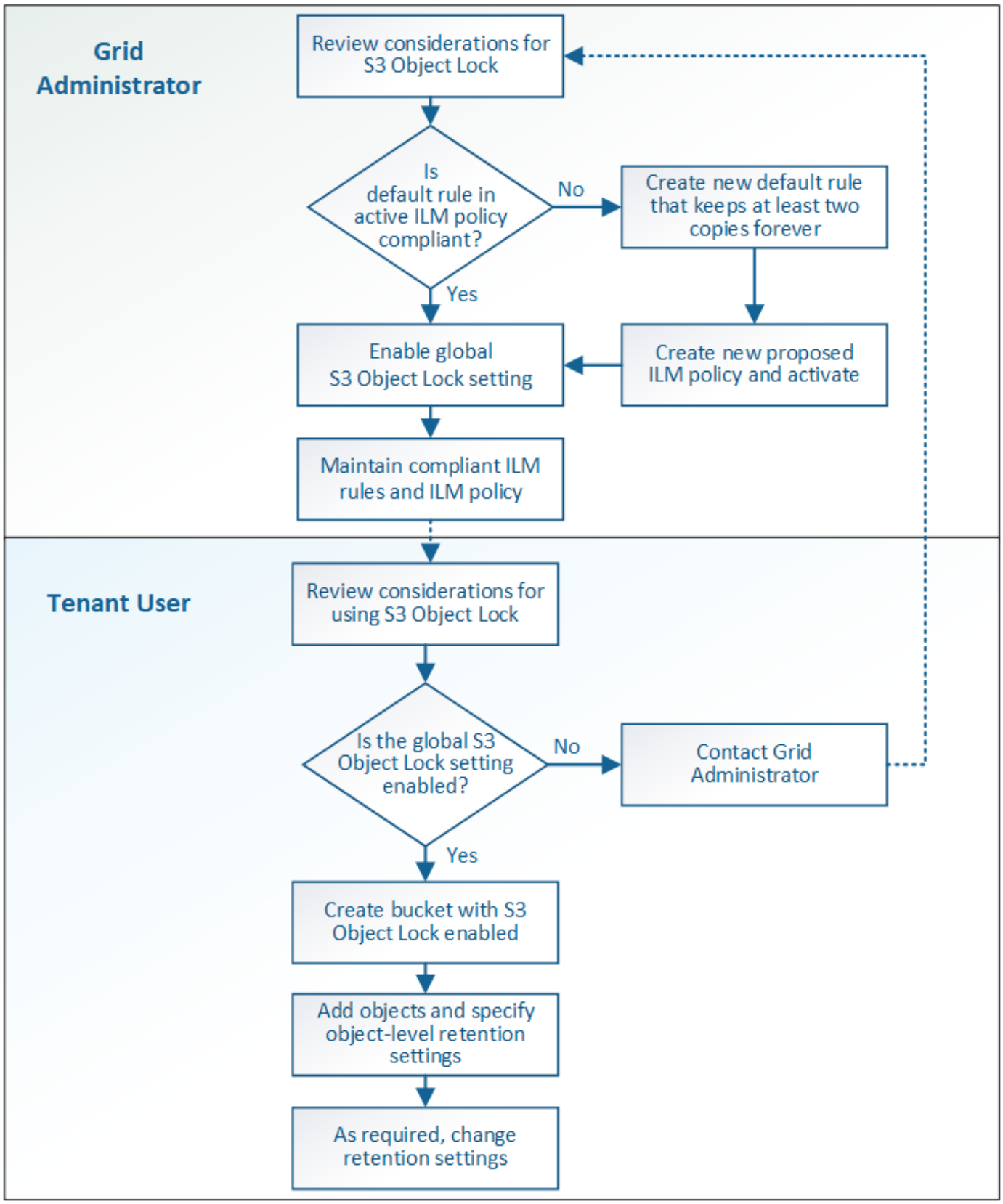
	Bloqueo de objetos de S3 (nuevo)	Cumplimiento (heredado)
¿Cómo se habilita la función a nivel global?	En Grid Manager, seleccione **CONFIGURACIÓN** > **sistema** > **S3 Object Lock**.	Ya no es compatible. **Nota:** Si ha activado la configuración de cumplimiento global con una versión anterior de StorageGRID, la configuración de bloqueo de objetos S3 está activada en StorageGRID 11.6. Puede seguir utilizando StorageGRID para gestionar la configuración de los bloques compatibles existentes; sin embargo, no puede crear nuevos bloques compatibles.
¿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.	Los usuarios ya no pueden crear nuevos bloques con el cumplimiento habilitado; sin embargo, pueden continuar agregando objetos nuevos a bloques compatibles existentes.
¿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 La función de cumplimiento heredado no permite el control de versiones de bloques.
¿Cómo se establece la retención de objetos?	Los usuarios pueden establecer una fecha de retención hasta cada versión de objeto.	Los usuarios deben establecer un período de retención para todo el segmento. El período de retención se aplica a todos los objetos del bloque.
¿Puede un bloque tener la configuración predeterminada para la retención y la retención legal?	Sí. Los bloques StorageGRID que tienen el bloqueo de objetos S3 habilitado pueden tener un período de retención predeterminado que se aplica a las versiones de objetos que no tienen su propia configuración de retención especificada durante el procesamiento.	Sí
¿Se puede cambiar el período de retención?	La fecha de retención hasta la versión de un objeto se puede aumentar pero nunca disminuir.	El período de retención del cucharón se puede aumentar pero nunca disminuir.

	Bloqueo de objetos de S3 (nuevo)	Cumplimiento (heredado)
¿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?	Una versión de objeto se puede eliminar después de alcanzar la fecha de retención hasta la fecha, suponiendo que el objeto no esté en espera 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 que cumpla las normativas y convierta esa regla en la regla predeterminada en la 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. Especifique la configuración de retención predeterminada para el bloque, que se aplica a los objetos agregados al bloque que no especifican sus propias configuraciones de retención.
3. Agregue objetos a esos bloques y especifique los períodos de retención a nivel de objeto y la configuración de retención legal.
4. Según sea necesario, actualice un período de retención o cambie la configuración de retención legal de un objeto individual.

Información relacionada

- Usar una cuenta de inquilino
- Use S3
- Use la retención de bloque predeterminada de Object Lock de S3

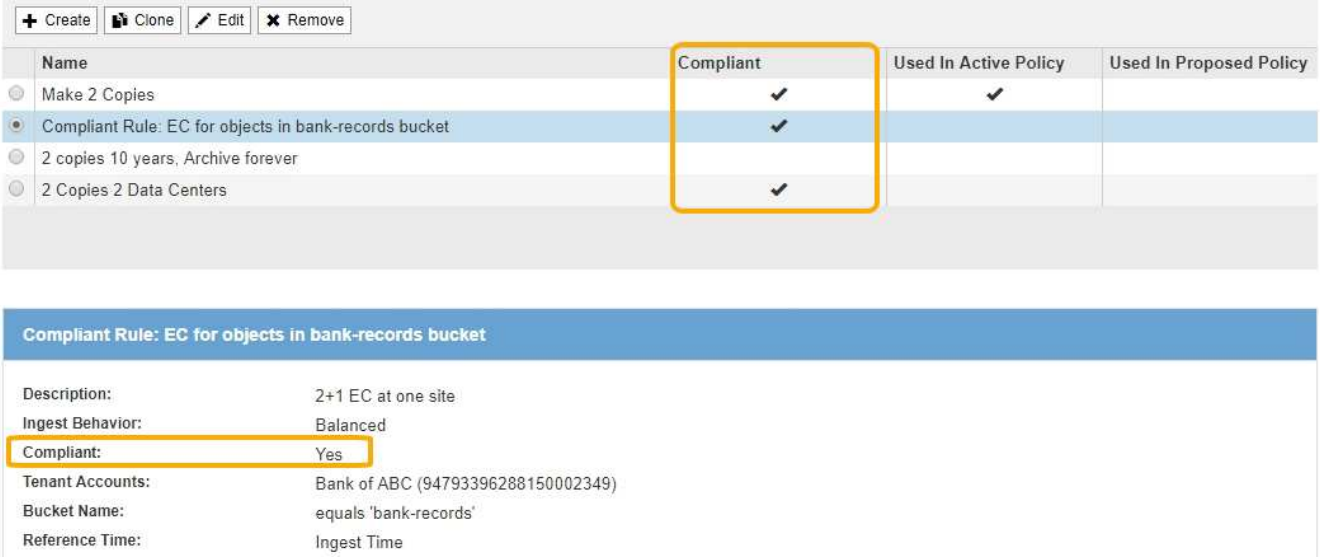
Requisitos para el bloqueo de objetos de S3

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 de bloqueo de objetos S3, no se puede deshabilitar esa opción.
- No puede habilitar el bloqueo de objetos global de S3 a menos que la regla predeterminada de la política de ILM activa sea *conforme a* (es decir, la regla predeterminada debe cumplir con los requisitos de los bloques con el bloqueo de objetos S3 habilitado).
- Cuando la configuración de bloqueo de objetos global de S3 está habilitada, no se puede crear una nueva política de ILM propuesta ni activar una política de ILM propuesta existente, a menos que la regla predeterminada de la política sea conforme con la normativa. Una vez habilitada la configuración global de bloqueo de objetos de S3, las páginas de reglas de ILM y políticas de ILM indican qué reglas de ILM son compatibles.

  En el siguiente ejemplo, la página de reglas de ILM enumera tres reglas que cumplen con los bloques con el bloqueo de objetos S3 habilitado.

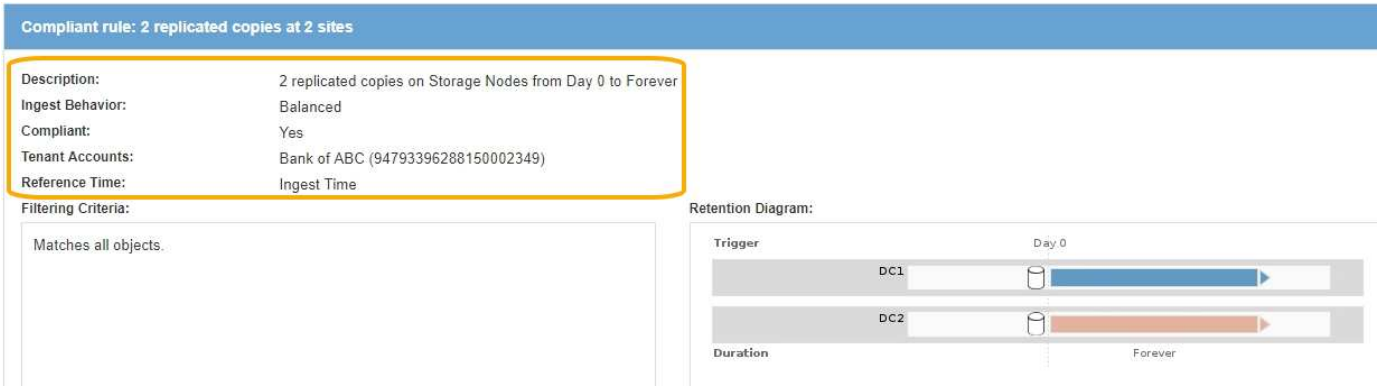


Requisitos para las reglas de ILM que cumplen con las normativas

Si desea habilitar la configuración global de bloqueo de objetos S3, debe asegurarse de que la regla predeterminada de la política de ILM activa 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 cloud.
- 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 procesamiento** como tiempo de referencia.
- Al menos una línea de las instrucciones de colocación deberá ser «'para siempre».

Por ejemplo, esta regla satisface los requisitos de los bloques con el bloqueo de objetos S3 habilitado. Almacena dos copias de objetos replicados del tiempo de procesamiento (día 0) al estado «'eternamente». Los objetos se almacenarán en nodos de almacenamiento en dos centros de datos.



Requisitos para políticas de ILM activas y propuestas

Cuando se habilita la configuración global de bloqueo de objetos S3, las políticas de ILM activas y propuestas pueden incluir reglas tanto conformes a la normativa como no.

- La regla predeterminada de la política de ILM activa o propuesta debe ser conforme.
- Las reglas no compatibles solo se aplican a los objetos en bloques que no tienen habilitada el bloqueo de objetos S3 o que no tienen habilitada la función de cumplimiento 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.

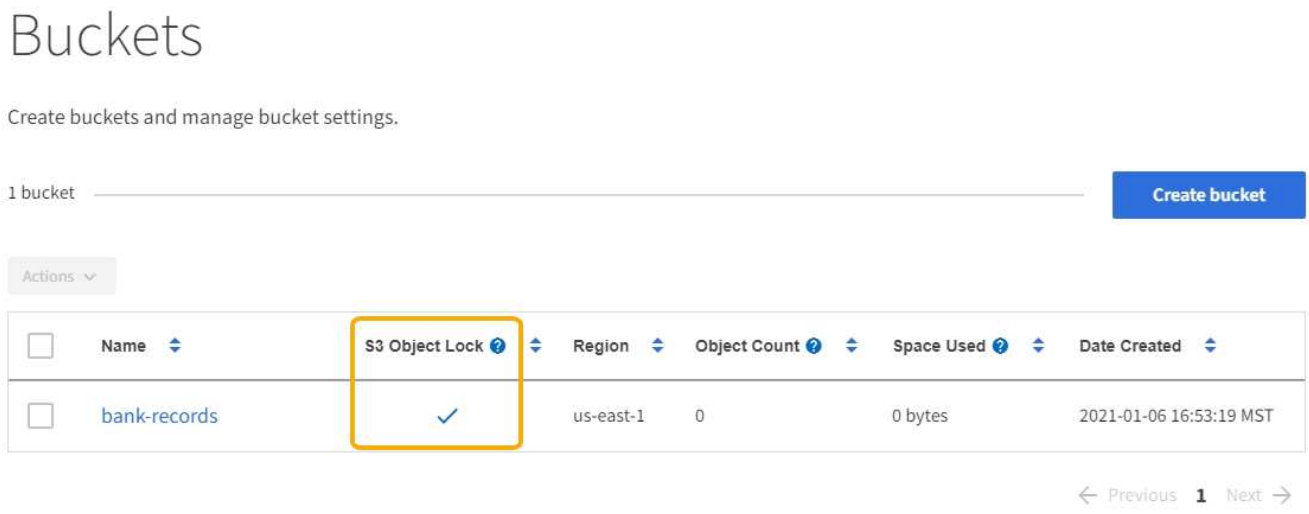
Una política de ILM compatible puede incluir estas tres reglas:

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 bloques que no tienen habilitado el bloqueo de objetos S3 o el cumplimiento heredado, ya que solo almacena una 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.

  Este ejemplo del Administrador de inquilinos muestra un bloque 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 es posible habilitar el bloqueo de objetos de S3 para un bloque existente.
- Se requiere el versionado de bloques con S3 Object Lock. Cuando se habilita el bloqueo de objetos S3 para un bloque, StorageGRID habilita automáticamente el control de versiones para ese bloque.

- Después de crear un bloque con el bloqueo de objetos S3 habilitado, no se puede deshabilitar el bloqueo de objetos S3 ni suspender el control de versiones de ese bloque.
- Si lo desea, puede configurar la retención predeterminada para un bloque. Cuando se carga una versión de objeto, la retención predeterminada se aplica a la versión del objeto. Puede anular el valor predeterminado de bloque especificando un modo de retención y retener hasta la fecha en la solicitud para cargar una versión de objeto.
- Se admite la configuración del ciclo de vida de bloques para los bloques del ciclo de vida de objetos S3.
- 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, la aplicación cliente S3 debe configurar la retención predeterminada de bloques o especificar la configuración de retención en cada solicitud de carga.
- Puede aumentar la fecha de retención hasta una versión de objeto, pero nunca puede disminuir este valor.
- Si recibe una notificación de una acción legal pendiente o una investigación normativa, puede conservar la información relevante colocando una retención legal en una versión del objeto. Cuando una versión de objeto se encuentra bajo una retención legal, ese objeto no se puede eliminar de StorageGRID, aunque haya alcanzado su fecha de retención. Tan pronto como se levante la retención legal, la versión del objeto se puede eliminar si se ha alcanzado la fecha de retención.
- El bloqueo de objetos de S3 requiere el uso de bloques con versiones. 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 bloque con el bloqueo de objetos S3 habilitado atraviesa tres etapas:

1. **Procesamiento de objetos**
   - Cuando se añade una versión de objeto a un bloque con S3 Object Lock habilitado, la aplicación cliente S3 puede usar la configuración de retención de bloque predeterminada o especificar, opcionalmente, la configuración de retención para el objeto (retenga hasta la fecha, la conservación legal o ambos). A continuación, StorageGRID genera metadatos para ese objeto, que incluye un identificador de objeto (UUID) único y la fecha y la hora de procesamiento.
   - Después de procesar una versión de objeto con configuración de retención, sus datos y los metadatos definidos por el usuario de S3 no se pueden modificar.
   - StorageGRID almacena los metadatos del objeto de forma independiente de los datos del objeto. Mantiene tres copias de todos los metadatos de objetos en cada sitio.
2. **Retención de objetos**
   - StorageGRID almacena varias copias del objeto. El número y el tipo exactos de copias y las ubicaciones del almacenamiento se determinan según las reglas conformes de la política de ILM activa.
3. **Eliminación de objetos**
   - Un objeto se puede eliminar cuando se alcanza su fecha de retención.
   - No se puede eliminar un objeto que se encuentra bajo una retención legal.

Información relacionada

- Usar una cuenta de inquilino
- Use S3
- Comparación del bloqueo de objetos de S3 con el cumplimiento de normativas heredado
- Ejemplo 7: Política de ILM conforme con la normativa para el bloqueo de objetos S3
- Revisar los registros de auditoría
- Use la retención de bloque predeterminada de Object Lock de 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.

Lo que necesitará

- Tiene el permiso 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 debe comprender estas consideraciones.
- La regla predeterminada de la política de ILM activa es compatible.
  - Cree una regla de ILM predeterminada
  - Cree una política de ILM

Acerca de esta tarea

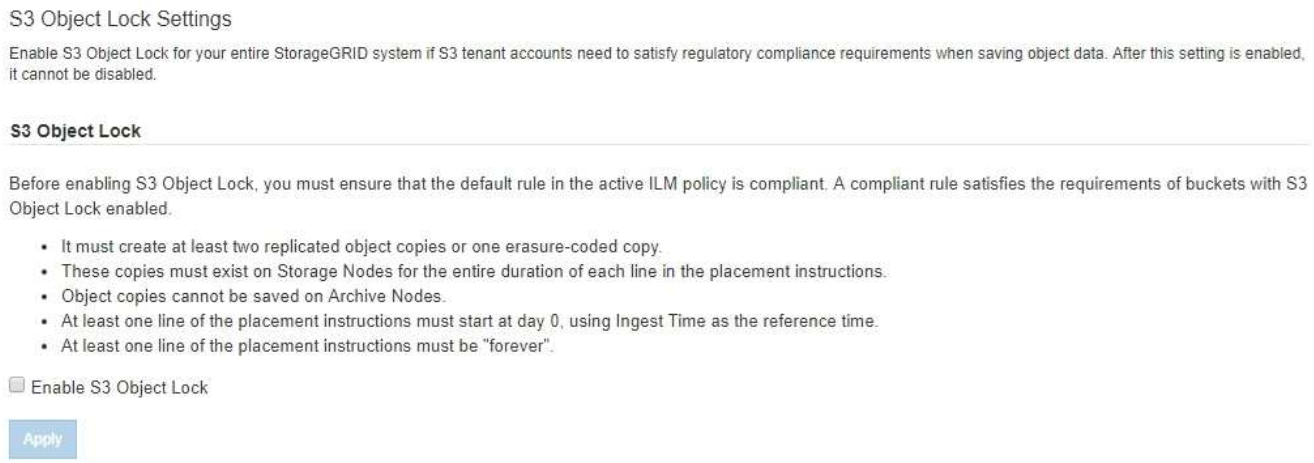
Un administrador de grid debe habilitar la configuración global de bloqueo de objetos S3 para permitir a los usuarios inquilinos crear nuevos bloques con el bloqueo de objetos S3 habilitado. Una vez que este ajuste está activado, no se puede desactivar.

> Si habilitó la opción de cumplimiento global mediante una versión anterior de StorageGRID, la opción de bloqueo de objetos S3 se habilita en StorageGRID 11.6. Puede seguir utilizando StorageGRID para gestionar la configuración de los bloques compatibles existentes; sin embargo, no puede crear nuevos bloques compatibles. Consulte "Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5".

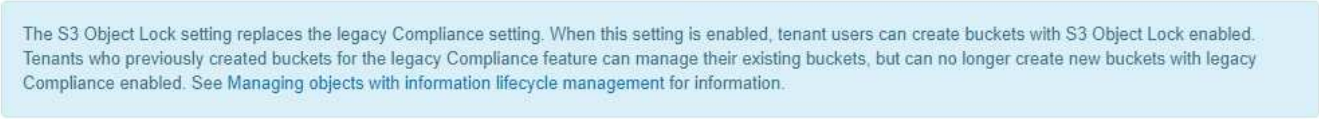
Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **S3 Object Lock**.

   Se muestra la página S3 Object Lock Settings.



Si ha habilitado la configuración de cumplimiento global con una versión anterior de StorageGRID, la página incluye la siguiente nota:



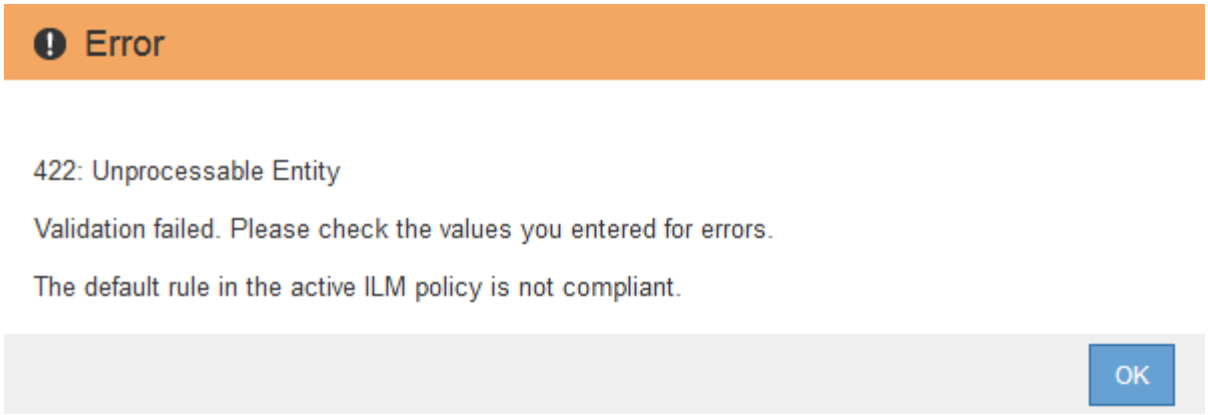
2. Seleccione **Activar el bloqueo de objetos S3**.
3. Seleccione **aplicar**.

   Aparece un cuadro de diálogo de confirmación que le recuerda que no puede deshabilitar el bloqueo de objetos S3 después de estar activado.

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, el bloqueo de objetos S3 ahora está habilitado para toda la cuadrícula y no puede deshabilitarse.
   - Si la regla predeterminada no es compatible, aparece un error que indica que debe crear y activar una nueva política de ILM que incluya una regla de cumplimiento como regla predeterminada. Seleccione **Aceptar**, cree una nueva directiva propuesta, simule y actívela.



Después de terminar

Después de habilitar la configuración global de bloqueo de objetos S3, es posible que deba hacerlo cree una regla predeterminada eso es compatible y. Cree una política de ILM eso es conforme. Una vez activada la configuración, la política de ILM puede incluir de manera opcional una regla predeterminada que cumpla las normativas y una regla predeterminada que no sea compatible. Por ejemplo, puede que desee usar una regla no conforme a la normativa que no tenga filtros para los objetos de los bloques que no tengan habilitado el bloqueo de objetos S3.

Información relacionada

- Compare el bloqueo de objetos de S3 con el cumplimiento de normativas heredado

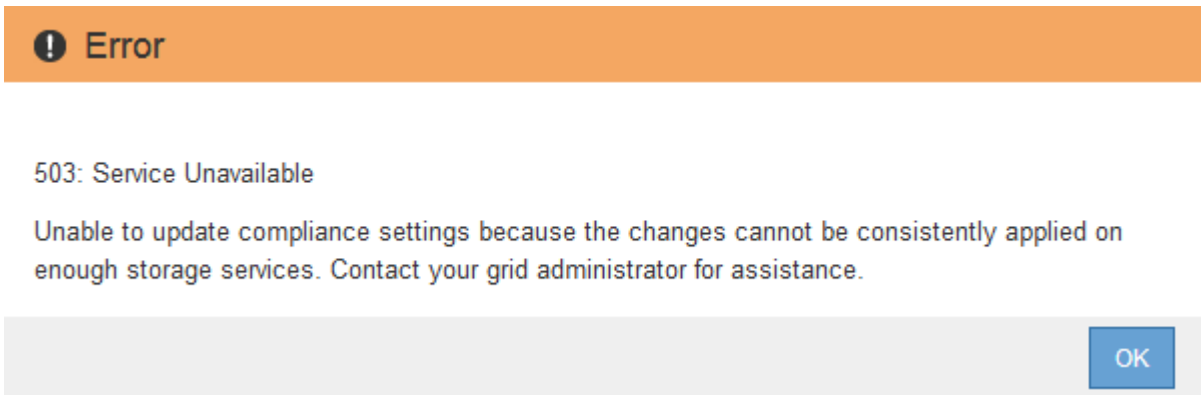
Resuelva los errores de coherencia al actualizar la configuración de bloqueo de objetos de S3 o cumplimiento heredado

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 debido a que un sitio de centro de datos o varios nodos de almacenamiento no están disponibles, se muestra un mensaje de error. Específicamente:

- Los usuarios de tenant Manager ven el siguiente mensaje de error:



- Los usuarios de la API de gestión de inquilinos y los usuarios de la API S3 reciben un código de respuesta de `503 Service Unavailable` con texto de mensaje similar.

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 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 directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

Regla 1 de ILM, por ejemplo 1: Copiar datos de objetos en dos centros de datos

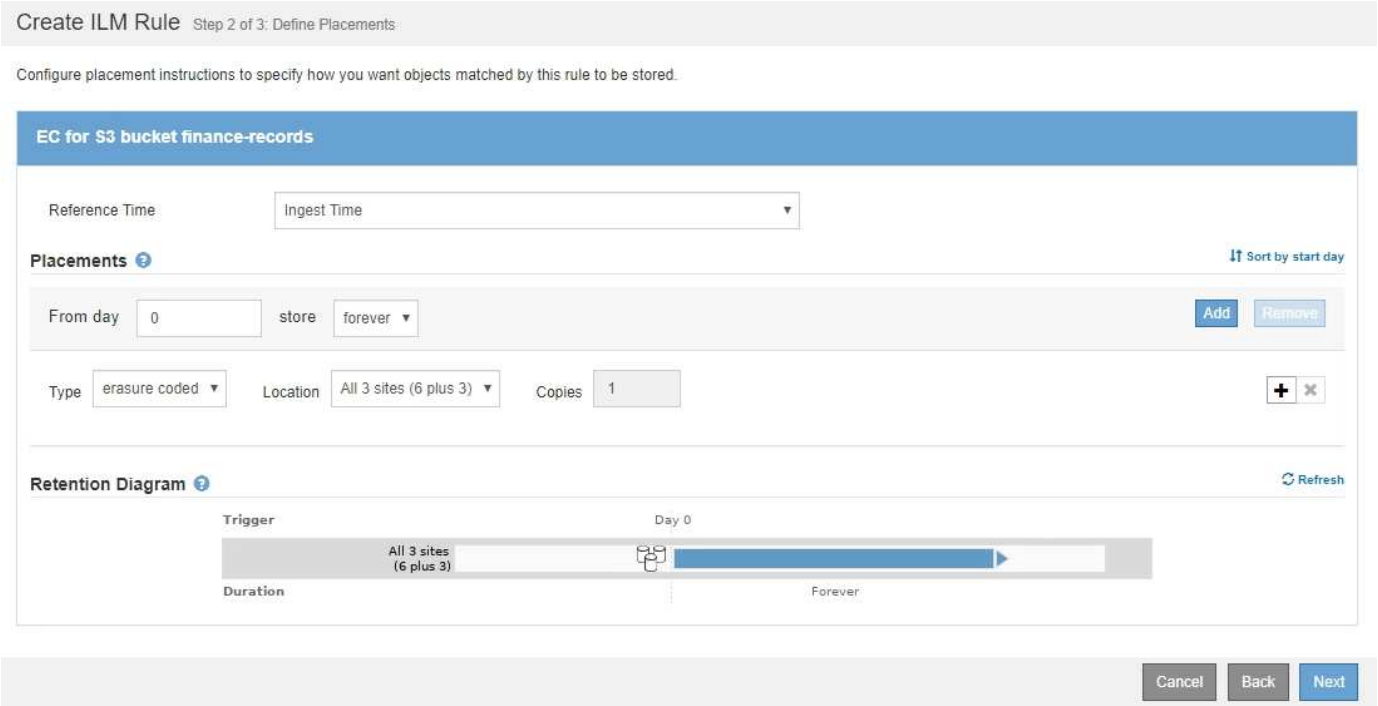
Esta regla de ILM de ejemplo copia los datos de objetos en dos pools de almacenamiento en dos centros de datos.

Definición de regla	Valor de ejemplo
Pools de almacenamiento	Dos pools de almacenamiento, cada uno en centros de datos diferentes, llamados Storage Pool DC1 y Storage Pool DC2.
Nombre de regla	Dos copias dos centros de datos
Tiempo de referencia	Tiempo de ingesta
Colocación del contenido	El día 0, mantenga dos copias replicadas para siempre: Una en el DC1 del pool de almacenamiento y otra en el DC2 del pool de almacenamiento.

Regla 2 de ILM por ejemplo 1: Perfil de código de borrado con coincidencia de bloques

Esta regla de ILM de ejemplo 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
Perfil de código de borrado	• Un único pool de almacenamiento en tres centros de datos (los 3 sitios) • Utilice un esquema de codificación de borrado de 6+3
Nombre de regla	EC para registros financieros de bloques de S3
Tiempo de referencia	Tiempo de ingesta
Colocación del contenido	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

El sistema StorageGRID permite diseñar políticas de ILM sofisticadas y complejas; sin embargo, en la práctica, la mayoría de las políticas de ILM son simples.

Una política de ILM típica de una topología de varios sitios puede incluir reglas de ILM como las siguientes:

- Durante la ingesta, use la codificación de borrado 6+3 para almacenar todos los objetos que pertenecen al bloque de S3 denominado `finance-records` en tres centros de datos.
- Si un objeto no coincide con la primera regla de ILM, utilice la regla de ILM predeterminada de la política, dos copias de dos centros de datos, para almacenar una copia de ese objeto en dos centros de datos,

DC1 y DC2.

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 directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

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 utilice la codificación de borrado para objetos de menos de 200 KB con el fin de evitar la sobrecarga de gestión de fragmentos codificados con borrado de muy pequeño tamaño.

Definición de regla	Valor de ejemplo
Nombre de regla	Sólo objetos de EC > 1 MB
Tiempo de referencia	Tiempo de ingesta
Filtrado avanzado para el tamaño del objeto	Tamaño de objeto (MB) mayor que 1
Colocación del contenido	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
Filtrado avanzado para el tamaño del objeto	Ninguno
Colocación del contenido	Cree dos copias replicadas y guárdelas en dos centros de datos, DC1 y DC2

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 a fin de garantizar que las imágenes mayores de 1 MB estén codificadas para el borrado y que haya dos copias 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 directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

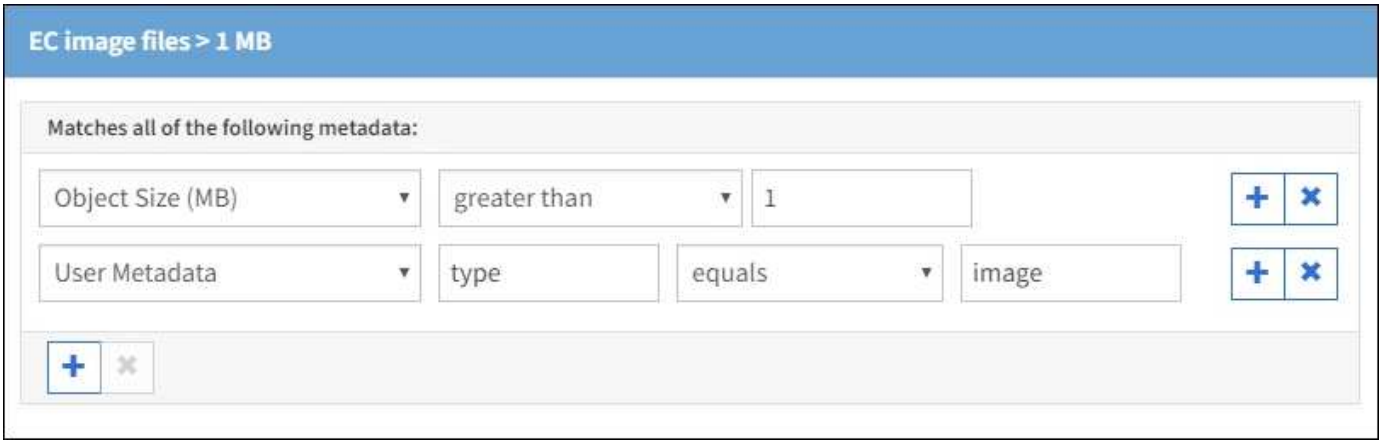
Regla ILM 1 por ejemplo 3: Utilice EC para archivos de imagen superiores a 1 MB

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 utilice la codificación de borrado para objetos de menos de 200 KB con el fin de evitar la sobrecarga de gestión de fragmentos codificados con borrado de muy pequeño tamaño.

Definición de regla	Valor de ejemplo
Nombre de regla	Archivos de imagen EC > 1 MB
Tiempo de referencia	Tiempo de ingesta
Filtrado avanzado para el tamaño del objeto	Tamaño de objeto (MB) mayor que 1.0

Definición de regla	Valor de ejemplo
Filtrado avanzado para metadatos de usuario	El tipo de metadatos de usuario es igual a la imagen
Colocación del contenido	Cree una copia codificada con borrado al 2+1 mediante tres ubicaciones



Dado que esta regla se configura como la primera regla de la política, la instrucción de colocación de codificación de borrado sólo se aplica a las imágenes que son superiores a 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
Filtrado avanzado para metadatos de usuario	El tipo de metadatos de usuario equivale a los archivos de imagen
Colocación del contenido	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 bloque de S3 con el control de versiones activado, puede gestionar las versiones de objetos no actuales incluyendo reglas en su política de ILM que utilicen **tiempo no corriente** como tiempo de referencia.

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 directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

> Si crea políticas de ILM para gestionar versiones de objetos no actuales, tenga en cuenta que debe conocer el UUID o el CBID de la versión del objeto para simular la política. Para buscar el UUID y el CBID de un objeto, utilice Búsqueda de metadatos de objetos mientras el objeto sigue estando actualizado. Consulte Comprobar una política de ILM con la búsqueda de metadatos de objetos.

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 centros de datos 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 en centros de datos diferentes, denominados DC1, DC2 y DC3.
Nombre de regla	Tres copias diez años
Tiempo de referencia	Tiempo de ingesta
Colocación del contenido	En el día 0, guarde tres copias replicadas durante 10 años (3,652 días), una en CD1, una en DC2 y una en CD3. 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

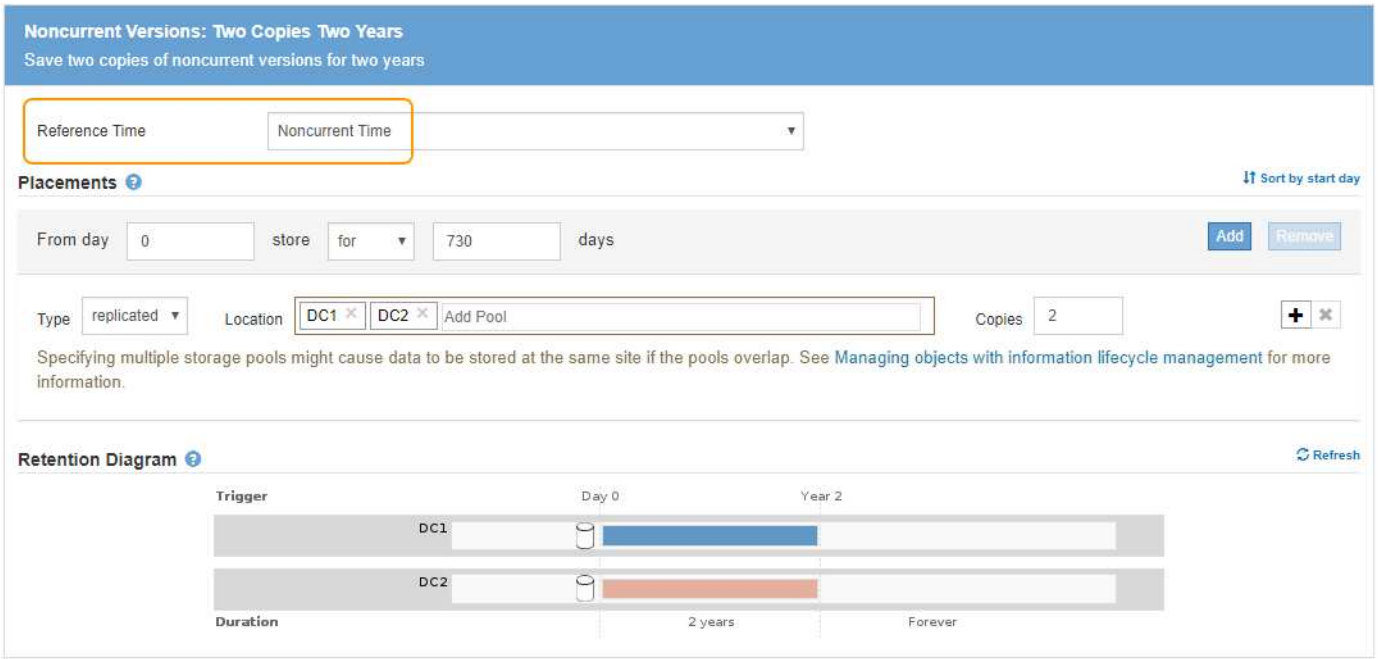
Esta regla de ILM de ejemplo almacena dos copias de las versiones no actuales de un objeto con versiones de S3 durante 2 años.

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. Esta regla utiliza la opción **tiempo no corriente** para tiempo de referencia.

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 centros de datos diferentes, denominados DC1 y DC2.
Nombre de regla	Versiones no corrientes: Dos copias dos años
Tiempo de referencia	Hora no actual
Colocación del contenido	El día 0 en relación con 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 de objeto no corrientes durante 2 años (730 días), una en DC1 y otra en DC2. 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 diferente a la versión actual, las reglas que utilizan **Hora no corriente** como Hora de referencia deben aparecer en la directiva ILM antes de las reglas que se aplican a la versión actual del objeto.

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 tiempo no corrientes deben aparecer en la directiva antes de las reglas que se aplican a la versión de objeto actual. De lo contrario, las versiones de objeto no actuales nunca serán coincidentes con la regla de tiempo no corriente.

- Cuando se procesa, cree tres copias replicadas y almacene una copia en cada uno de los tres centros de datos. 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).

> Para simular versiones de objeto no actuales, debe utilizar el UUID o CBID de esa versión. Mientras el objeto sigue siendo actual, puede utilizar Búsqueda de metadatos de objetos para buscar su UUID y CBID.

- La versión actual del objeto coincidiría con la segunda regla. Cuando la versión actual del objeto se ha almacenado durante 10 años, el proceso ILM agrega un marcador DELETE como la versión actual del objeto, y hace que la versión anterior del objeto "'no actual'". La próxima vez que se realice la evaluación de ILM, esta versión no actual coincide con la primera regla. Como resultado, la copia en DC3 se purga y las dos copias en DC1 y DC2 se almacenan durante dos 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 directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

Información relacionada

- Opciones de protección de datos para consumo
- Paso 3 de 3: Definir el comportamiento de la ingesta

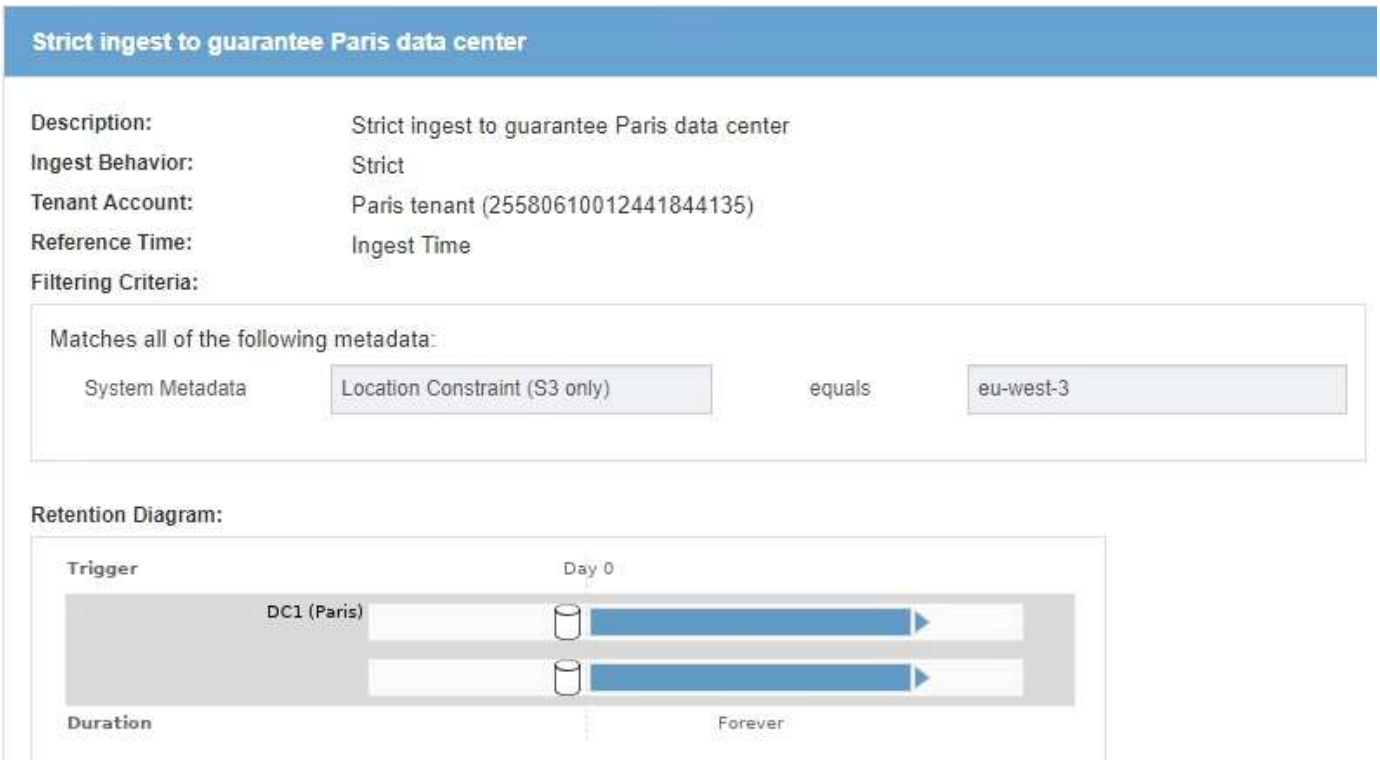
Regla 1 de ILM, por ejemplo 5: Ingesta estricta para garantizar el centro de datos de París

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

Definición de regla	Valor de ejemplo
Filtrado avanzado	La limitación de ubicación es igual a la ue-oeste-3
Pools de almacenamiento	CD1 (París)
Nombre de regla	Ingesta estricta para garantizar el centro de datos París
Tiempo de referencia	Tiempo de ingesta
Colocación del contenido	El día 0, conservar para siempre dos copias replicadas en DC1 (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 satisfacer 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.

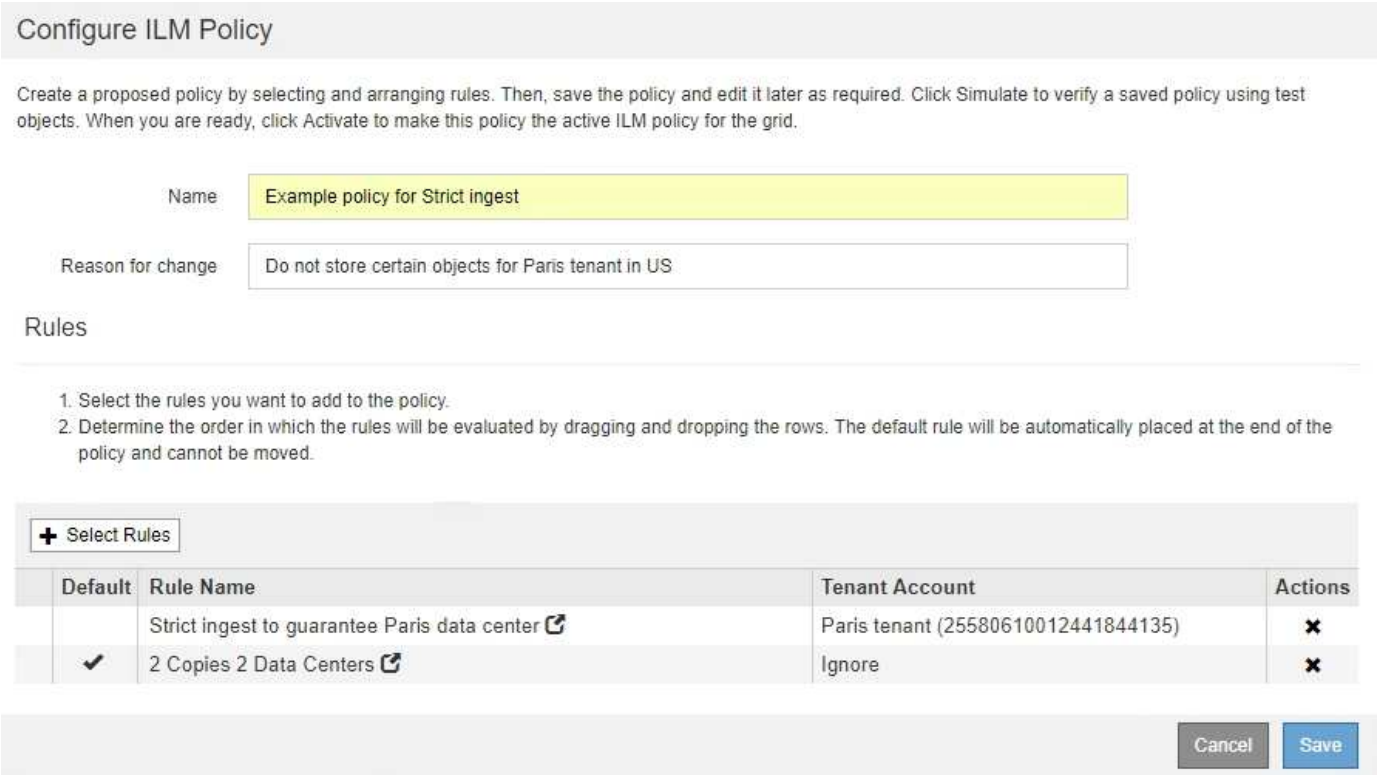
Definición de regla	Valor de ejemplo
Cuenta de inquilino	Ignorar
Filtrado avanzado	*No especificado*
Pools de almacenamiento	DC1 (París) y DC2 (EE. UU.)
Nombre de regla	2 copias 2 centros de datos
Tiempo de referencia	Tiempo de ingesta
Colocación del contenido	Desde el día 0, mantenga dos copias replicadas 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. Haga copias provisionales en cualquier ubicación disponible si no se puede cumplir la instrucción de colocación.



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 se comparan con la segunda regla, incluidos los objetos que pertenecen al inquilino de París y que no tienen la región de 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

Es posible que deba crear y activar una nueva política de ILM si sus necesidades de protección de datos cambian o si añade nuevos sitios.

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 añadido un nuevo sitio StorageGRID en una ampliación y se debe revisar la política activa de ILM para almacenar datos en el nuevo sitio.

> Las siguientes reglas y políticas de ILM son solo ejemplos. Existen varias formas de configurar las reglas de ILM. Antes de activar una nueva directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

¿Cómo afecta el rendimiento el cambio de una política de ILM

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.

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 codificación de borrado diferente a los objetos existentes codificados con borrado.

  > StorageGRID considera que cada perfil de código de borrado es único y no reutiliza fragmentos de código de borrado cuando se utiliza un perfil nuevo.

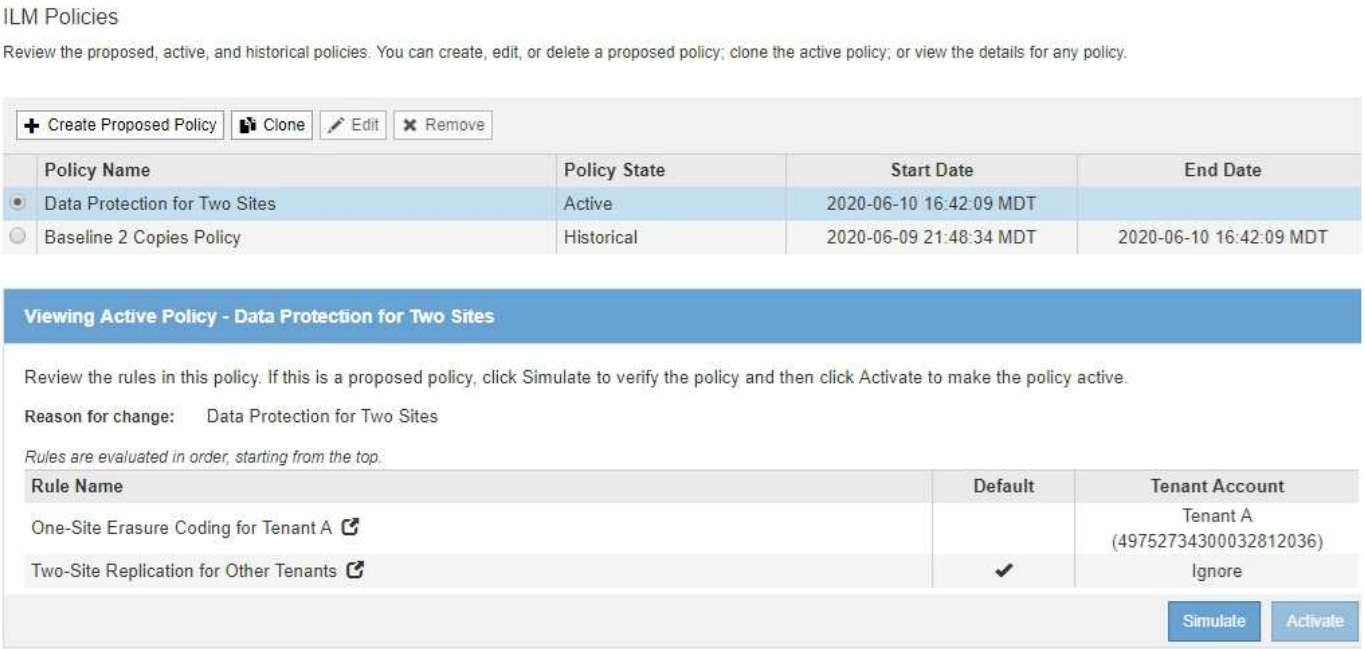
- Cambiar el tipo de copias necesarias para los objetos existentes; por ejemplo, convertir un gran porcentaje de objetos replicados en objetos de código de borrado.
- Mover copias de objetos existentes a una ubicación completamente diferente; por ejemplo, mover un gran número de objetos hacia o desde un pool de almacenamiento en cloud, o desde un sitio remoto.

Información relacionada

Cree una política de ILM

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.

> La primera regla de este ejemplo utiliza un filtro avanzado para garantizar que la codificación de borrado no se utilice para objetos pequeños. Cualquiera de los objetos del arrendatario A que sean menores de 1 MB estará protegido por la segunda regla, que utiliza la replicación.

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	Centro de datos 1
Colocación del contenido	Codificación de borrado 2+1 en el centro de datos 1 del día 0 al para siempre

Regla 2: Replicación de dos sitios para otros inquilinos

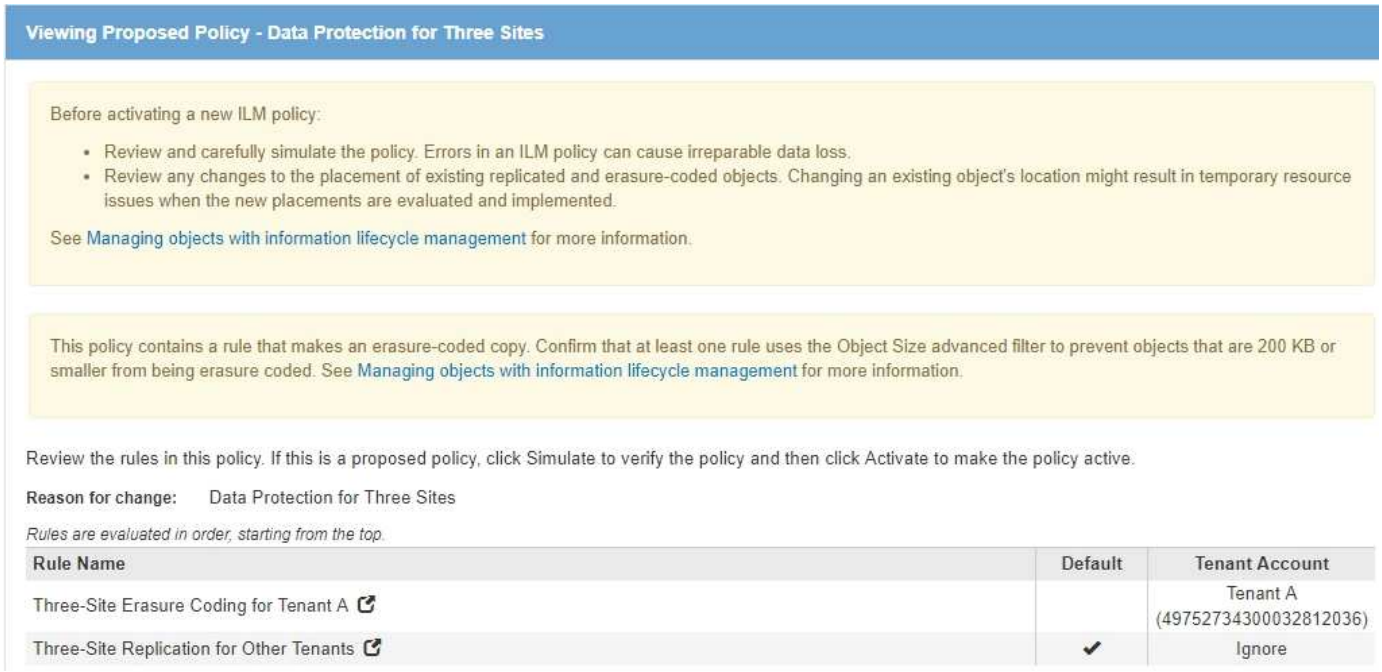
Definición de regla	Valor de ejemplo
Nombre de regla	Replicación de dos sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Pools de almacenamiento	Data Center 1 y Data Center 2

Definición de regla	Valor de ejemplo
Colocación del contenido	Dos copias replicadas del día 0 para siempre: Una copia en el centro de datos 1 y una copia en el centro de datos 2.

Propuesta de política de ILM, por ejemplo 6: Protección de datos en tres sitios

En este ejemplo, se está actualizando la política de ILM para un sistema StorageGRID de tres sitios.

Tras realizar una ampliación para añadir el nuevo sitio, el administrador de grid creó dos nuevos pools de almacenamiento: Un pool de almacenamiento para Data Center 3 y un pool de almacenamiento que contiene los tres sitios (no es lo mismo que el pool de almacenamiento predeterminado de todos los nodos de almacenamiento). Posteriormente, el administrador creó dos nuevas reglas de ILM y una nueva política de ILM propuesta, diseñada para proteger datos en 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	Los 3 centros de datos (incluye el centro de datos 1, el centro de datos 2 y el centro de datos 3)

Definición de regla	Valor de ejemplo
Colocación del contenido	Codificación de borrado 2+1 en los 3 centros de datos del día 0 para 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	Data Center 1, Data Center 2 y Data Center 3
Colocación del contenido	Tres copias replicadas del día 0 para siempre: Una copia en el centro de datos 1, una copia en el centro de datos 2 y una copia en el centro de datos 3.

Activar la política de ILM propuesta por ejemplo 6

Al activar una nueva política de ILM propuesta, es posible que los objetos existentes se muevan a nuevas ubicaciones o que se puedan crear copias de objetos nuevas para los objetos existentes, según las instrucciones de colocación 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 activa actualmente para este ejemplo, los objetos del inquilino A están protegidos mediante codificación de borrado 2+1 en el centro de datos 1. En la nueva política de ILM propuesta, los objetos del inquilino A se protegerán mediante codificación de borrado 2+1 en los centros de datos 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. A continuación, cada uno de los tres fragmentos se almacena en un centro de datos 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 totalmente nuevos codificados por borrado a los tres centros de datos.

> Los fragmentos 2+1 existentes en el centro de datos 1 no se reutilizan. StorageGRID considera que cada perfil de código de borrado es único y no reutiliza fragmentos de código de borrado cuando se utiliza un perfil nuevo.

Qué ocurre cuando cambian las instrucciones de replicación

En la política de ILM activa actualmente para este ejemplo, los objetos que pertenecen a otros inquilinos se protegen con dos copias replicadas en los pools de almacenamiento en los centros de datos 1 y 2. En la nueva política de ILM propuesta, los objetos que pertenecen a otros clientes se protegerán mediante tres copias replicadas de los pools de almacenamiento en los centros de datos 1, 2 y 3.

Cuando se activa la nueva política de ILM, se producen las siguientes operaciones de ILM:

- Cuando un inquilino distinto De inquilino procesa un objeto nuevo, StorageGRID crea tres copias y guarda una copia en cada centro de datos.
- Los objetos existentes que pertenecen a estos otros inquilinos se reevalúan durante el proceso de análisis de ILM en curso. Debido a que las copias de objetos existentes en el centro de datos 1 y en el centro de datos 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 centro de datos 3.

Impacto en el rendimiento de la activación de esta política

Si se activa la política de ILM propuesta en este ejemplo, el rendimiento general de este sistema StorageGRID se verá afectado temporalmente. Se necesitarán niveles más altos que los niveles normales de los recursos de grid para crear nuevos fragmentos con código de borrado para los objetos existentes De inquilino A y las nuevas copias replicadas en el centro de datos 3 para los objetos existentes de otros clientes.

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 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 ingesta como 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 directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas.

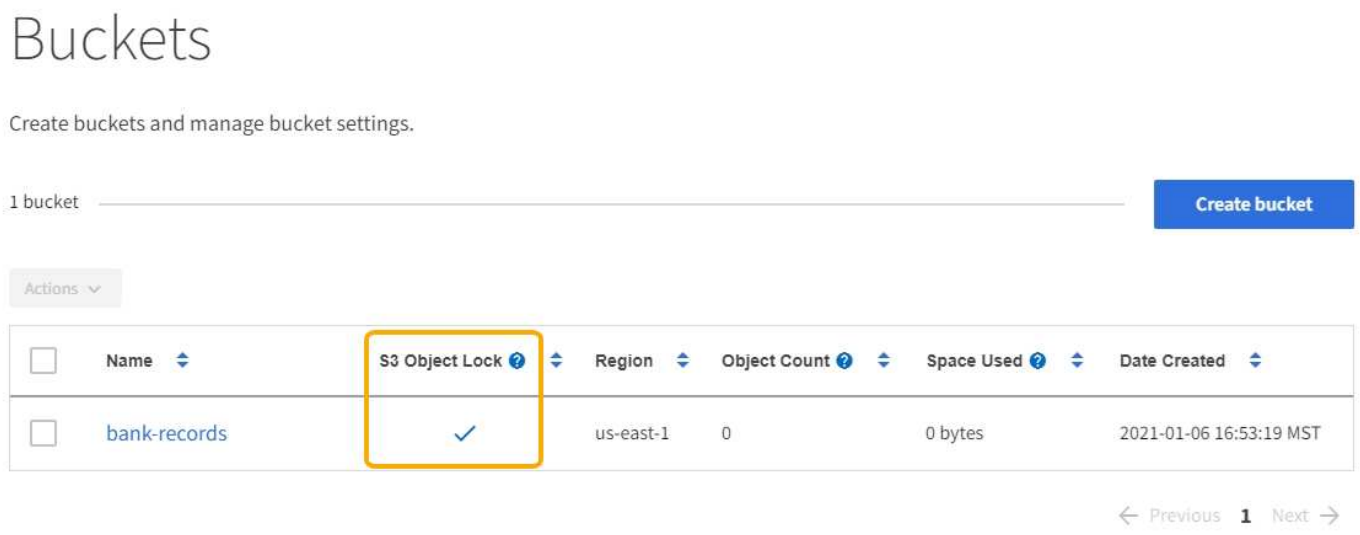
Información relacionada

- 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.

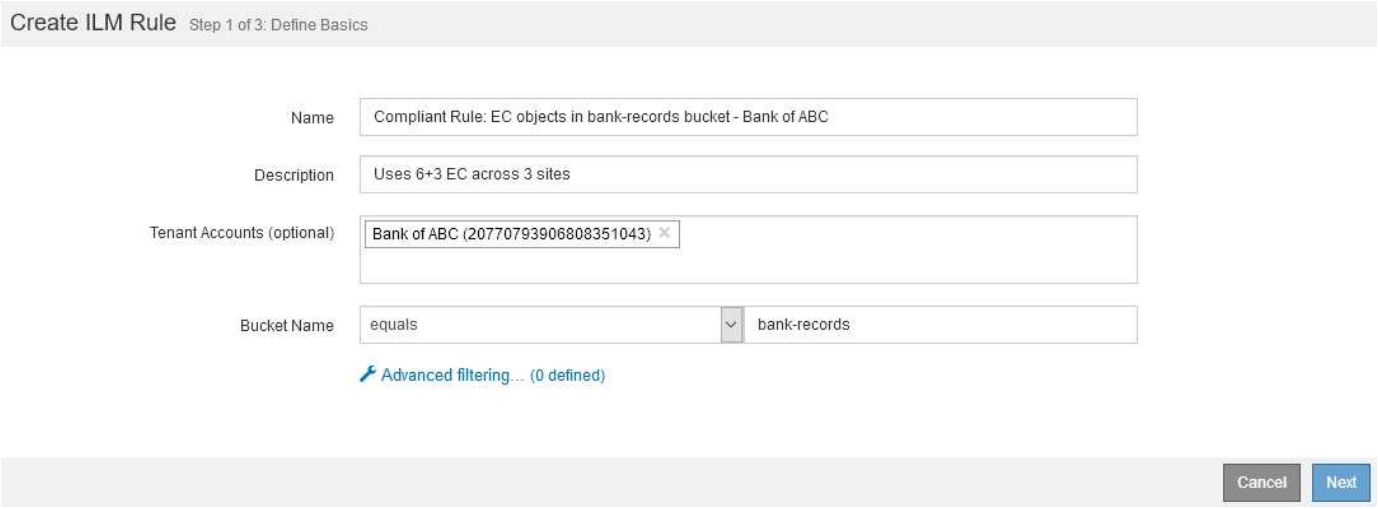
Configuración para cada objeto	Valor de ejemplo
`retain-until-date`	`"2030-12-30T23:59:59Z"` (30 de diciembre de 2030) Cada versión de objeto tiene su propia `retain-until-date` ajuste. Este ajuste se puede aumentar, pero no disminuir.

Configuración para cada objeto	Valor de ejemplo
`legal hold`	`"OFF"` (No en vigor) Se puede colocar o levantar una retención legal en cualquier versión del objeto en cualquier momento durante el período de retención. Si un objeto se encuentra bajo una retención legal, el objeto no se puede eliminar incluso si el `retain-until-date` se ha alcanzado.

Ejemplo de regla de ILM 1 para el bloqueo de objetos S3: Perfil de código de borrado con coincidencia de bloques

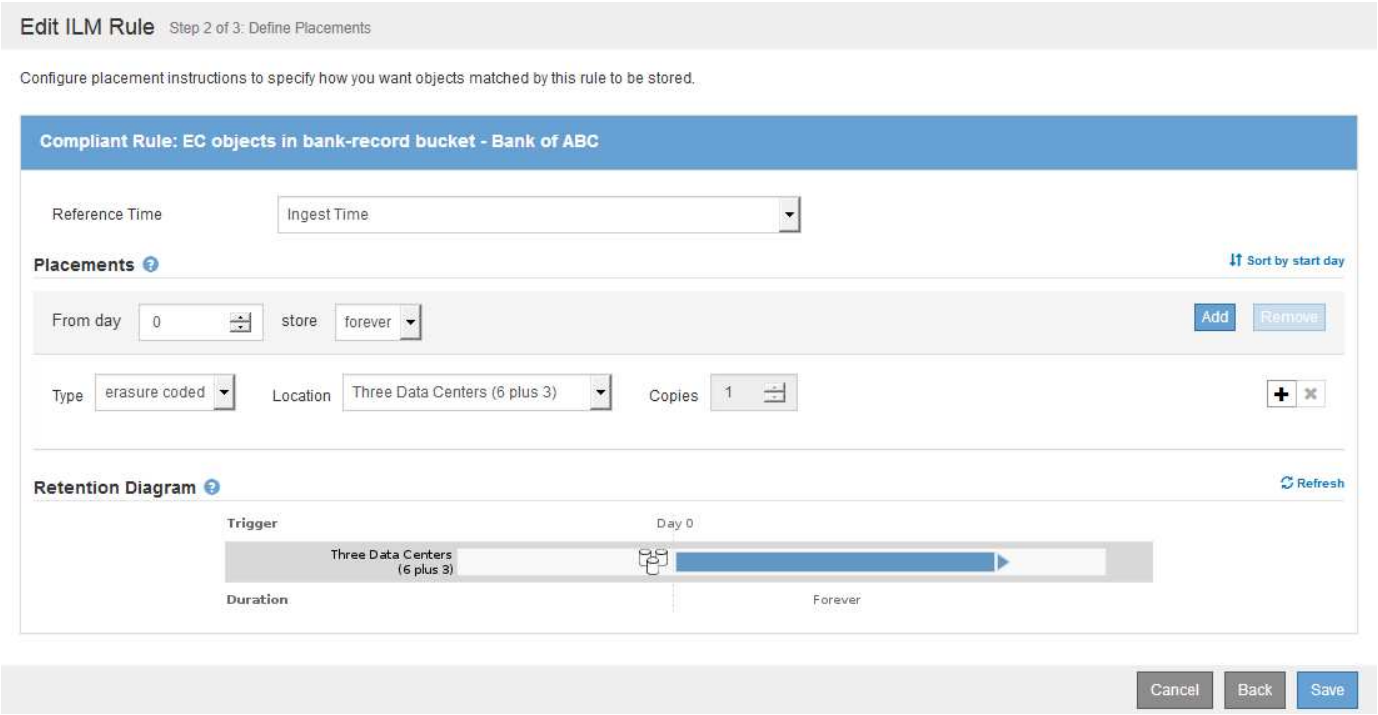
Esta regla de ILM de ejemplo se aplica solo a la cuenta de inquilino de S3 llamada Bank of ABC. Coincide con cualquier objeto de `bank-records` Bucket y, a continuación, utiliza la codificación de borrado para almacenar el objeto en nodos de almacenamiento en tres sitios de centro de datos mediante un perfil de código de borrado 6+3. Esta regla satisface los requisitos de los bloques con el bloqueo de objetos S3 habilitado: Se conserva una copia codificada con borrado en los nodos de almacenamiento desde el día 0 hasta siempre utilizando el tiempo de ingesta como hora de referencia.

Definición de regla	Valor de ejemplo
Nombre de regla	Regla conforme: Objetos de EC en bloque de registros bancarios - Banco de ABC
Cuenta de inquilino	Banco de ABC
Nombre del bloque	`bank-records`
Filtrado 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

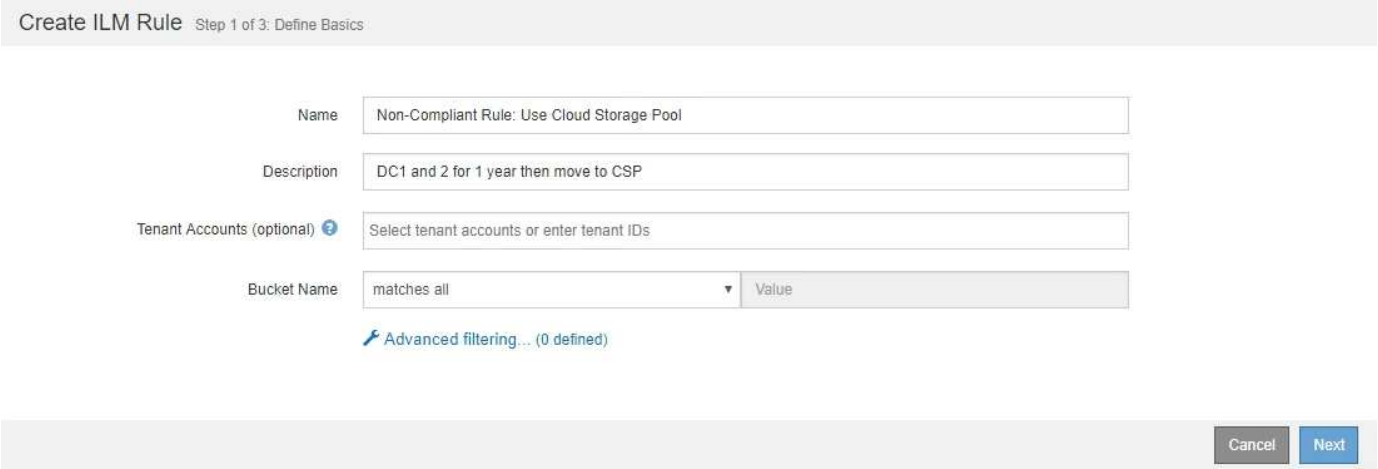
Definición de regla	Valor de ejemplo
Ubicaciones	Desde el día 0 almacenar para siempre
Perfil de código de borrado	• Cree una copia codificada con borrado en los nodos de almacenamiento en tres centros de datos • Utiliza un esquema de codificación de borrado de 6+3



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: Utilizar pool de almacenamiento en cloud
Cuentas de inquilino	No especificado
Nombre del bloque	No se especifica, pero solo se aplica a bloques que no tienen habilitado el bloqueo de objetos de S3 (o la función de cumplimiento heredado).
Filtrado avanzado	No especificado

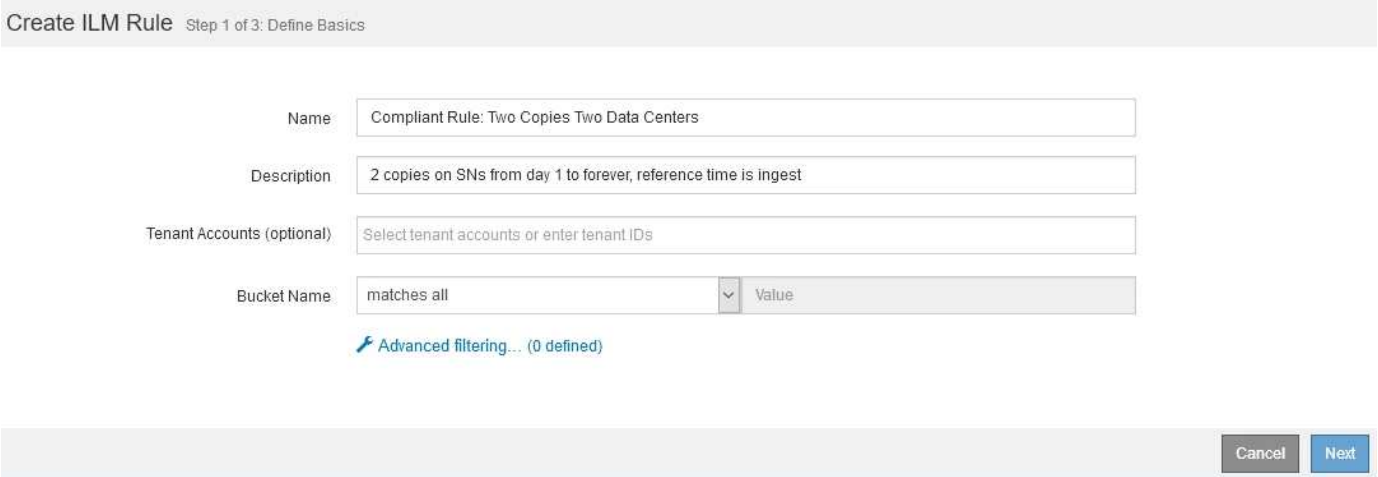


Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Ubicaciones	• El día 0, conserve dos copias replicadas en los nodos de almacenamiento en el centro de datos 1 y en el centro de datos 2 durante 365 días • Después de 1 año, mantenga siempre una copia replicada en un pool de almacenamiento en cloud

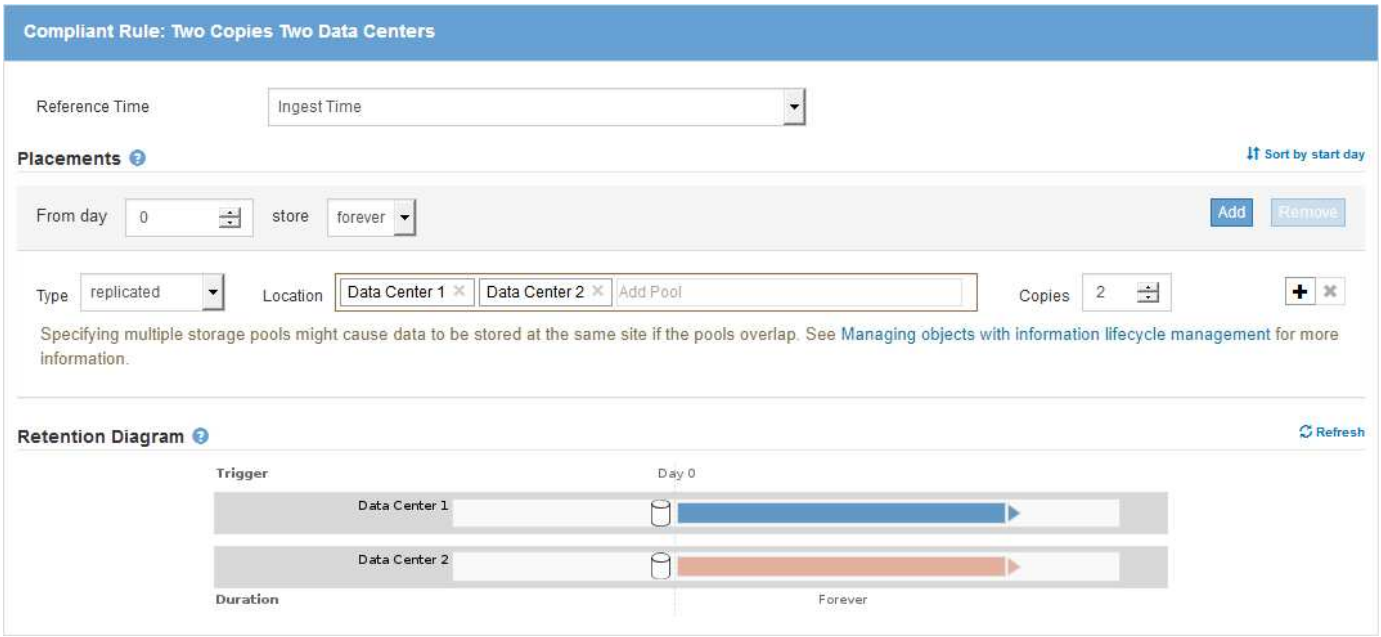
Ejemplo de regla ILM 3 para bloqueo de objetos S3: Regla predeterminada

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
Filtrado 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).



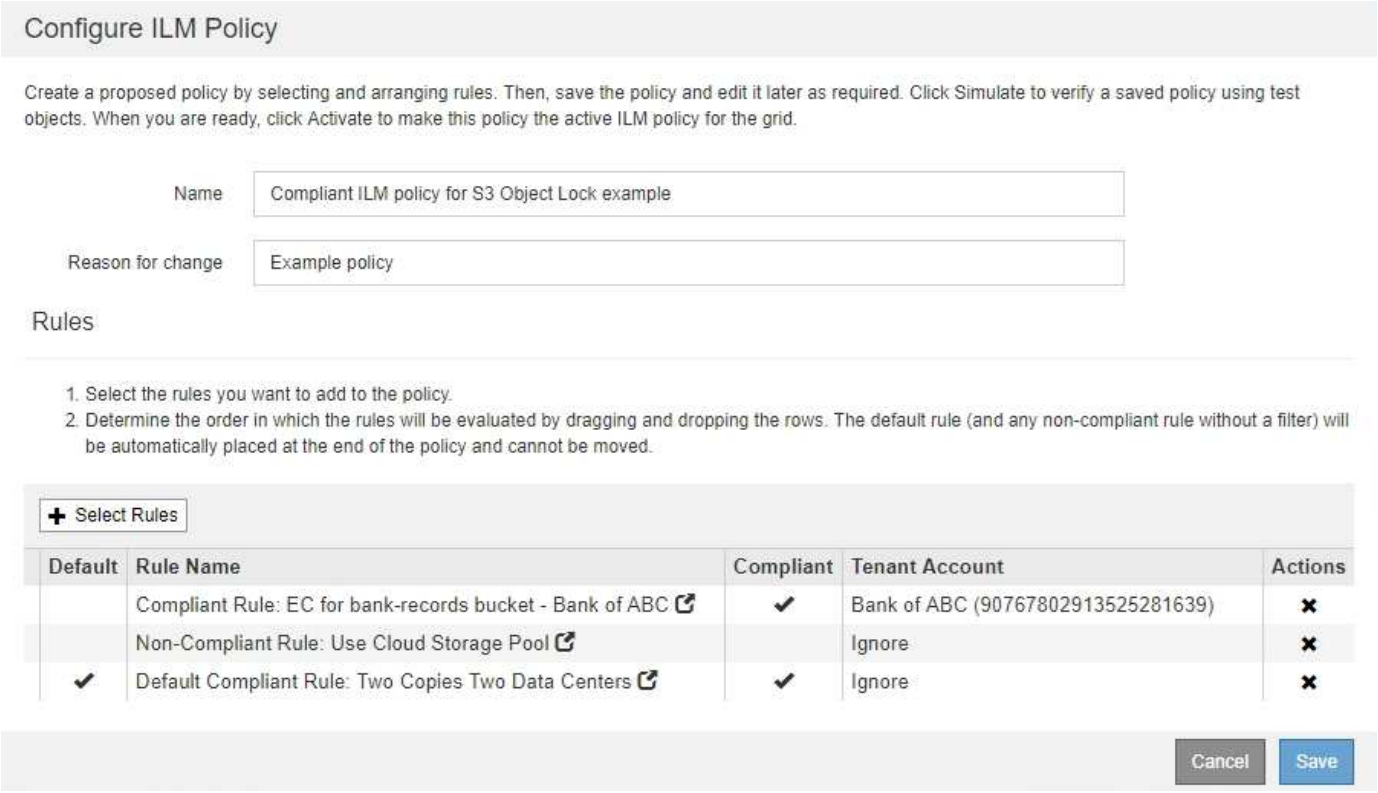
Ejemplo de política de ILM conforme a la normativa para el bloqueo de objetos S3

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 directiva propuesta.

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.



Simular la política propuesta

Después de añadir reglas a la política propuesta, elegir una regla de cumplimiento predeterminada y organizar las demás reglas, debe simular la política probando objetos desde el bloque con el bloqueo de objetos S3 habilitado y desde otros bloques. 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.

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 la 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.

Información relacionada

"Política de manejo de vulnerabilidades"

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 seguridad reforzada que no se incluyen en las versiones anteriores.

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 la página de descarga del software StorageGRID. Para obtener instrucciones paso a paso para actualizar el software StorageGRID, consulte las instrucciones para actualizar StorageGRID. Para obtener instrucciones sobre cómo aplicar una revisión, consulte las instrucciones de recuperación y mantenimiento.

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.

Utilice la herramienta matriz de interoperabilidad de NetApp para obtener una lista de las versiones compatibles.

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.

Utilice la herramienta matriz de interoperabilidad de NetApp para obtener una lista de las versiones compatibles.

Actualizar 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.

Utilice la herramienta matriz de interoperabilidad de NetApp para obtener una lista de las versiones compatibles.

Información relacionada

"Descargas de NetApp: StorageGRID"

Actualizar el software de

Recuperación y mantenimiento

"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.

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 la lista de puertos internos en la guía de instalación de su plataforma.
- 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 la lista de puertos internos en la guía de instalación de su plataforma.
- Acepte tráfico de cliente entrante sólo en puntos finales configurados explícitamente. Consulte Administración de redes de clientes que no son de confianza.

Información relacionada

Directrices sobre redes

Imprimador de rejilla

Administre StorageGRID

Instale Red Hat Enterprise Linux o CentOS

Instalar Ubuntu o Debian

Instale VMware

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.

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 utiliza un firewall interno que se gestiona automáticamente. 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 la guía de instalación de su plataforma.

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 impedirán que el malware acceda a los datos protegidos con StorageGRID si tanto StorageGRID como 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.

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 tiene pensado configurar el acceso de cliente a los recursos compartidos de auditoría de CIFS o NFS, bloquee o deshabilite el acceso a estos servicios.

Proteja los nodos durante la instalación

No permita que los usuarios que no son de confianza accedan a los nodos de StorageGRID a través de la red cuando los nodos se están instalando. 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 les permita tener 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.
- De manera opcional, use un proxy de administrador para obtener más control sobre la comunicación de AutoSupport desde los nodos de administrador al soporte de NetApp. Consulte los pasos para crear un proxy de administrador en las instrucciones para administrar StorageGRID.
- 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 para administrar 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 clientes que no son de confianza se conecten directamente a los nodos de almacenamiento. Utilice un extremo de equilibrio de carga servido por un nodo de puerta de enlace o un equilibrador de carga de terceros.
- No habilite los servicios de salida para inquilinos que no sean de confianza. Por ejemplo, al crear la cuenta para un arrendatario que no sea de confianza, no permita que el arrendatario utilice su propio origen de identidad y no permita el uso de servicios de plataforma. Consulte los pasos para crear una cuenta de inquilino en las instrucciones para administrar StorageGRID.
- 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 obtener más control sobre los pools de almacenamiento en cloud y la comunicación de servicios de plataforma de los nodos de almacenamiento a los servicios externos. Consulte los pasos para crear un proxy de almacenamiento en las instrucciones para administrar StorageGRID.
- Opcionalmente, conéctese a servicios externos mediante la red cliente. A continuación, seleccione **CONFIGURACIÓN** > **Red** > **redes de cliente no fiables** e indique que la red de clientes 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:

- Configure y utilice puntos finales del equilibrador de carga en lugar de utilizar el servicio CLB en nodos de puerta de enlace. Consulte los pasos para gestionar el equilibrio de carga en las instrucciones para administrar StorageGRID.

  El servicio CLB está obsoleto.

- 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** > **Red** > **redes de cliente no fiables** e indique que la red de cliente del nodo de puerta de enlace 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.
- Si la controladora de almacenamiento del dispositivo incluye unidades FDE o FIPS y la función Drive Security está habilitada, use SANtricity para configurar las claves de seguridad de unidades.
- Para dispositivos sin unidades FDE o FIPS, habilite el cifrado de nodos con un servidor de gestión de claves (KMS).

Consulte las instrucciones de instalación y mantenimiento de su dispositivo de hardware de StorageGRID.

Información relacionada

- Instale Red Hat Enterprise Linux o CentOS
- Instalar Ubuntu o Debian
- Instale VMware
- Administre StorageGRID
- Usar una cuenta de inquilino
- Servicios de aplicaciones SG100 y SG1000
- Dispositivos de almacenamiento SG5600
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG6000

Directrices de refuerzo para certificados de servidor

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.

> StorageGRID gestiona los certificados utilizados para los extremos del equilibrador de carga por separado. Para configurar certificados de equilibrador de carga, consulte los pasos para configurar los extremos de equilibrador de carga en las instrucciones para administrar StorageGRID.

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 de la expulsión" en "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 extremo de estilo alojado virtual de S3, que requiere el uso de un comodín si los nombres de bloque no se conocen con anterioridad.
- 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 `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.

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 las instrucciones para supervisar y solucionar problemas para obtener más información acerca de los registros de StorageGRID. Consulte las instrucciones de los mensajes de auditoría para obtener más información acerca de los mensajes de auditoría de StorageGRID.

AutoSupport de NetApp

La función AutoSupport de StorageGRID le permite supervisar de forma proactiva el estado del sistema y enviar automáticamente mensajes y detalles al soporte técnico de NetApp, al equipo de soporte interno de su organización o a un partner de soporte. De manera predeterminada, los mensajes de AutoSupport al soporte técnico de NetApp se habilitan cuando se configura StorageGRID 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 sensible de los mensajes de AutoSupport, NetApp recomienda encarecidamente utilizar HTTPS como protocolo de transporte predeterminado para enviar mensajes de AutoSupport a la compatibilidad de NetApp.

De manera opcional, se puede configurar un proxy de administrador para obtener más control sobre la comunicación de AutoSupport desde los nodos de administrador al soporte técnico de NetApp. Consulte los pasos para crear un proxy de administrador en las instrucciones para administrar StorageGRID.

Uso compartido de recursos de origen cruzado (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un bloque de S3 si desea que dicho bloque y los objetos de ese bloque sean accesibles a las aplicaciones web de otros dominios. En general, no active CORS a menos que sea necesario. Si se requiere CORS, restringirlo a orígenes de confianza.

Consulte los pasos para configurar el uso compartido de recursos de origen cruzado (CORS) en las instrucciones para utilizar cuentas de arrendatario.

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.

Información relacionada

Supervisión y solución de problemas

Revisar los registros de auditoría

Usar cuenta de inquilino

Administre StorageGRID

Configure FabricPool

Configure StorageGRID para FabricPool: Información general

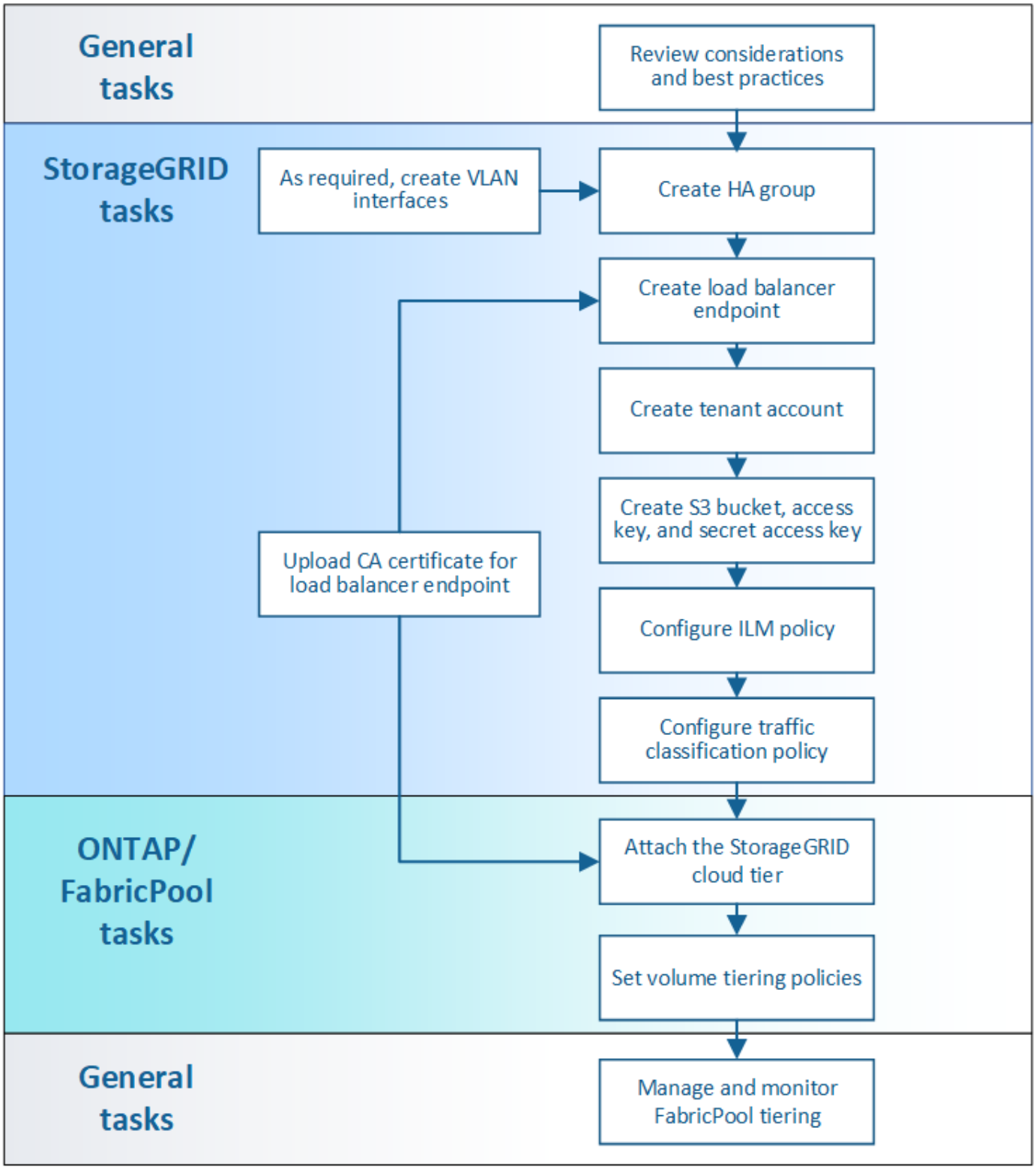
Si utiliza el software ONTAP de NetApp, puede utilizar FabricPool de NetApp para organizar los datos en niveles inactivos o inactivos en un sistema de almacenamiento de objetos StorageGRID de NetApp.

Acerca de estas instrucciones

Utilice estas instrucciones para:

- Obtenga información general sobre la configuración de un sistema de almacenamiento de objetos StorageGRID para usar con FabricPool.
- Aprenda cómo obtener la información que ofrece a ONTAP cuando asocie StorageGRID como un nivel de cloud de FabricPool.
- Obtenga más información sobre las prácticas recomendadas para configurar la política de gestión del ciclo de vida de la información (ILM) de StorageGRID, una política de clasificación del tráfico de StorageGRID y otras opciones de StorageGRID para la carga de trabajo de FabricPool.

Flujo de trabajo de configuración



Antes de empezar

- 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, incluidos Grid Manager y el inquilino Manager.

- Revise estos recursos adicionales, que ofrecen detalles sobre el uso y la configuración de FabricPool:
  - "TR-4598: Prácticas recomendadas de FabricPool en ONTAP 9.9.1"
  - "Documentación de ONTAP 9"

¿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. Los datos se almacenan en el medio de almacenamiento primario o en el almacén de datos de objetos según se acceda con frecuencia o no. El uso de agregados habilitados para FabricPool le ayuda a reducir el coste del almacenamiento sin comprometer el rendimiento, la eficiencia o la protección.

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 es una arquitectura de almacenamiento que gestiona los datos como objetos, a diferencia de otras arquitecturas de almacenamiento, como el almacenamiento de archivos o bloques. Los objetos se mantienen dentro de un único contenedor (como un bloque) 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 los datos de ONTAP en niveles en diversos proveedores de almacenes de objetos, incluido 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.

¿Puedo usar varios clústeres de ONTAP con StorageGRID?

Estas instrucciones describen cómo conectar StorageGRID a un único clúster de ONTAP. Sin embargo, se recomienda conectar el mismo sistema StorageGRID a varios clústeres de ONTAP.

El único requisito para organizar los datos en niveles desde varios clústeres de ONTAP en un único sistema StorageGRID es que debe utilizar un bloque de S3 diferente para cada clúster. En función de sus requisitos, puede utilizar el mismo grupo de alta disponibilidad (ha), el extremo de equilibrio de carga y la cuenta de inquilino para todos los clústeres, o bien puede configurar cada uno de estos elementos para cada clúster.

Adjuntar StorageGRID como nivel de cloud

Información necesaria para adjuntar StorageGRID como nivel de cloud

Antes de poder asociar StorageGRID como nivel de cloud para FabricPool, debe realizar algunos pasos de configuración en StorageGRID y obtener ciertos valores.

Acerca de esta tarea

La siguiente tabla enumera la información que debe proporcionar a ONTAP cuando asocia StorageGRID como nivel de cloud para FabricPool. En los temas de esta sección se explica cómo utilizar el administrador de grid y el administrador de inquilinos de StorageGRID para obtener la información que necesita.

> Los nombres de campo exactos que se muestran y el proceso que se utiliza para introducir los valores necesarios en ONTAP dependen de si está utilizando la CLI de ONTAP (Storage aggregate object-store config create) o el Administrador del sistema de ONTAP (**almacenamiento** > **agregados y discos** > **nivel de cloud**).

Si quiere más información, consulte lo siguiente:

- "TR-4598: Prácticas recomendadas de FabricPool en ONTAP 9.9.1"
- "Documentación de ONTAP 9"

Campo ONTAP	Descripción
Nombre de almacén de objetos	Cualquier nombre único y descriptivo. Por ejemplo: `StorageGRID_Cloud_Tier`.
Tipo de proveedor	StorageGRID (Administrador del sistema de ONTAP) o. `SGWS` (CLI de ONTAP).
Puerto	El puerto que FabricPool utilizará cuando se conecte a StorageGRID. Determina qué número de puerto se va a utilizar al definir el punto final del equilibrador de carga de StorageGRID. Cree un extremo de equilibrador de carga para FabricPool
Nombre del servidor	El nombre de dominio completo (FQDN) para el extremo de equilibrador de carga de StorageGRID. Por ejemplo: `s3.storagegrid.company.com`. Tenga en cuenta lo siguiente: • El nombre de dominio que especifique aquí debe coincidir con el nombre de dominio del certificado de CA que cargue para el extremo de equilibrador de carga de StorageGRID. • El registro DNS de este nombre de dominio debe asignar a cada dirección IP que utilice para conectarse a StorageGRID. Configure el servidor DNS para las direcciones IP de StorageGRID

Campo ONTAP	Descripción
Nombre del contenedor	El nombre del bloque de StorageGRID que utilizará con este clúster de ONTAP. Por ejemplo: `fabricpool-bucket`. Puede crear este bloque en el Administrador de inquilinos o, a partir del Administrador del sistema ONTAP 9.10, puede crear el bloque con el asistente de configuración de FabricPool. Tenga en cuenta lo siguiente: • El nombre del bloque no se puede cambiar una vez creada la configuración. • El bloque no puede tener habilitado el control de versiones. • Debe utilizar un bloque diferente para cada clúster de ONTAP que organice los datos en niveles en StorageGRID. Cree un bloque de S3 y obtenga una clave de acceso
Clave de acceso y contraseña secreta	La clave de acceso y la clave de acceso secreta de la cuenta de inquilino de StorageGRID. Estos valores se generan en el Administrador de arrendatarios. Cree un bloque de S3 y obtenga una clave de acceso
SSL	Debe estar habilitado.
Certificado de almacén de objetos	El certificado de CA que cargó al crear el extremo del equilibrador de carga StorageGRID. **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. Cree un extremo de equilibrador de carga para FabricPool

Después de terminar

Una vez que haya obtenido la información de StorageGRID necesaria, podrá ir a ONTAP para añadir StorageGRID como nivel de cloud, añadir el nivel de cloud como agregado y establecer políticas de organización en niveles del volumen.

Prácticas recomendadas para el equilibrio de carga

Antes de asociar StorageGRID como un nivel de cloud de FabricPool, debe utilizar el Administrador de grid de StorageGRID para configurar al menos un extremo de equilibrador de carga.

¿Qué es el equilibrio de carga?

Cuando los datos se organizan en niveles desde FabricPool a un sistema StorageGRID, StorageGRID utiliza un equilibrio de carga para gestionar la carga de trabajo de procesamiento y recuperación. El equilibrio de carga maximiza la velocidad y la capacidad de conexión mediante la distribución de la carga de trabajo FabricPool 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".

> El servicio de equilibrador de carga de conexión (CLB) independiente en los nodos de puerta de enlace queda obsoleto y ya no se recomienda su uso con FabricPool.

Prácticas recomendadas para el balanceo de carga de StorageGRID

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).

Debe configurar un extremo de equilibrador de carga de StorageGRID para definir el puerto que utilizarán los nodos de puerta de enlace y los nodos de administración para las solicitudes de FabricPool entrantes y salientes.

Prácticas recomendadas para el certificado de extremo de equilibrio de carga

Al crear un extremo de equilibrio de carga para utilizarlo con FabricPool, debe utilizar HTTPS como protocolo. Se admite la comunicación con StorageGRID sin cifrado TLS, pero no se recomienda

A continuación, se puede cargar un certificado firmado por una CA de confianza pública o una entidad de certificación (CA) privada, o bien se puede generar un certificado autofirmado. El certificado permite la autenticación de ONTAP con StorageGRID.

Como práctica recomendada, debe usar un certificado de servidor de CA para proteger la conexión. Los certificados firmados por una CA se pueden rotar de forma no disruptiva.

Cuando solicite un certificado de CA para utilizarlo con el extremo de equilibrador de carga, asegúrese de que el nombre de dominio del certificado coincide con el nombre de servidor que escriba en ONTAP para ese extremo de equilibrador de carga. Si es posible, utilice un comodín (*) para permitir URL de tipo host virtual. Por ejemplo:

```
*.s3.storagegrid.company.com
```

Cuando añade StorageGRID como un nivel de cloud de FabricPool, debe instalar el mismo certificado en el clúster de ONTAP, así como en el certificado raíz y en todos los certificados de una entidad de certificación (CA) subordinados.

> StorageGRID utiliza certificados de servidor para diversos fines. Si se conecta al servicio Load Balancer, de manera opcional, se puede usar el certificado API S3 y Swift.

Para obtener más información acerca del certificado de servidor para un extremo de equilibrio de carga:

- Configurar puntos finales del equilibrador de carga
- Directrices de refuerzo para certificados de servidor

Mejores prácticas para grupos de alta disponibilidad

Antes de asociar StorageGRID como nivel de cloud FabricPool, debe usar el Administrador de grid de StorageGRID para configurar un grupo de alta disponibilidad.

¿Qué es un grupo de alta disponibilidad?

Para garantizar que el servicio Load Balancer esté siempre disponible para gestionar datos FabricPool, puede agrupar las interfaces de red de varios nodos de administración y puerta de enlace en una sola entidad, conocida como grupo de alta disponibilidad. Si el nodo activo del grupo ha falla, otro nodo del grupo puede seguir gestionando la carga de trabajo.

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 crear un grupo de alta disponibilidad, debe realizar estos pasos generales:

1. Seleccione interfaces de red para uno o más nodos de administración o nodos de puerta de enlace. Puede seleccionar la interfaz de red de cuadrícula (eth0), la interfaz de red de cliente (eth2) o una interfaz VLAN.

   > Si piensa utilizar una interfaz VLAN para segregar el tráfico FabricPool, un administrador de red primero debe configurar una interfaz troncal y la VLAN correspondiente. Cada VLAN se identifica por un ID o etiqueta numéricos. Por ejemplo, la red puede usar VLAN 100 para el tráfico de FabricPool.

2. Asigne una o varias direcciones IP virtuales (VIP) al grupo. Las aplicaciones cliente, como FabricPool, pueden utilizar cualquiera de estas direcciones VIP para conectarse a StorageGRID.
3. Especifique una interfaz que sea la interfaz principal y determine el orden de prioridad de las interfaces de copia de seguridad. La interfaz Primary es la interfaz activa a menos que se produzca un fallo.

Si el grupo ha incluye más de una interfaz y la interfaz principal falla, las direcciones 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. Por lo general, este proceso de conmutación por error solo 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.

Una vez resuelto el fallo y haya una interfaz de mayor prioridad disponible de nuevo, las direcciones VIP se mueven automáticamente a la interfaz de mayor prioridad disponible.

Prácticas recomendadas para grupos de alta disponibilidad

Las prácticas recomendadas para crear un grupo de alta disponibilidad de StorageGRID para FabricPool dependen de la carga de trabajo de la siguiente manera:

- 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.

Configure el servidor DNS para las direcciones IP de StorageGRID

Después de configurar los grupos de alta disponibilidad y los extremos de equilibrador de carga, debe asegurarse de que el sistema de nombres de dominio (DNS) del sistema ONTAP incluye un registro para asociar el nombre del servidor StorageGRID (nombre de dominio completo) a la dirección IP que FabricPool utilizará 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, FabricPool se conectará a las direcciones IP virtuales de dicho grupo de alta disponibilidad.
- Si no está utilizando un grupo de alta disponibilidad, FabricPool 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.

También debe asegurarse de que el registro DNS hace referencia a todos los nombres de dominio de extremo requeridos, incluidos los nombres de comodín.

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 consta de una o varias interfaces de red en los nodos de administración, los nodos de puerta de enlace o ambos.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

- Si planea utilizar una VLAN, ha creado la interfaz VLAN. Consulte Configure las interfaces VLAN.

Acerca de esta tarea

Cada grupo de alta disponibilidad utiliza direcciones IP virtuales (VIP) para proporcionar acceso de alta disponibilidad a los servicios compartidos de los nodos asociados.

Para obtener más detalles sobre esta tarea, consulte Gestión de grupos de alta disponibilidad.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **grupos de alta disponibilidad**.
2. Seleccione **Crear**.
3. Introduzca un nombre único y, opcionalmente, una descripción.
4. 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.

5. Determine la interfaz primaria y cualquier interfaz de backup para este grupo de alta disponibilidad.

   Arrastre y suelte filas para cambiar los valores de 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 ha incluye más de una interfaz y la interfaz activa falla, las direcciones 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. Especifique la subred VIP en notación CIDR—una dirección IPv4 seguida de una barra diagonal y la longitud de la subred (0-32).

   La dirección de red no debe tener ningún bit de host configurado. Por ejemplo: `192.16.0.0/22`.

7. De manera opcional, si las direcciones IP de ONTAP que se utilizan 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.
8. Introduzca una o más direcciones IP virtuales para el grupo de alta disponibilidad. Puede añadir hasta 10 direcciones IP. Todos los VIP deben estar dentro de la subred VIP.

   Debe proporcionar al menos una dirección IPv4. De manera opcional, es posible especificar direcciones IPv4 e IPv6 adicionales.

9. Seleccione **Crear grupo ha** y, a continuación, seleccione **Finalizar**.

Cree un extremo de equilibrador de carga para FabricPool

Al configurar StorageGRID para su uso con FabricPool, debe configurar un extremo de equilibrador de carga y cargar el certificado de extremo de equilibrador de carga, que se utiliza para proteger la conexión entre ONTAP y StorageGRID.

Lo que necesitará

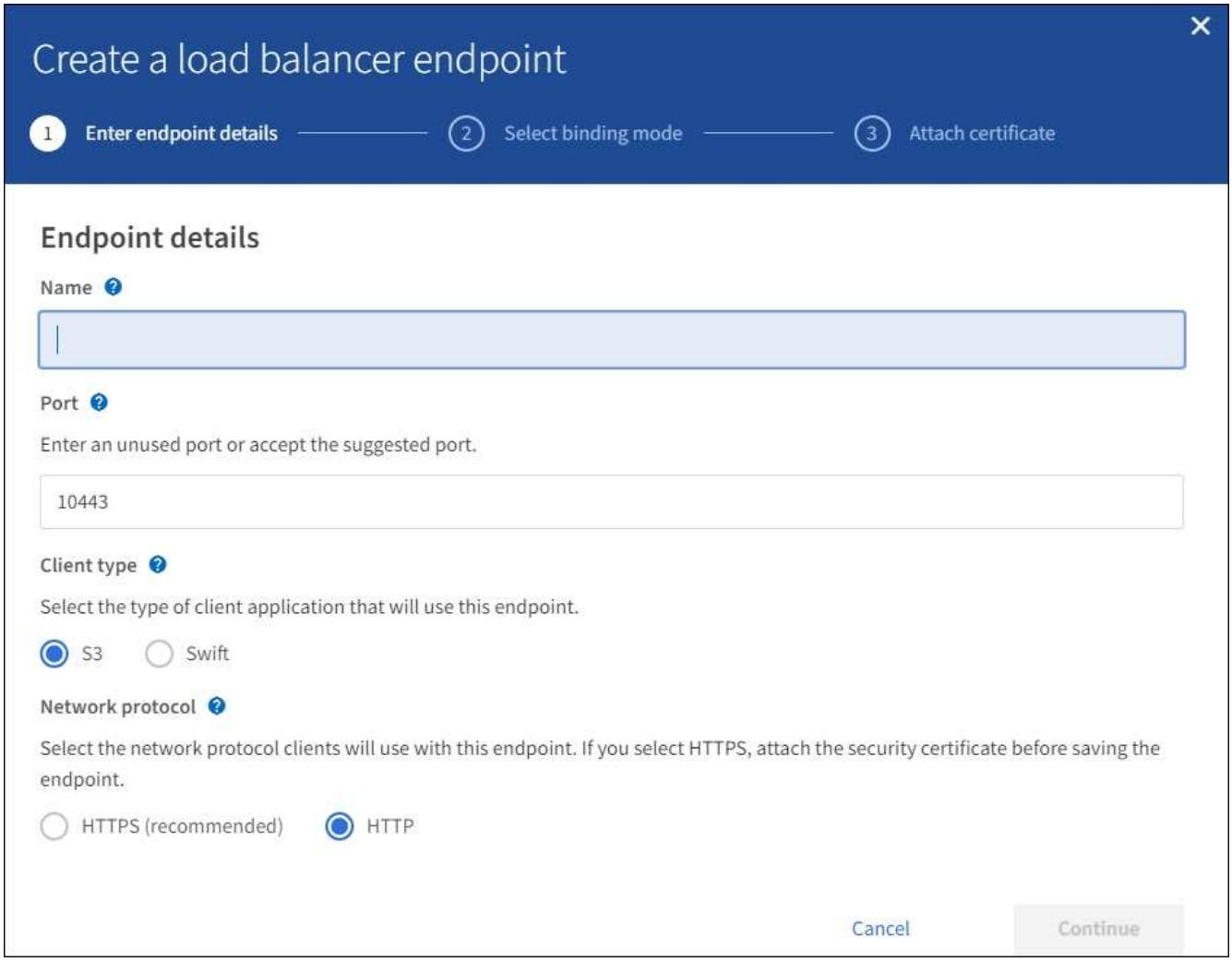
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.
- Tiene los siguientes archivos:
  - Certificado de servidor: El archivo de certificado de servidor personalizado.
  - Clave privada del certificado de servidor: El archivo de claves privadas del certificado de servidor personalizado.
  - Paquete DE CA: Un único archivo opcional que contiene 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.

Acerca de esta tarea

Para obtener más detalles sobre esta tarea, consulte Configurar puntos finales del equilibrador de carga.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**.
2. Seleccione **Crear**.



3. Introduzca los detalles de los extremos.

Campo	Descripción
Nombre	Nombre descriptivo para el extremo
Puerto	El puerto StorageGRID que desea usar para el equilibrio de carga. De forma predeterminada, este campo es 10433, pero puede introducir cualquier puerto externo no utilizado. Si introduce 80 o 443, el extremo se configura únicamente en los nodos de puerta de enlace, ya que estos puertos están reservados en los nodos de administración. **Nota:** los puertos utilizados por otros servicios de red no están permitidos. ConsulteReferencia de puerto de red. Debe proporcionar este mismo número de puerto a ONTAP al asociar StorageGRID como un nivel de cloud de FabricPool.
Tipo de cliente	Seleccione **S3**.
Protocolo de red	Seleccione **HTTPS**. **Nota**: Se admite el uso de **HTTP** pero no se recomienda.

4. Seleccione **continuar**.
5. Especifique el modo de encuadernación.

   Utilice el ajuste **Global** (recomendado) o restrinja la accesibilidad de este punto final a uno de los siguientes puntos:

   - Interfaces de red específicas de nodos específicos.
   - Direcciones IP virtuales (VIP) de alta disponibilidad específica. Utilice esta selección solo si necesita niveles mucho más altos de aislamiento de las cargas de trabajo.
6. Seleccione **continuar**.
7. Seleccione **cargar certificado** (recomendado) y, a continuación, busque el certificado de servidor, la clave privada de certificado y el paquete opcional de CA.
8. 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.

Lo que necesitará

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

Acerca de esta tarea

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.

Se puede usar la misma cuenta de inquilino para varios clústeres de ONTAP. O bien, puede crear una cuenta de inquilino dedicada para cada clúster de ONTAP según sea necesario.

> En estas instrucciones se asume que ha configurado el inicio de sesión único (SSO) para Grid Manager. Si SSO no está habilitado, utilice estas instrucciones para crear una cuenta de inquilino en su lugar.

Pasos

1. Seleccione **ARRENDATARIOS**.
2. Seleccione **Crear**.
3. Introduzca un nombre para mostrar y una descripción.
4. Seleccione **S3**.
5. Deje en blanco el campo **cuota de almacenamiento**.
6. Seleccione **permitir servicios de plataforma** para permitir el uso de servicios de plataforma.

   Si se habilitan los servicios de plataforma, un inquilino puede usar características, como la replicación de CloudMirror, que accedan a servicios externos.

7. No seleccione **usar fuente de identidad propia**.
8. No seleccione **permitir selección de S3**.
9. Seleccione un grupo federado existente en el Gestor de grid para tener el permiso acceso raíz inicial para el arrendatario.
10. Seleccione **Crear arrendatario**.

Cree un bloque de S3 y obtenga una clave 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.

Lo que necesitará

- Creó una cuenta de inquilino para uso de FabricPool.

Acerca de esta tarea

Estas instrucciones describen cómo usar el responsable de inquilinos de StorageGRID para crear un bloque y obtener claves de acceso. También puede realizar estas tareas con la API de gestión de inquilinos o la API DE REST de StorageGRID S3. O bien, si utiliza ONTAP 9.10, puede crear el bloque con el asistente de configuración de FabricPool.

Si quiere más información:

- Usar una cuenta de inquilino
- Use S3

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 **ALMACENAMIENTO (S3)** > **Cuchos**.
   b. Seleccione **Crear cucharón**.
   c. Introduzca el nombre del bloque de StorageGRID que utilizará con FabricPool. Por ejemplo: `fabricpool-bucket`.

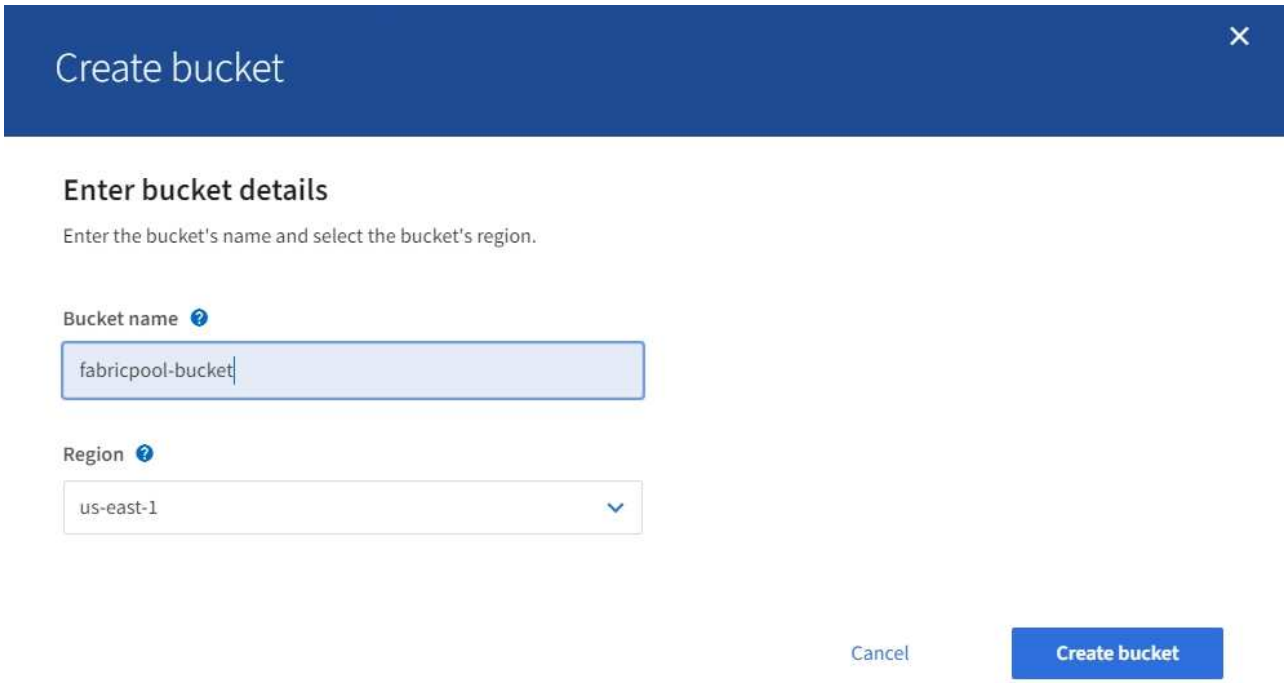
      No se puede cambiar el nombre del bloque después de crear el bloque.

      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.

   d. Seleccione la región para este segmento.

      De forma predeterminada, todos los bloques se crean en la `us-east-1` región.



e. Seleccione **Crear cucharón**.

> Para los depósitos FabricPool, el nivel de consistencia del cucharón recomendado es **Leer-después-nuevo-escribir**, que es la configuración predeterminada para un nuevo cucharón. No edite los depósitos de FabricPool para usar **Disponible** o cualquier otro nivel de consistencia.

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 crea una nueva clave de acceso y una clave de acceso secreta en el futuro, recuerde actualizar los valores correspondientes en ONTAP de inmediato para garantizar que ONTAP pueda almacenar y recuperar datos en StorageGRID sin interrupción.

Utilice la gestión del ciclo de vida de la información de StorageGRID con los datos de FabricPool

Si utiliza FabricPool para organizar los datos en niveles en StorageGRID, debe comprender los requisitos para la creación de reglas de la gestión del ciclo de vida de la información (ILM) de StorageGRID y una política de ILM para gestionar los datos de

FabricPool. Debe asegurarse de que las reglas de ILM que se aplican a los datos de FabricPool no sean disruptivas.

> 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. Consulte Gestión de objetos con ILM Para obtener instrucciones detalladas de ILM.

Revise estas directrices para asegurarse de que las reglas de ILM y la política de ILM sean adecuadas para los datos de FabricPool y los requisitos de su negocio. Si ya utiliza ILM de StorageGRID, es posible que deba actualizar la política de ILM activa para cumplir 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.

- No utilice 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 ILM como "para siempre" a fin de garantizar que la gestión del ciclo de vida de la información de StorageGRID no elimine los objetos de FabricPool.
- No cree reglas que muevan los datos de niveles de cloud de FabricPool fuera del bloque a otra ubicación. No se pueden utilizar reglas de ILM para archivar datos de FabricPool a cinta mediante un nodo de archivado o usar un pool de almacenamiento en cloud para mover datos de FabricPool a otro almacén de objetos.

  > 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.

Ejemplo de política de ILM para datos FabricPool

Use esta sencilla política de ejemplo como punto de partida para sus propias reglas y políticas 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 directiva, simule la política propuesta para confirmar que funcionará con el fin de proteger el contenido de las pérdidas. Para obtener más información, consulte Gestión de objetos con ILM.

Pasos

1. Cree un grupo de almacenamiento denominado **DEN**. Seleccione el sitio de Denver.
2. Cree un perfil de código de borrado denominado **2 más 1**. Seleccione el esquema de codificación de borrado 2+1 y el pool de almacenamiento **DEN**.
3. 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	2 más 1 codificación de borrado para datos de FabricPool
Nombre del bloque	`fabricpool-bucket` También puede filtrar en la cuenta de inquilino de FabricPool.
Filtrado avanzado	Tamaño de objeto (MB) superior a 0.2 MB. **Nota:** FabricPool sólo escribe objetos de 4 MB, pero debe agregar un filtro de tamaño de objeto porque esta regla usa código de borrado.
Tiempo de referencia	Tiempo de ingesta
Ubicación	Desde el día 0 almacenar para siempre
Tipo	Código de borrado
Ubicación	DEN (2 más 1)
Comportamiento de ingesta	Equilibrado

4. Cree una regla de ILM que cree dos copias replicadas de cualquier objeto que no coincida con la primera regla. No seleccione un filtro básico (nombre de cuenta de inquilino o de bloque) ni ningún filtro avanzado.

Definición de regla	Valor de ejemplo
Nombre de regla	Dos copias replicadas
Nombre del bloque	*none*
Filtrado avanzado	*none*

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Ubicación	Desde el día 0 almacenar para siempre
Tipo	Replicado
Ubicación	DEN
Snapshot	2
Comportamiento de ingesta	Equilibrado

5. Cree una política de ILM propuesta y seleccione las dos reglas. Como la regla de replicación no utiliza ningún filtro, puede ser la regla predeterminada (última) de la directiva.
6. Ingesta de objetos de prueba en el grid.
7. Simule la directiva con los objetos de prueba para verificar el comportamiento.
8. 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 mediante el esquema de codificación 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 replicadas y codificadas de borrado se mantendrán en StorageGRID hasta que el cliente S3 las elimine. El ILM de StorageGRID no eliminará nunca estos elementos.

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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso 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 tiene pensado organizar en niveles los datos de carga de trabajo primaria de FabricPool en StorageGRID, debe asegurarse de que la carga de trabajo de FabricPool tenga la mayor parte del 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.

- Como regla general, no debe imponer límites de calidad de servicio a ninguna carga de trabajo de FabricPool; solo debe limitar las otras 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.

Si quiere más información: Administrar directivas de clasificación de tráfico

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.
2. Introduzca un nombre y una descripción.
3. En la sección Reglas coincidentes, cree al menos una regla.
   a. Seleccione **Crear**.
   b. Seleccione **Endpoint** y seleccione el extremo del equilibrador de carga que ha creado para FabricPool.

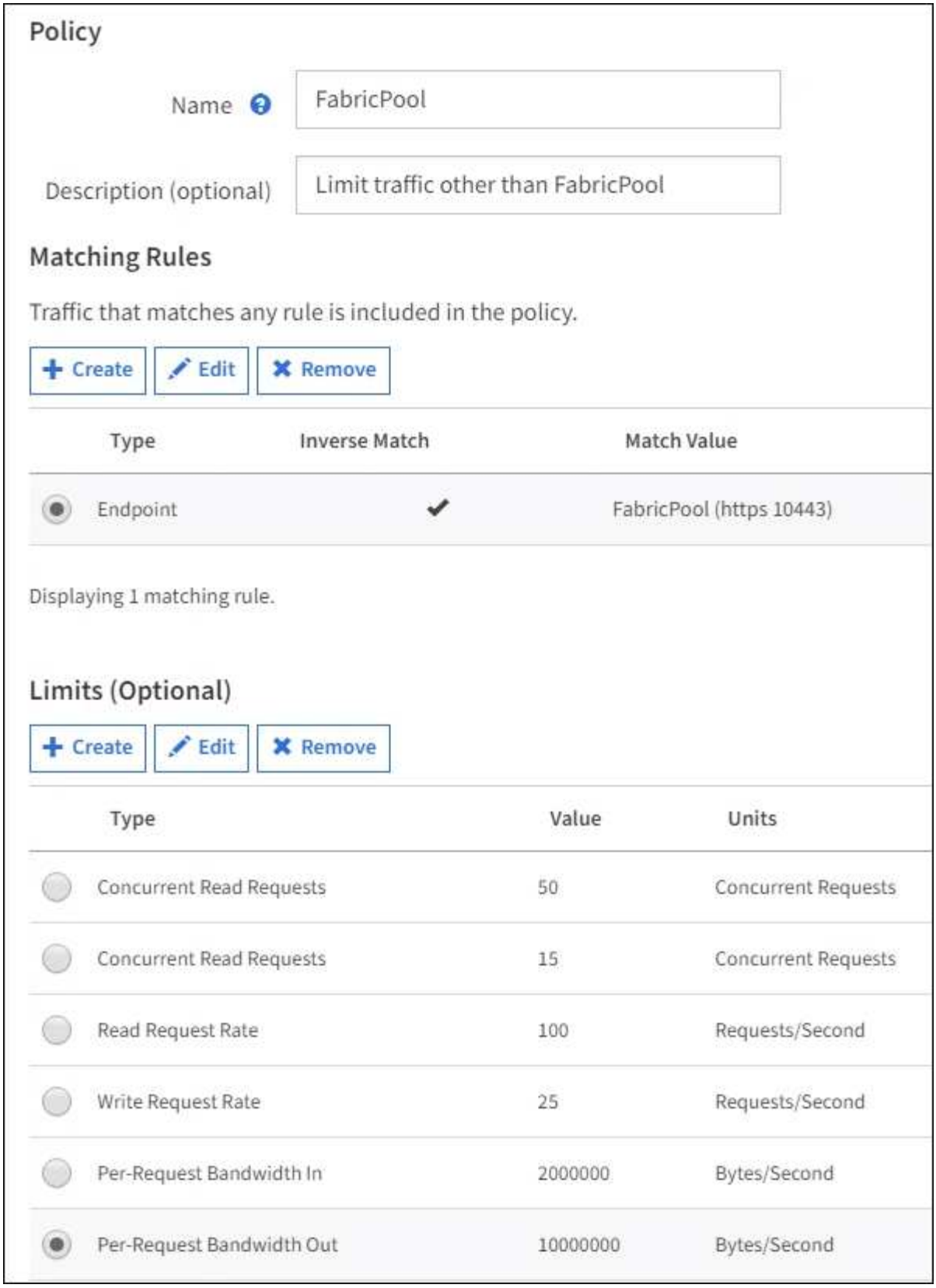
      También puede seleccionar la cuenta de inquilino o el bloque de FabricPool.

   c. Si desea que esta directiva de tráfico limite el tráfico de los otros puntos finales, seleccione **coincidencia inversa**.
4. Opcionalmente, cree uno o varios límites.

   > Aunque no se haya establecido ningún límite para una directiva de clasificación de tráfico, se recopilan las métricas para que pueda comprender las tendencias de tráfico.

   a. Seleccione **Crear**.
   b. Seleccione el tipo de tráfico que desea limitar y el límite que desea aplicar.

      En este ejemplo, la directiva de clasificación del tráfico FabricPool muestra los tipos de tráfico de red que puede limitar y los tipos de valores que puede seleccionar. Los límites de una política real se basarían en sus requisitos específicos.



5. Después de crear la directiva de clasificación de tráfico, seleccione la directiva y, a continuación, seleccione **métricas** para determinar si la directiva limita el tráfico como se espera.

Otras prácticas recomendadas para StorageGRID y FabricPool

Al configurar un sistema StorageGRID para utilizarlo con FabricPool, debe evitar establecer opciones globales que puedan afectar al modo en que se guardan los datos.

Cifrado de objetos

Al configurar StorageGRID, puede activar opcionalmente la configuración global **cifrado de objetos almacenados** si se requiere cifrado de datos para otros clientes StorageGRID (**CONFIGURATION** > **System** > **Opciones de cuadrícula**). 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 active el ajuste global **comprimir objetos almacenados** (**CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**). Los datos que se organizan en niveles de FabricPool a StorageGRID ya están comprimidos. La activación de **comprimir objetos almacenados** no reducirá aún más el tamaño de un objeto.

Nivel de coherencia

Para los depósitos FabricPool, el nivel de consistencia del cucharón recomendado es **Leer-después-nuevo-escribir**, que es la configuración predeterminada para un nuevo cucharón. No edite los depósitos de FabricPool para usar **Disponible** o cualquier otro nivel de consistencia.

Organización en niveles de FabricPool

Si el nodo StorageGRID utiliza almacenamiento asignado desde un sistema ONTAP de NetApp, confirme que el volumen no tiene habilitada la política de organización en niveles de FabricPool. 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.

Utilice 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.

Opcionalmente, las cuentas de arrendatarios 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 Instrucciones para implementar aplicaciones cliente de S3.

- **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 la siguiente información:

- Nombre para mostrar del arrendatario (el ID de cuenta del arrendatario se asigna automáticamente y no se puede modificar).
- Si la cuenta de inquilino usa S3 o Swift.
- Para las cuentas de inquilino de S3: Si la cuenta de inquilino está permitida para usar los servicios de la plataforma. Si se permite el uso de servicios de plataforma, la cuadrícula debe configurarse para que admita su uso.
- Opcionalmente, una cuota de almacenamiento para la cuenta de inquilino: El número máximo de gigabytes, terabytes o petabytes disponibles para los objetos del inquilino. La cuota de almacenamiento de un inquilino representa una cantidad lógica (tamaño de objeto), no una cantidad física (tamaño en disco).
- Si está habilitada la federación de identidades para el sistema StorageGRID, el grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.

- Si el sistema StorageGRID no utiliza el inicio de sesión único (SSO), tanto si la cuenta de inquilino usará su propio origen de identidad como si comparte el origen de identidad de la cuadrícula, así como la contraseña inicial del usuario raíz local del inquilino.

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 identidades se comparta con la cuadrícula) o crear grupos y usuarios locales
- Gestión de claves de acceso de S3
- Creación y gestión de bloques de S3, incluidos los bloques conformes a la normativa
- Uso de servicios de plataforma (si está activado)
- Supervisión del uso de almacenamiento

> Aunque puede crear y gestionar bloques de S3 con el administrador de inquilinos, debe tener Las claves de acceso S3 y use la API DE REST de S3 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 identidades se comparta con la cuadrícula) y crear grupos y usuarios locales
- Supervisión del uso de almacenamiento

> Los usuarios de Swift deben tener el permiso acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso acceso raíz no permite a los usuarios autenticarse 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.

Utilice el Administrador de arrendatarios

El Administrador de inquilinos le permite gestionar todos los aspectos de una cuenta de inquilino de StorageGRID.

Puede usar el Administrador de inquilinos para supervisar el uso del almacenamiento de una cuenta de inquilino y para gestionar los usuarios con federación de identidades o creando grupos y usuarios locales. En las cuentas de inquilinos S3, también se pueden gestionar claves S3, gestionar bloques S3 y configurar servicios de plataforma.

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.

Lo que necesitará

- Debe tener sus credenciales de inicio de sesión.
- Debe tener una dirección URL para acceder al Administrador de inquilinos, tal y como le ha suministrado 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 contiene el nombre de dominio completo (FQDN) o la dirección IP utilizada para acceder a un nodo de administrador, y también puede incluir, de manera opcional, un número de puerto, el ID de cuenta de inquilino de 20 dígitos o ambos.

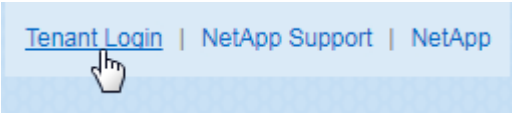
- Si la URL no incluye el ID de cuenta de 20 dígitos del inquilino, debe tener este ID de cuenta.
- Debe usar un navegador web compatible.
- Las cookies deben estar habilitadas en su navegador web.
- Debe tener permisos de acceso específicos.

Pasos

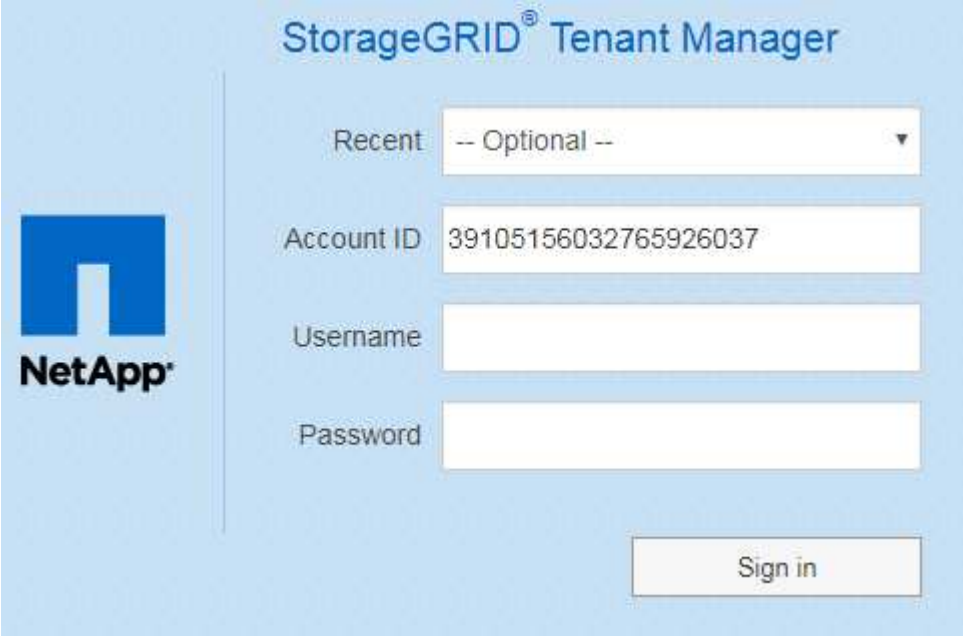
1. Inicie un navegador web compatible.
2. En la barra de dirección del navegador, introduzca la URL para acceder al Administrador de inquilinos.
3. Si se le solicita una alerta de seguridad, instale el certificado con el asistente de instalación del explorador.
4. Inicie sesión en el Administrador de inquilinos.

   La pantalla de inicio de sesión que ve depende de la dirección URL introducida y de si su empresa utiliza el inicio de sesión único (SSO). Verá una de las siguientes pantallas:

   - La página de inicio de sesión de Grid Manager. Haga clic en el enlace **Ingreso de inquilino** de la parte superior derecha.



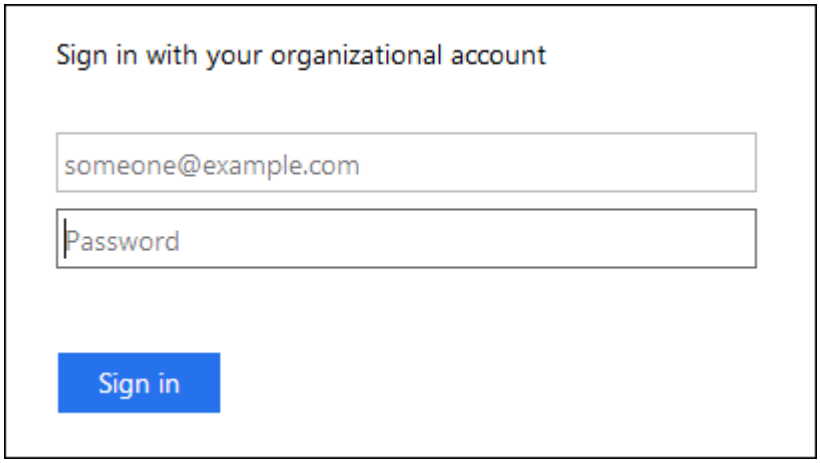
- La página de inicio de sesión del administrador de inquilinos. Es posible que el campo **ID de cuenta** ya esté completo, como se muestra a continuación.



  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. Haga clic en **Iniciar sesión**.

  Aparecerá la consola del administrador de inquilinos.

- Si el inicio de sesión único de su organización está habilitado en el grid. Por ejemplo:



Introduzca sus credenciales de SSO estándar y haga clic en **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. Haga clic en **Iniciar sesión**.

iii. Inicie sesión con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización.

Aparecerá la consola del administrador de inquilinos.

5. Si ha recibido una contraseña inicial de otra persona, cambie la contraseña para proteger su cuenta. Seleccione ***username*** > **Change Password**.

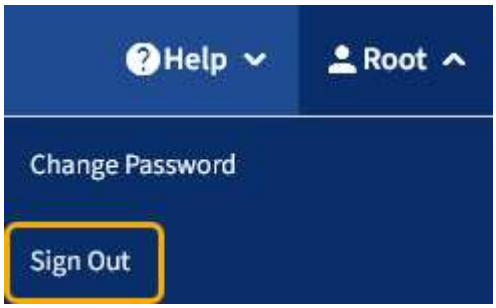
> Si SSO está habilitado para el sistema StorageGRID, no puede cambiar la contraseña del administrador de inquilinos.

Cierre la sesión del responsable de inquilinos

Una vez que haya terminado de trabajar con el Administrador de inquilinos, debe cerrar sesión para garantizar 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, a continuación, 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.

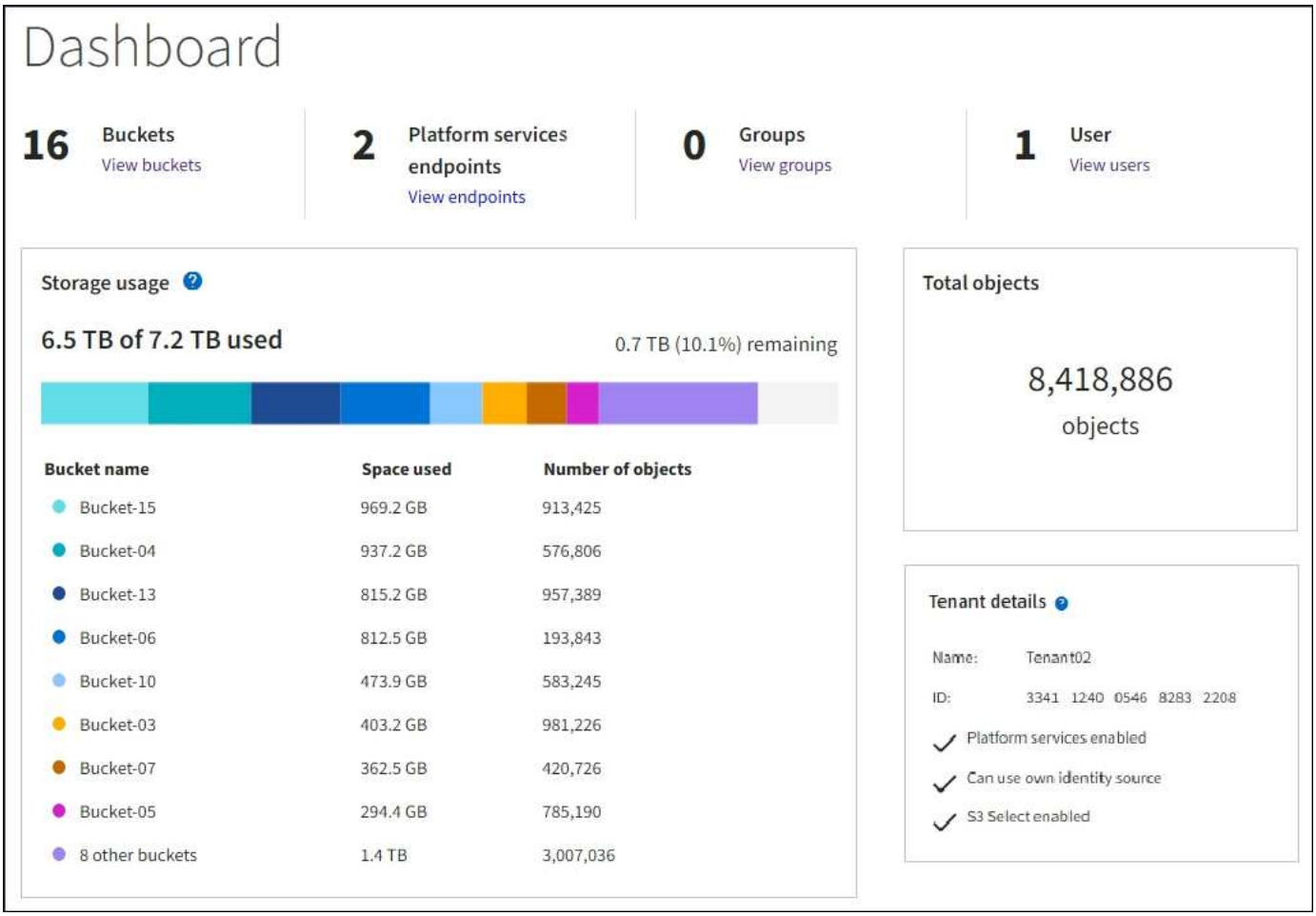
> Si SSO está activado y también ha iniciado sesión en Grid Manager, también debe cerrar sesión en Grid Manager para cerrar sesión en SSO.

Comprender la consola del administrador de inquilinos

La consola de tenant Manager proporciona una información general de la configuración de una cuenta de inquilino y la cantidad de espacio utilizado por los objetos en los bloques de inquilino (S3) o contenedores (Swift). Si el cliente tiene una cuota, en Dashboard se muestra cuánto de la cuota se usa y cuánto queda. Si hay algún error relacionado con la cuenta de inquilino, los errores se muestran en la consola.

> 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 cargan objetos, la consola se parece al siguiente ejemplo:



Resumen de la cuenta de inquilino

La parte superior de la consola 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 de la consola contiene la siguiente información:

- Número total de objetos para el arrendatario.

  Para una cuenta de S3, si no se han ingerido objetos y tiene el permiso de acceso raíz, se muestran las directrices de introducción 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, 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.

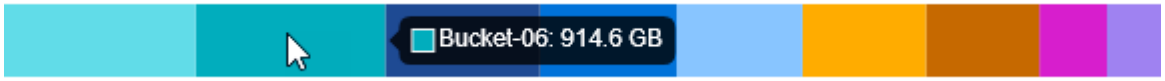
> Este valor indica la cantidad total de datos de objeto cargados y no representa el espacio utilizado para almacenar copias de esos objetos y sus metadatos.

- 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.

> 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.

- 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

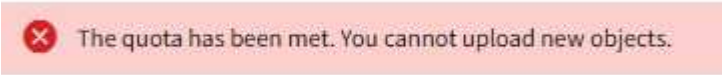
  Si el inquilino tiene más de nueve cubos o contenedores, el resto de cubos o contenedores se combinan en una sola entrada al final de la lista.

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**. Para obtener más información, consulte la referencia de alertas en las instrucciones para supervisar y solucionar problemas de StorageGRID.

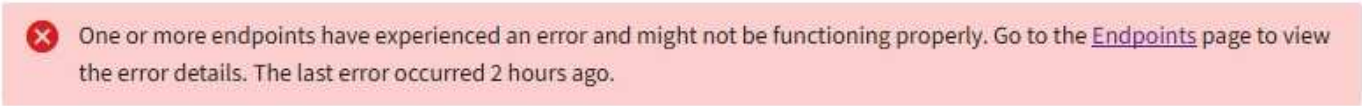
Si supera la cuota, no podrá cargar nuevos objetos.



> Para ver detalles adicionales y gestionar reglas y notificaciones para alertas, consulte las instrucciones para supervisar y solucionar problemas de StorageGRID.

Errores de punto final

Si ha utilizado Grid Manager para configurar uno o más extremos para utilizarlos con los servicios de la plataforma, el Panel de arrendatarios muestra una alerta si se han producido errores en los últimos siete días.



Para ver detalles sobre un error de punto final, seleccione endpoints para mostrar la página endpoints.

Información relacionada

Solucionar errores de extremos de servicios de plataforma

Supervisión y solución de problemas

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:

Pasos

1. Inicie sesión en el Administrador de inquilinos.
2. En la parte superior del Administrador de inquilinos, seleccione el icono de ayuda y seleccione **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 arrendatario actual, incluyendo 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 la versión del producto y las versiones de la API de Gestión de arrendatarios. Puede mostrar la versión de la versión del producto y las versiones principales de la API que admite esa versión.
- **Containers** — Operaciones en bloques de S3 o contenedores Swift, como se indica a continuación:

  S3

  - Crear bloque (con y sin S3 Object Lock habilitado)
  - Modificar la retención predeterminada de bloque (para bloques con bloqueo de objetos S3 habilitado)
  - Configure el control de coherencia para las operaciones realizadas en los objetos
  - Crear, actualizar y eliminar la configuración de CORS de un bloque
  - Activar y desactivar las actualizaciones de la hora de último acceso para los objetos
  - Gestionar la configuración de los servicios de plataforma, incluida la replicación de CloudMirror, las notificaciones y la integración de búsqueda (metadatos-notification)
  - Eliminar cubos vacíos

  Swift: Establece el nivel de consistencia utilizado para los contenedores

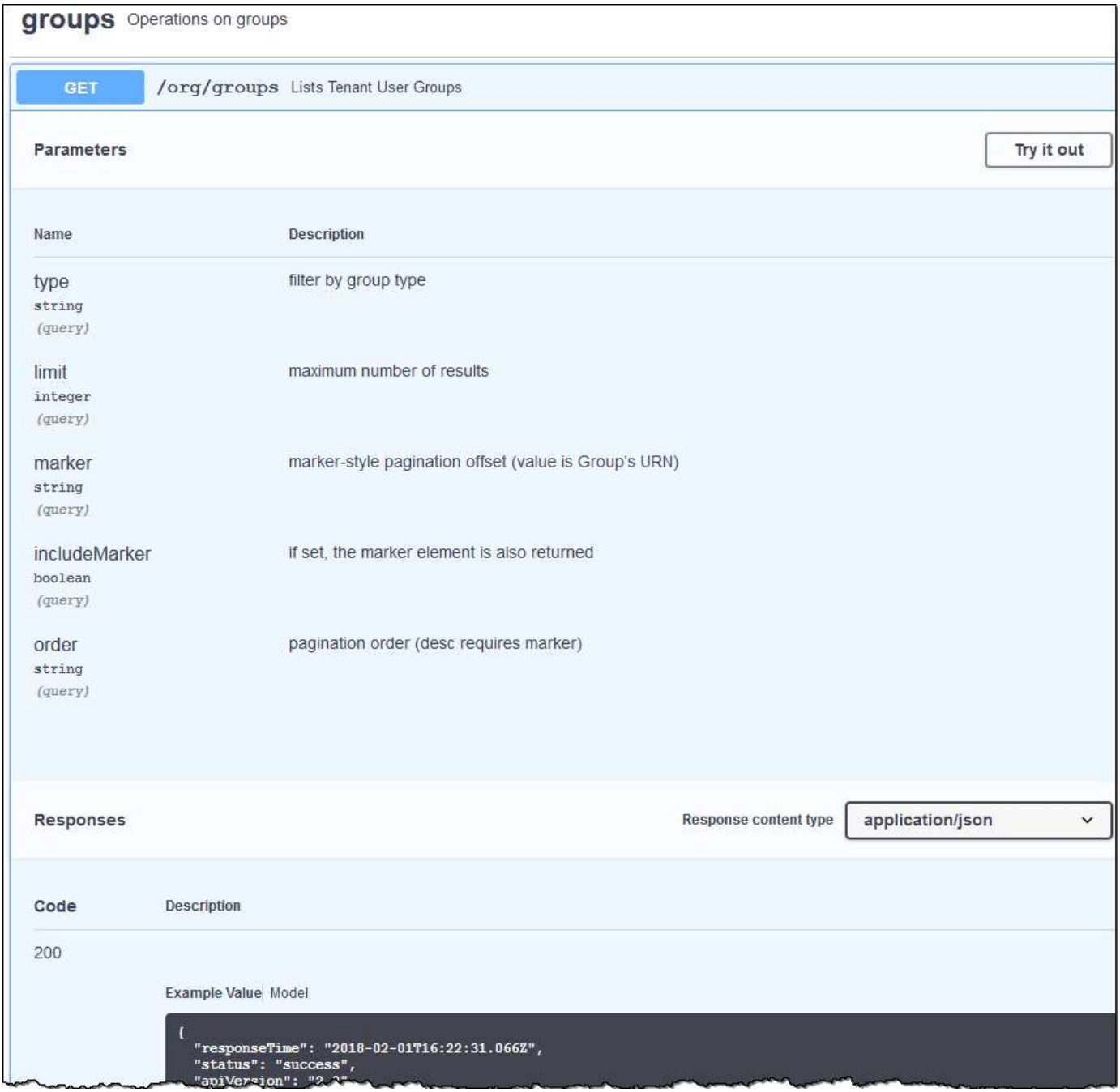
- **Características desactivadas** — Operaciones para ver las funciones que podrían haberse desactivado.
- **Endpoints** — Operaciones para administrar un punto final. Los extremos permiten que un bloque de S3

use un servicio externo para la replicación de CloudMirror de StorageGRID, notificaciones o integración de búsqueda.

- **Grupos** — Operaciones para administrar grupos de inquilinos locales y recuperar grupos de inquilinos federados de un origen de identidades externo.
- **Identity-source** — Operaciones para configurar un origen de identidad externo y sincronizar manualmente la información del grupo federado y del usuario.
- **Regiones** — Operaciones para determinar qué regiones se han configurado para el sistema StorageGRID.
- **s3** — Operaciones para administrar claves de acceso S3 para usuarios inquilinos.
- **s3-object-lock** — Operaciones en la configuración global de S3 Object Lock, que se utiliza para respaldar el cumplimiento normativo.
- **Usuarios** — Operaciones para ver y administrar usuarios de arrendatarios.

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 3 de la API.

```
https://hostname_or_ip_address/api/v3/authorize
```

La versión principal de la API de administración de arrendatarios se bONTAP cuando se realizan cambios que son ***no compatibles*** con versiones anteriores. La versión menor de la API de administración de arrendatarios se bONTAP cuando se hacen cambios que ***are sea compatible*** 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

Cuando el software StorageGRID se instala por primera vez, solo se habilita la versión más reciente de la API de gestión de inquilinos. Sin embargo, cuando StorageGRID se actualiza a una versión de función nueva, sigue teniendo acceso a la versión de API anterior para al menos una versión de la función StorageGRID.

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

Determine qué versiones de API son compatibles en la versión actual

Utilice la siguiente solicitud de API para devolver una lista de las versiones principales de API admitidas:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Especifique la versión de API para la solicitud

Puede especificar la versión de API mediante un parámetro path (`/api/v3`) o un encabezado (`Api-Version: 3`). Si proporciona ambos valores, el valor de encabezado anula el valor de ruta de acceso.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" 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 harán cumplir el `"Content-Type: application/json"` Encabezado para cualquier solicitud que espera un cuerpo de solicitud JSON como protección adicional contra ataques CSRF.

Gestione el acceso al sistema

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.

Lo que necesitará

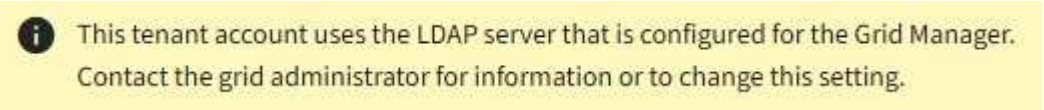
- Ha iniciado sesión en el administrador de inquilinos mediante un navegador web compatible.
- Tiene permisos de acceso específicos.
- Se utiliza Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidades.

> 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 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

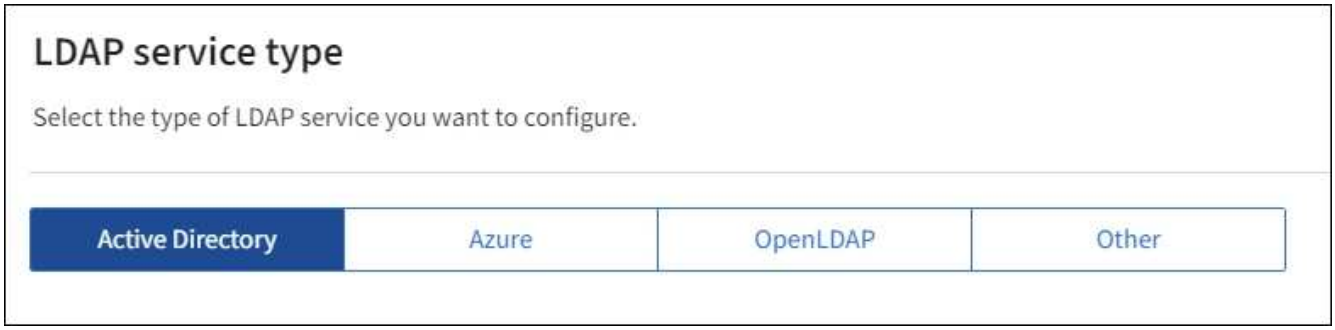
Si puede configurar un servicio de federación de identidades para su inquilino depende de cómo se haya configurado su cuenta de inquilino. Es posible que el inquilino comparta el servicio de federación de identidades configurado para Grid Manager. Si ve este mensaje al acceder a la página Federación de identidades, no podrá configurar un origen de identidad federado independiente para este arrendatario.



Introducir configuración

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.
   - **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 Bind** (opcional): El patrón de nombre de usuario predeterminado StorageGRID debe utilizar 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.

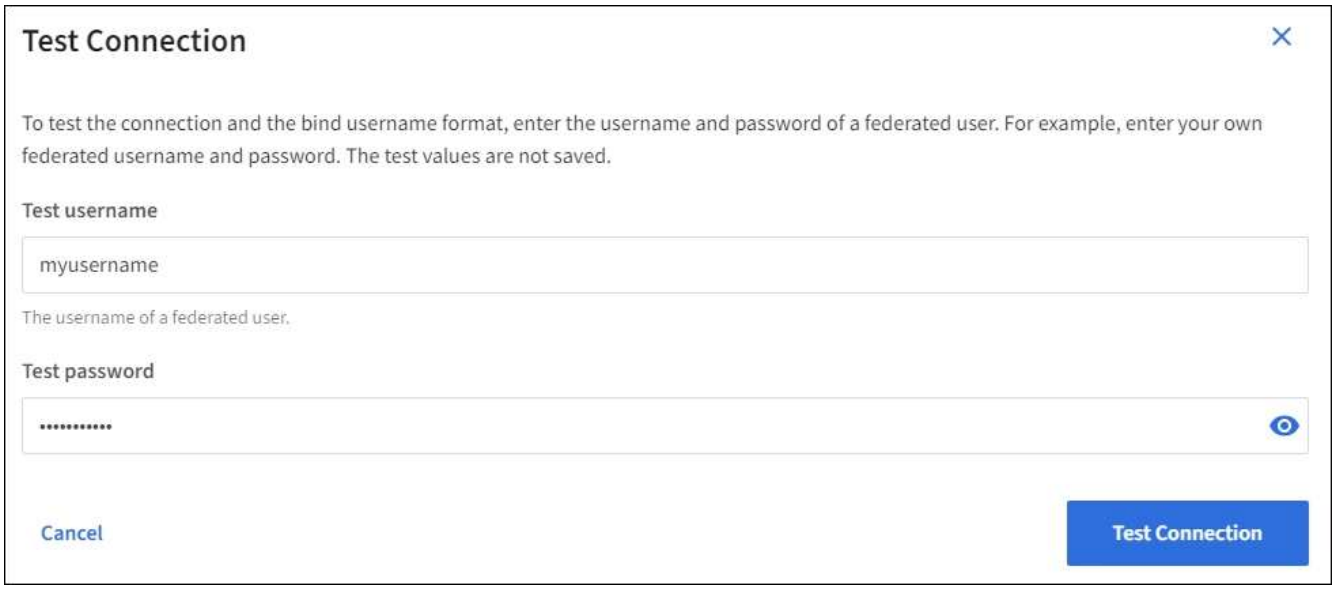
     Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto del certificado de CA.

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.

1. Seleccione **probar conexión**.
2. Si no se proporciona un formato de nombre de usuario de enlace:
   - Aparecerá el mensaje «"probar conexión correcta"» si los ajustes de conexión son válidos. Seleccione **Guardar** para guardar la configuración.
   - Aparece el mensaje «"no se ha podido establecer la conexión de prueba"» si los ajustes de conexión no son válidos. 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 /.



- Aparecerá el mensaje «"probar conexión correcta"» si los ajustes de conexión son válidos. 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 **Activar federación de identidades** está desactivada si el inicio de sesión único (SSO) está establecido en **activado** o **modo Sandbox**. 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. Desactive la casilla de verificación **Activar federación de identidades**.

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.

> Para los orígenes de identidad que no son 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 del usuario y quite el 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 enhttp://www.openldap.org/doc/admin24/index.html["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 lahttp://www.openldap.org/doc/admin24/index.html["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"^].

Gestionar grupos

Cree grupos para un inquilino de S3

Es posible gestionar permisos para grupos de usuarios S3 importando grupos federados

o creando grupos locales.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz. Consulte Permisos de gestión de inquilinos.
- Si planea importar un grupo federado, ha configurado la federación de identidades y el grupo federado ya existe en el origen de identidades configurado.

Para obtener más información sobre S3, consulte Use S3.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.

2. Seleccione **Crear grupo**.
3. 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.

4. 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.
5. Seleccione **continuar**.
6. Seleccione un modo de acceso. 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.

- **Read-write** (valor predeterminado): Los usuarios pueden iniciar sesión en el Administrador de inquilinos y administrar la configuración de arrendatario.
- **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden realizar cambios ni realizar ninguna operación en el Administrador de inquilinos ni en la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

7. Seleccione los permisos de grupo para este grupo.

   Consulte la información sobre los permisos de administración de inquilinos.

8. Seleccione **continuar**.
9. Seleccione una política de grupo para determinar qué permisos de acceso S3 tendrán los miembros de este grupo.
   - **Sin acceso S3**: Predeterminado. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que se conceda el acceso mediante una política de bloques. 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.
   - **Personalizado**: A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto. Consulte las instrucciones para implementar una aplicación cliente S3 para obtener información detallada acerca de las políticas de grupo, incluidos la sintaxis del idioma y ejemplos.
10. 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.

    En este ejemplo, sólo se permite a los miembros del grupo enumerar y acceder a una carpeta que coincida con su nombre de usuario (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.

11. Seleccione el botón que aparece, dependiendo de si está creando un grupo federado o un grupo local:
    - Grupo federado: **Crear grupo**
    - Grupo local: **Continuar**

    Si está creando un grupo local, el paso 4 (Agregar usuarios) aparece después de seleccionar **continuar**. Este paso no aparece para grupos federados.

12. Seleccione la casilla de verificación de cada usuario que desee agregar al grupo y, a continuación, seleccione **Crear grupo**.

    Opcionalmente, puede guardar el grupo sin agregar usuarios. Puede agregar usuarios al grupo más tarde o seleccionar el grupo cuando agregue nuevos usuarios.

13. Seleccione **Finalizar**.

    El grupo creado aparece en la lista de grupos. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

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.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.
- Si planea importar un grupo federado, ha configurado la federación de identidades y el grupo federado ya existe en el origen de identidades configurado.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.

2. Seleccione **Crear grupo**.
3. 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.

4. 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.
5. Seleccione **continuar**.
6. Seleccione un modo de acceso. 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.
   - **Read-write** (valor predeterminado): Los usuarios pueden iniciar sesión en el Administrador de inquilinos y administrar la configuración de arrendatario.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden realizar cambios ni

realizar ninguna operación en el Administrador de inquilinos ni en la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

7. Establezca el permiso Grupo.
   - Active la casilla de verificación **acceso raíz** si los usuarios necesitan iniciar sesión en el Administrador de inquilinos o la API de administración de inquilinos. (Predeterminado)
   - Anule la selección de la casilla de verificación **acceso raíz** si los usuarios no necesitan acceso al Administrador de inquilinos o a la API de administración de inquilinos. Por ejemplo, anule la selección de la casilla de verificación de las aplicaciones que no necesitan acceder al arrendatario. A continuación, asigne el permiso **Swift Administrator** para permitir que estos usuarios administren contenedores y objetos.
8. Seleccione **continuar**.
9. Active la casilla de verificación **Swift Administrator** si el usuario necesita poder utilizar la API de REST de Swift.

   Los usuarios de Swift deben tener el permiso acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso Root Access 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.

10. Seleccione el botón que aparece, dependiendo de si está creando un grupo federado o un grupo local:
    - Grupo federado: **Crear grupo**
    - Grupo local: **Continuar**

      Si está creando un grupo local, el paso 4 (Agregar usuarios) aparece después de seleccionar **continuar**. Este paso no aparece para grupos federados.

11. Seleccione la casilla de verificación de cada usuario que desee agregar al grupo y, a continuación, seleccione **Crear grupo**.

    Opcionalmente, puede guardar el grupo sin agregar usuarios. Puede agregar usuarios al grupo más tarde o seleccionar el grupo cuando cree nuevos usuarios.

12. Seleccione **Finalizar**.

    El grupo creado aparece en la lista de grupos. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

Permisos de gestión de inquilinos

Use Swift

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. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Permiso	Descripción
Acceso raíz	Proporciona acceso completo al administrador de inquilinos y a la API de gestión de inquilinos. **Nota:** los usuarios de Swift deben tener permiso acceso raíz para iniciar sesión en la cuenta de arrendatario.
Administrador	Solo para inquilinos Swift. Proporciona acceso completo a los contenedores y objetos de Swift para esta cuenta de inquilino **Nota:** los usuarios de Swift deben tener el permiso de Administrador de Swift para realizar cualquier operación con la API de REST de Swift.
Gestione sus propias credenciales de S3	Solo inquilinos 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**.
Administrar todos los depósitos	• Inquilinos S3: Permite a los usuarios usar el administrador de inquilinos y la API de gestión de inquilinos para crear y eliminar bloques S3, así como para gestionar la configuración de todos los bloques de S3 de la cuenta del inquilino, independientemente de las políticas de grupo o bloque de S3. Los usuarios que no tienen este permiso no ven la opción de menú **Cuchos**. • Inquilinos Swift: Permite a los usuarios de Swift controlar el nivel de coherencia de los contenedores Swift mediante la API de gestión de inquilinos. **Nota:** sólo puede asignar el permiso Administrar todos los cucharones a grupos Swift desde la API de gestión de inquilinos. No puede asignar este permiso a grupos Swift mediante el administrador de inquilinos.

Permiso	Descripción
Gestionar extremos	Solo inquilinos de S3. Permite a los usuarios usar el administrador de inquilinos o la API de gestión de inquilinos crear o editar extremos que se usan como destino de los servicios de plataforma StorageGRID. Los usuarios que no tienen este permiso no ven la opción de menú **terminales de servicios de plataforma**.

Información relacionada

Use S3

Use Swift

Ver y editar detalles del grupo

Al ver los detalles de un grupo, puede cambiar el nombre para mostrar del grupo, los permisos, las directivas y los usuarios que pertenecen al grupo.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione el nombre del grupo cuyos detalles desee ver o editar.

   También puede seleccionar **acciones** > **Ver detalles del grupo**.

   Aparece la página de detalles del grupo. En el siguiente ejemplo, se muestra la página de detalles del grupo S3.

Groups > Applications

Overview

Display name:	**Applications**
Unique name:	**group/Applications**
Type:	**Local**
Access mode:	**Read-write**
Permissions:	**Root Access**
S3 Policy:	**None**
Number of users in this group:	**0**

Group permissions | S3 group policy | Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

(●) Read-write ( ) Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

[x] **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

[x] **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

[x] **Manage Endpoints**

Allows users to configure endpoints for platform services.

[x] **Manage Your Own S3 Credentials**

Allows users to create and delete their own S3 access keys.

Save changes

3. Realice cambios en la configuración del grupo según sea necesario.

> Para asegurarse de que se guardan los cambios, seleccione **Guardar cambios** después de realizar cambios en cada sección. Cuando se guarden los cambios, aparecerá un mensaje de confirmación en la esquina superior derecha de la página.

   a. De forma opcional, seleccione el nombre para mostrar o el icono de edición para actualizar el nombre para mostrar.

      No se puede cambiar el nombre exclusivo de un grupo. No se puede editar el nombre para mostrar de un grupo federado.

   b. Si lo desea, actualice los permisos.

   c. Para la política de grupo, realice los cambios adecuados para su inquilino S3 o Swift.

      - Si va a editar un grupo para un inquilino de S3, seleccione de forma opcional una política de grupo S3 diferente. Si selecciona una política de S3 personalizada, actualice la cadena JSON según sea necesario.
      - Si está editando un grupo para un inquilino Swift, también puede activar o desactivar la casilla de verificación **Swift Administrator**.

        Para obtener más información sobre el permiso de administrador de Swift, consulte las instrucciones para crear grupos para un inquilino Swift.

   d. Opcionalmente, agregue o elimine usuarios.

4. Confirme que ha seleccionado **Guardar cambios** para cada sección que haya cambiado.

   Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

Cree grupos para el inquilino de S3

Cree grupos para el inquilino Swift

Agregar usuarios a un grupo local

Puede agregar usuarios a un grupo local según sea necesario.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione el nombre del grupo local al que desea añadir usuarios.

   También puede seleccionar **acciones** > **Ver detalles del grupo**.

   Aparece la página de detalles del grupo.

Groups > Applications

Overview

Display name:	**Applications**
Unique name:	**group/Applications**
Type:	**Local**
Access mode:	**Read-write**
Permissions:	**Root Access**
S3 Policy:	**None**
Number of users in this group:	**0**

Group permissions | S3 group policy | Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

(●) Read-write ( ) Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

[x] **Root Access**

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

[x] **Manage All Buckets**

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

[x] **Manage Endpoints**

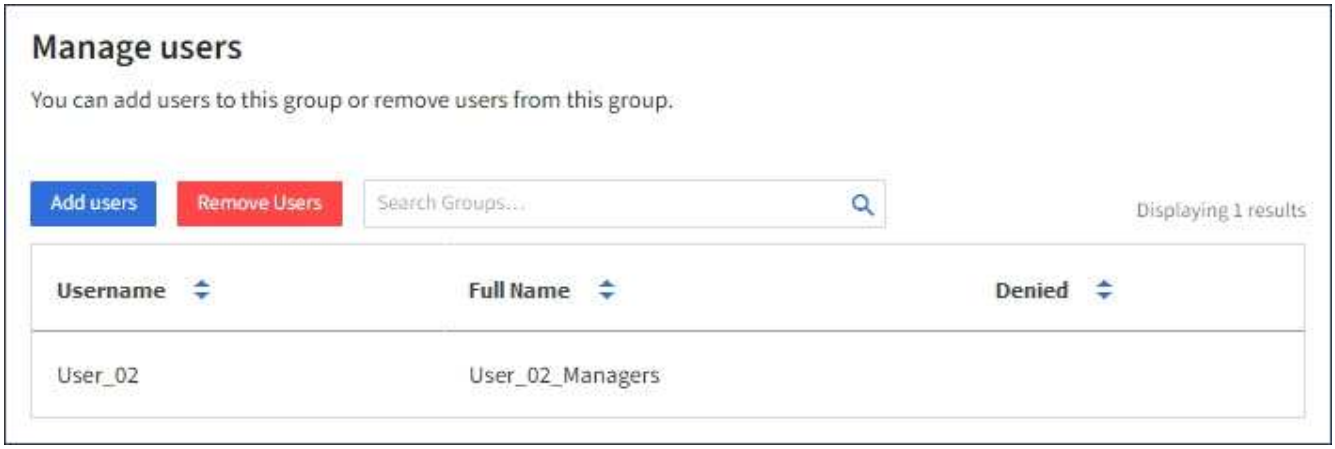
Allows users to configure endpoints for platform services.

[x] **Manage Your Own S3 Credentials**

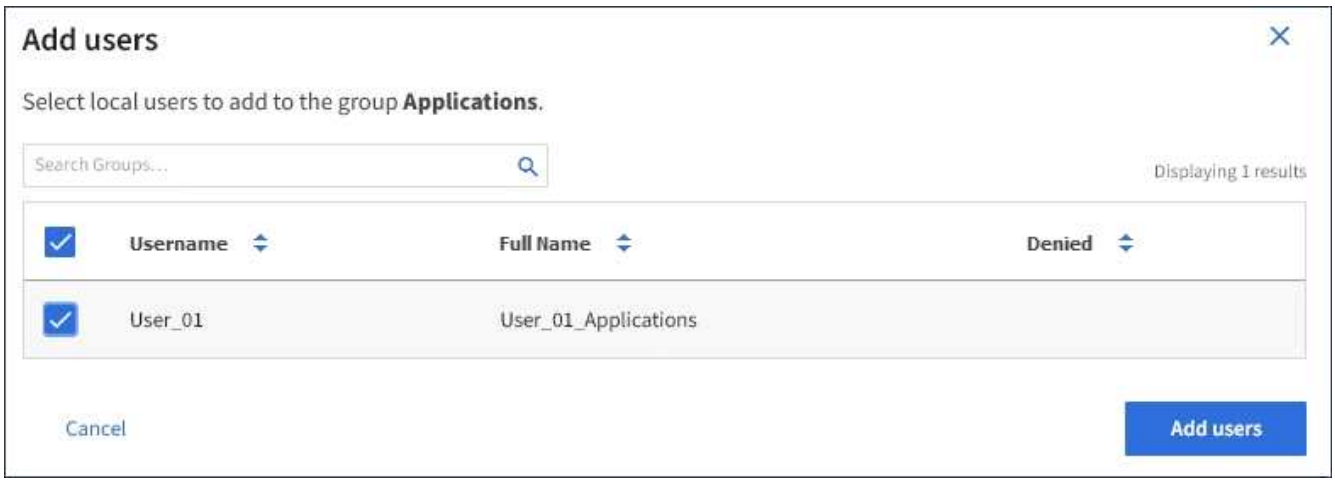
Allows users to create and delete their own S3 access keys.

Save changes

3. Seleccione **usuarios** y, a continuación, seleccione **Agregar usuarios**.



4. Seleccione los usuarios que desea agregar al grupo y, a continuación, seleccione **Agregar usuarios**.



Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Editar el nombre del grupo

Puede editar el nombre para mostrar de un grupo. No se puede editar el nombre único de un grupo.

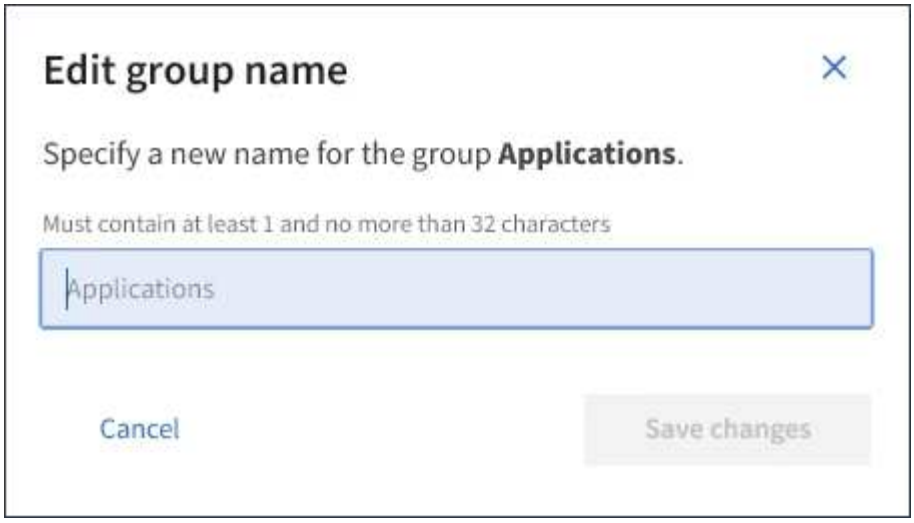
Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz. Consulte Permisos de gestión de inquilinos.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de verificación del grupo cuyo nombre para mostrar desee editar.
3. Seleccione **acciones** > **Editar nombre de grupo**.

   Aparece el cuadro de diálogo Editar nombre del grupo.



4. Si está editando un grupo local, actualice el nombre para mostrar según sea necesario.

   No se puede cambiar el nombre exclusivo de un grupo. No se puede editar el nombre para mostrar de un grupo federado.

5. Seleccione **Guardar cambios**.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Grupo duplicado

Puede crear nuevos grupos más rápidamente duplicando un grupo existente.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz. Consulte Permisos de gestión de inquilinos.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de verificación del grupo que desea duplicar.
3. Seleccione **Duplicar grupo**. Para obtener más información sobre cómo crear un grupo, consulte las instrucciones para crear grupos Un inquilino de S3 o para Un inquilino de Swift.
4. 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 activado 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 usar las aplicaciones cliente para gestionar los recursos del inquilino, basado en permisos de grupo.

5. 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.

6. Seleccione **continuar**.
7. Según sea necesario, modifique los permisos para este grupo.
8. Seleccione **continuar**.
9. Según sea necesario, si va a duplicar un grupo para un inquilino S3, seleccione opcionalmente una directiva diferente de los botones de opción * Agregar directiva S3*. Si seleccionó una política personalizada, actualice la cadena JSON como sea necesario.
10. Seleccione **Crear grupo**.

Eliminar grupo

Puede eliminar un grupo del sistema. Cualquier usuario que sólo pertenezca a ese grupo ya no podrá iniciar sesión en el Administrador de inquilinos ni utilizar la cuenta de arrendatario.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso acceso raíz. Consulte Permisos de gestión de inquilinos.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.

2. Seleccione las casillas de verificación de los grupos que desea eliminar.
3. Seleccione **acciones** > **Eliminar grupo**.

   Aparecerá un mensaje de confirmación.

4. Seleccione **Eliminar grupo** para confirmar que desea eliminar los grupos indicados en el mensaje de confirmación.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Gestionar usuarios locales

Puede crear usuarios locales y asignarles grupos locales para determinar las funciones a las que pueden acceder estos usuarios. El Administrador de arrendatarios incluye un usuario local predefinido denominado «'root'». Aunque puede agregar y quitar usuarios locales, no puede quitar el usuario raíz.

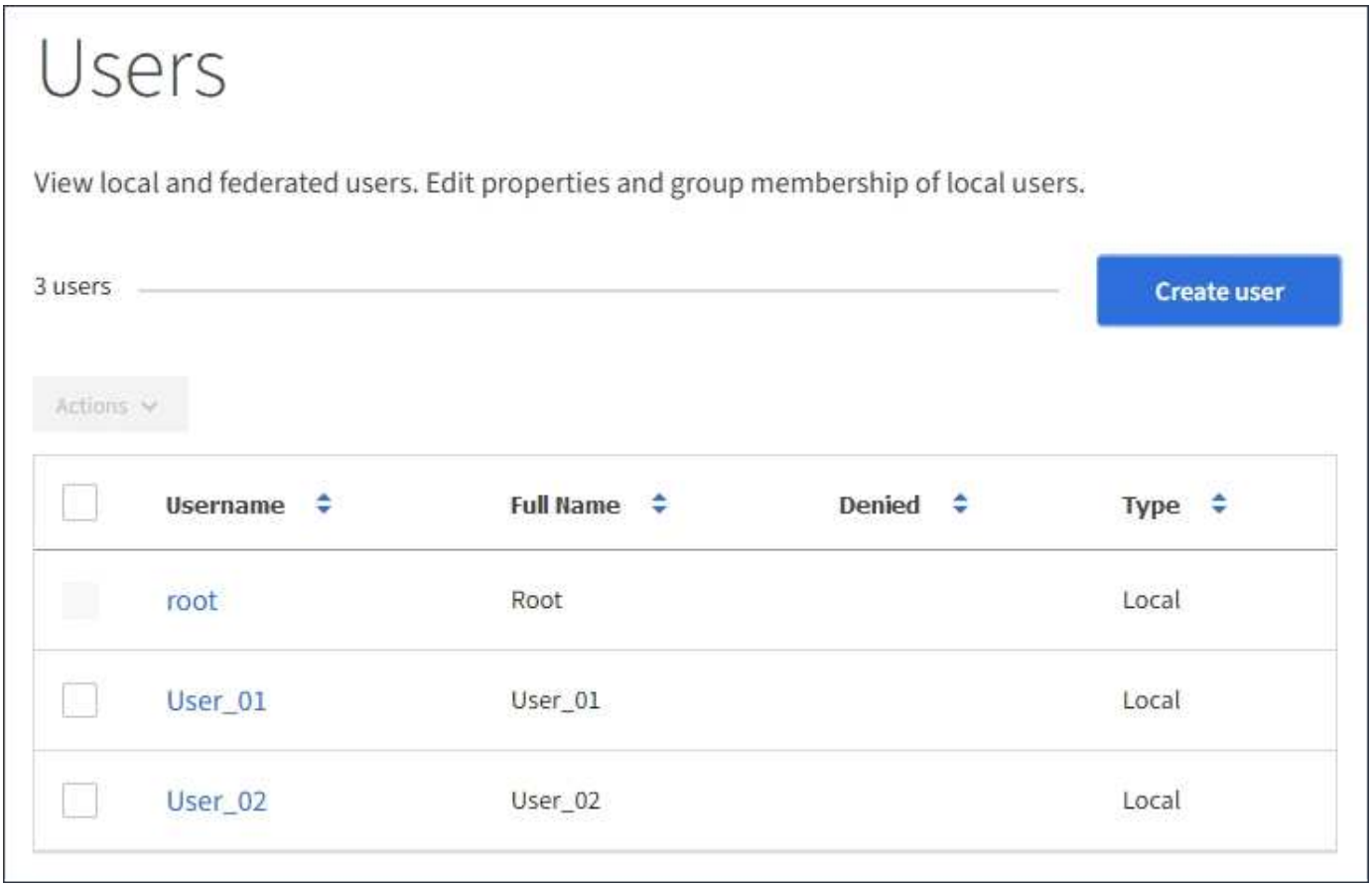
Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios de lectura y escritura que tenga el permiso acceso raíz. Consulte Permisos de gestión de inquilinos.

> Si se habilitó el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el administrador de inquilinos o la API de gestión de inquilinos, aunque puedan usar las aplicaciones cliente S3 o Swift para acceder a los recursos del inquilino, en función de los permisos de grupo.

Acceder a la página usuarios

Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.



Crear usuarios locales

Es posible crear usuarios locales y asignarles 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 gestión ni políticas de grupo S3 aplicadas. 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 pertenecen a ningún grupo no tienen permisos de gestión ni acceso al contenedor de Swift.

Pasos

1. Seleccione **Crear usuario**.
2. Complete los siguientes campos.
   - **Nombre completo**: El nombre completo de este usuario, por ejemplo, el nombre y apellido de una persona o el nombre de una aplicación.
   - **Nombre de usuario**: El nombre que este usuario utilizará para iniciar sesión. Los nombres de usuario deben ser únicos y no se pueden cambiar.
   - **Contraseña**: Contraseña que se utiliza cuando el usuario inicia sesión.
   - **Confirmar contraseña**: Escriba la misma contraseña que escribió en el campo Contraseña.
   - **Denegar acceso**: Si selecciona **Sí**, este usuario no puede iniciar sesión en la cuenta de arrendatario, aunque el usuario pueda seguir perteneciendo a uno o más grupos.

     Por ejemplo, puede utilizar esta función para suspender temporalmente la capacidad de un usuario

para iniciar sesión.

3. Seleccione **continuar**.
4. Asigne el usuario a uno o más grupos locales.

   Los usuarios que no pertenecen 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.

5. Seleccione **Crear usuario**.

   Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Edite los detalles del usuario

Al editar los detalles de un usuario, puede cambiar el nombre completo y la contraseña del usuario, agregar el usuario a grupos diferentes e impedir que el usuario acceda al arrendatario.

Pasos

1. En la lista usuarios, seleccione el nombre del usuario cuyos detalles desee ver o editar.

   Como alternativa, puede seleccionar la casilla de verificación para el usuario y, a continuación, seleccionar **acciones** > **Ver detalles del usuario**.

2. Realice los cambios necesarios en la configuración del usuario.
   a. Cambie el nombre completo del usuario según sea necesario seleccionando el nombre completo o el icono de edición En la sección Descripción general.

      No puede cambiar el nombre de usuario.

   b. En la ficha **Contraseña**, cambie la contraseña del usuario según sea necesario.
   c. En la ficha **Access**, permita que el usuario inicie sesión (seleccione **no**) o impida que el usuario inicie sesión (seleccione **Sí**) según sea necesario.
   d. En la ficha **grupos**, agregue el usuario a grupos o elimine el usuario de los grupos según sea necesario.
   e. Según sea necesario para cada sección, seleccione **Guardar cambios**.

      Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Duplique los usuarios locales

Puede duplicar un usuario local para crear un usuario nuevo más rápidamente.

Pasos

1. En la lista usuarios, seleccione el usuario que desea duplicar.
2. Seleccione **Duplicar usuario**.
3. Modifique los campos siguientes para el nuevo usuario.
   - **Nombre completo**: El nombre completo de este usuario, por ejemplo, el nombre y apellido de una persona o el nombre de una aplicación.
   - **Nombre de usuario**: El nombre que este usuario utilizará para iniciar sesión. Los nombres de usuario deben ser únicos y no se pueden cambiar.

- **Contraseña**: Contraseña que se utiliza cuando el usuario inicia sesión.
- **Confirmar contraseña**: Escriba la misma contraseña que escribió en el campo Contraseña.
- **Denegar acceso**: Si selecciona **Sí**, este usuario no puede iniciar sesión en la cuenta de arrendatario, aunque el usuario pueda seguir perteneciendo a uno o más grupos.

  Por ejemplo, puede utilizar esta función para suspender temporalmente la capacidad de un usuario para iniciar sesión.

4. Seleccione **continuar**.
5. Seleccione uno o más grupos locales.

   Los usuarios que no pertenecen 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.

6. Seleccione **Crear usuario**.

   Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Eliminar usuarios locales

Es posible eliminar de forma permanente usuarios locales que ya no necesiten acceder a la cuenta de inquilino de StorageGRID.

Con el Administrador de inquilinos, puede eliminar usuarios locales, pero no usuarios federados. Debe utilizar el origen de identidad federado para eliminar usuarios federados.

Pasos

1. En la lista usuarios, seleccione la casilla de verificación del usuario local que desea eliminar.
2. Seleccione **acciones** > **Eliminar usuario**.
3. En el cuadro de diálogo de confirmación, seleccione **Eliminar usuario** para confirmar que desea eliminar al usuario del sistema.

   Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Gestione cuentas de inquilinos S3

Gestión de claves de acceso de S3

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.

Acerca de esta tarea

Las claves de acceso S3 se pueden gestionar de la siguiente manera:

- Los usuarios que tengan el permiso **Administrar sus propias credenciales de S3** pueden crear o quitar sus propias claves de acceso S3.
- Los usuarios que tienen el permiso **acceso raíz** pueden administrar las claves de acceso para la cuenta raíz de S3 y el resto de 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 bloques y los objetos de la cuenta de inquilino de S3.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe tener el permiso gestionar sus propias credenciales de S3. Consulte Permisos de gestión de inquilinos.

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 motivos de seguridad, no cree más claves de las necesarias y elimine las claves que no esté 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 para la seguridad en su entorno es bajo y no necesita crear nuevas claves periódicamente, no tendrá que establecer un tiempo de caducidad para sus claves. Si decide más tarde crear claves nuevas, elimine manualmente las claves antiguas.

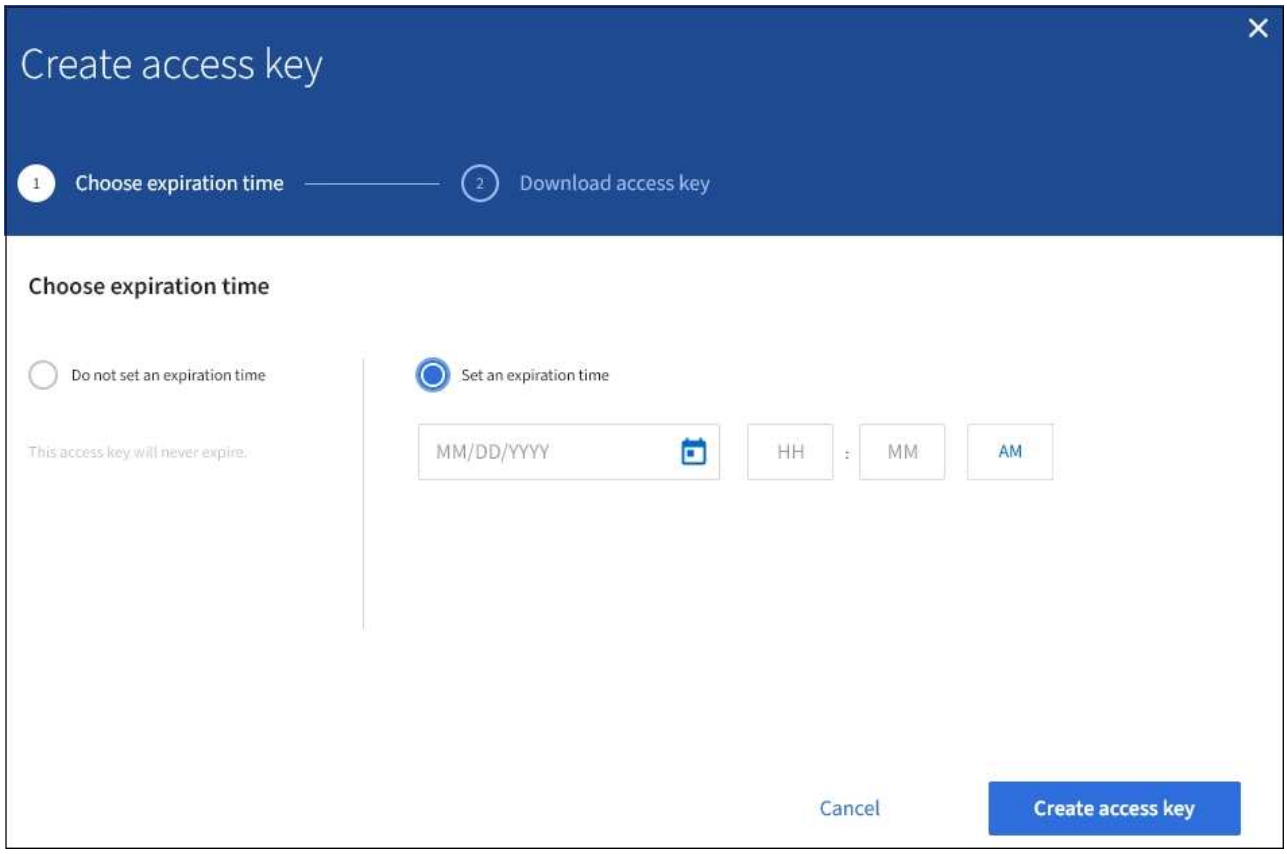
> Puede acceder a los bloques y los objetos de S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestra para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves 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.

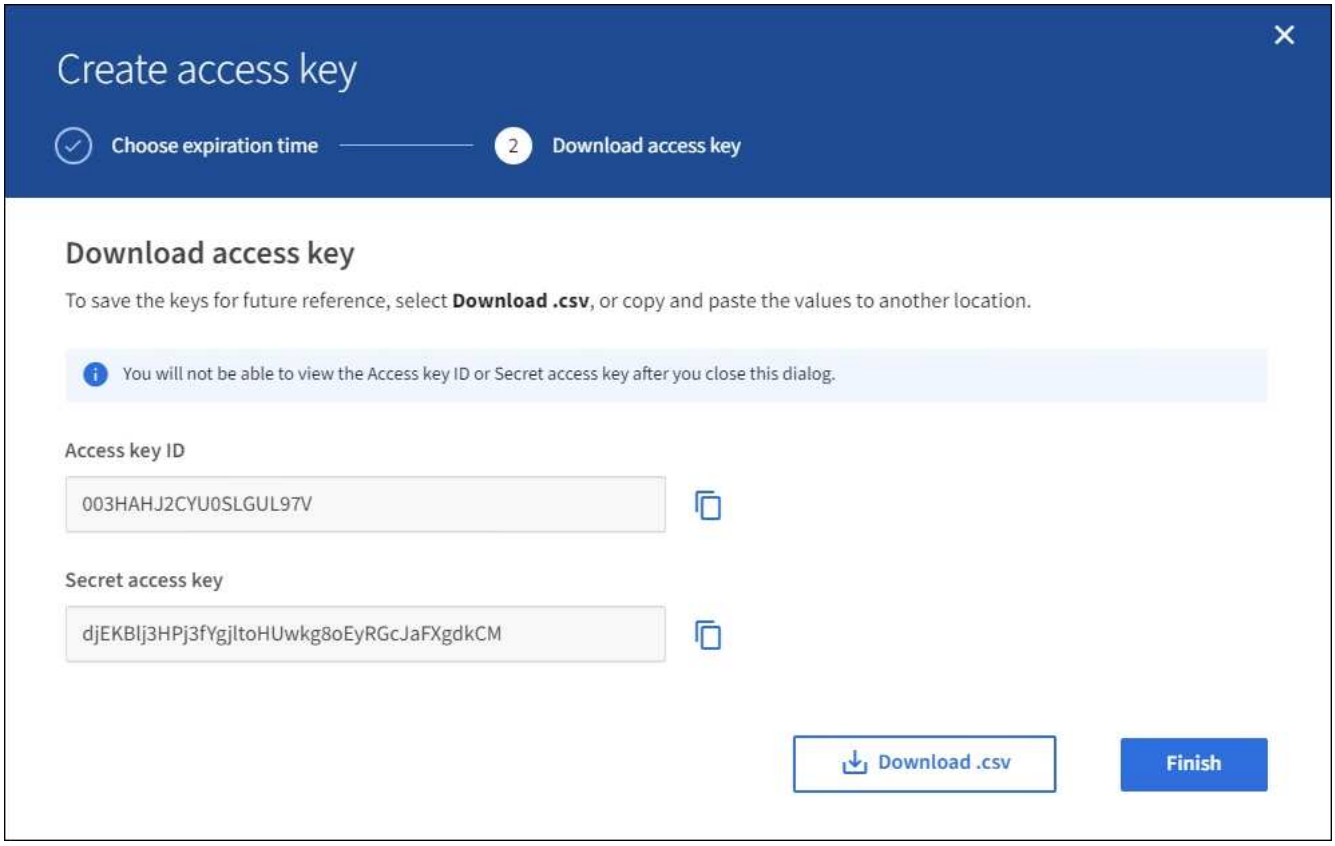


4. Seleccione **Crear clave de acceso**.

   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. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Consulte las claves de acceso de S3

Si usa un inquilino de S3 y tiene el permiso correspondiente, puede ver una lista de sus claves de acceso S3. Puede ordenar la lista por tiempo de caducidad, de modo que puede determinar qué claves caducarán pronto. Según sea necesario, puede crear nuevas claves o eliminar claves que ya no utilice.

Lo que necesitará

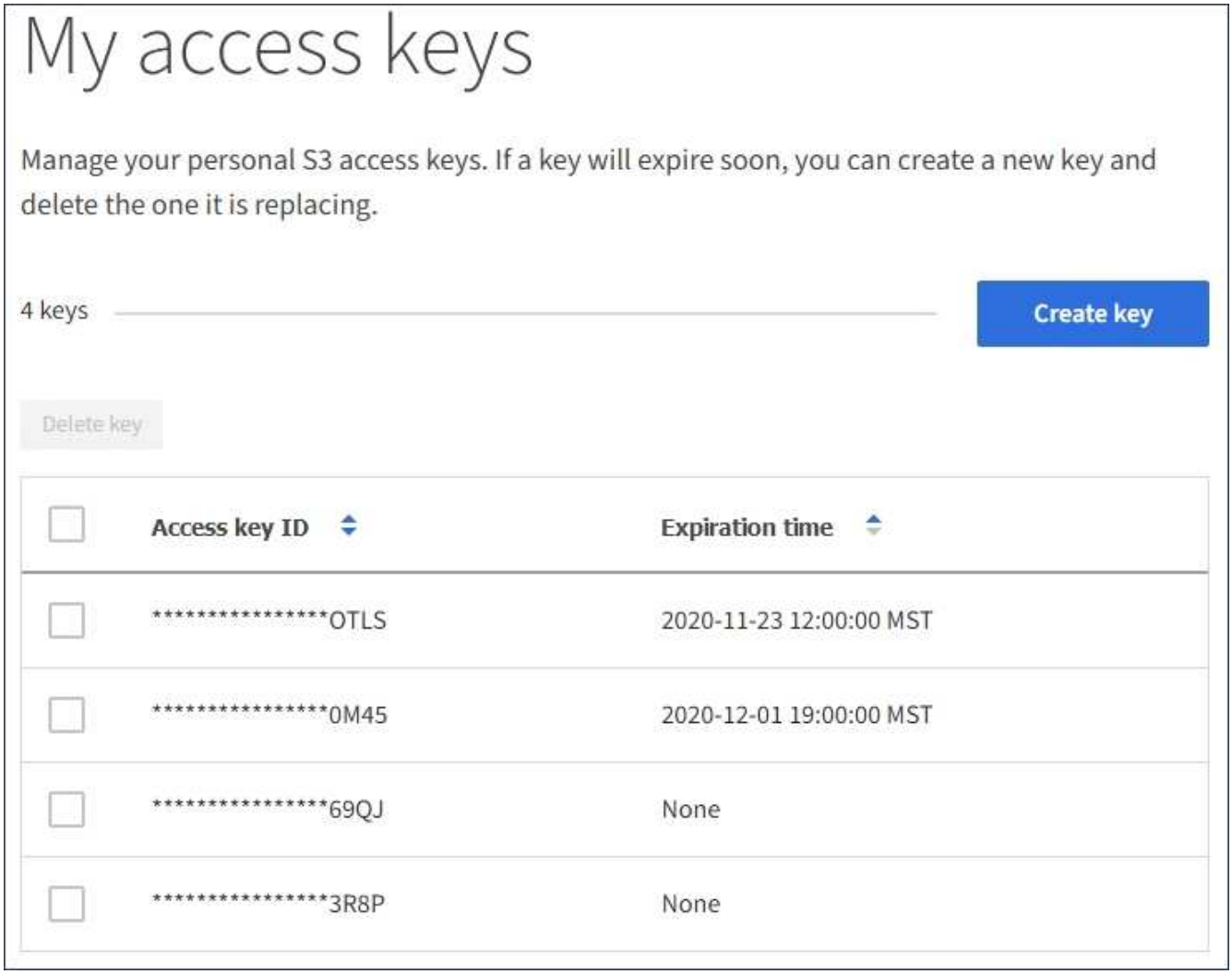
- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe tener el permiso gestionar sus propias credenciales de S3.

> 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**.

   Aparecerá la página Mis claves de acceso y mostrará una lista de las claves de acceso existentes.



2. Ordene las teclas por **tiempo de caducidad** o **ID de clave de acceso**.
3. Según sea necesario, cree nuevas claves y elimine manualmente las claves que ya no utilice.

   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.

Información relacionada

Cree sus propias claves de acceso S3

Elimine sus propias claves de acceso de S3

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.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.

- Debe tener el permiso gestionar sus propias credenciales de S3. Consulte Permisos de gestión de inquilinos.

> 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.

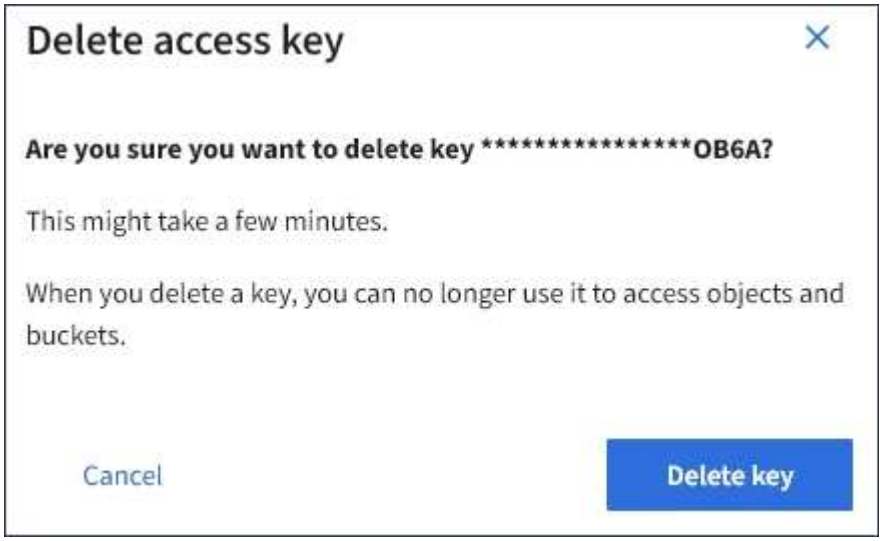
Pasos

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 la casilla de comprobación de cada clave de acceso que desea quitar.
3. Seleccione **tecla Eliminar**.

   Se muestra un cuadro de diálogo de confirmación.



4. Seleccione **tecla Eliminar**.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

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.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe tener el permiso 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 motivos de seguridad, no cree más claves de las que necesita el usuario y elimine las claves que no se estén 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 para la seguridad en su entorno es bajo y no necesita crear nuevas claves periódicamente, no tendrá que establecer un tiempo de caducidad para las claves. Si decide más tarde crear claves nuevas, elimine manualmente las claves antiguas.

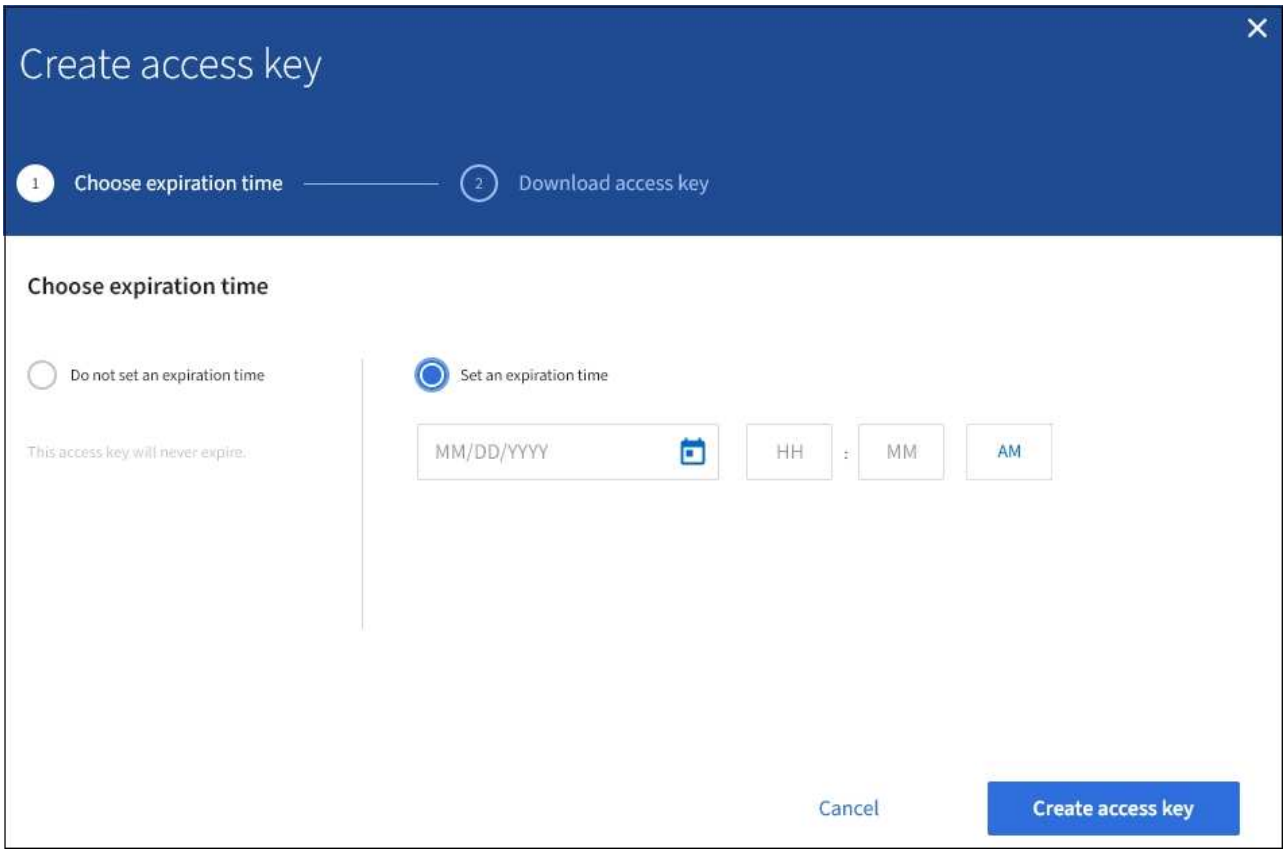
> Es posible acceder a los bloques y los objetos de S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta mostrada para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Gire las claves 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:
   - Seleccione **no establezca 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.

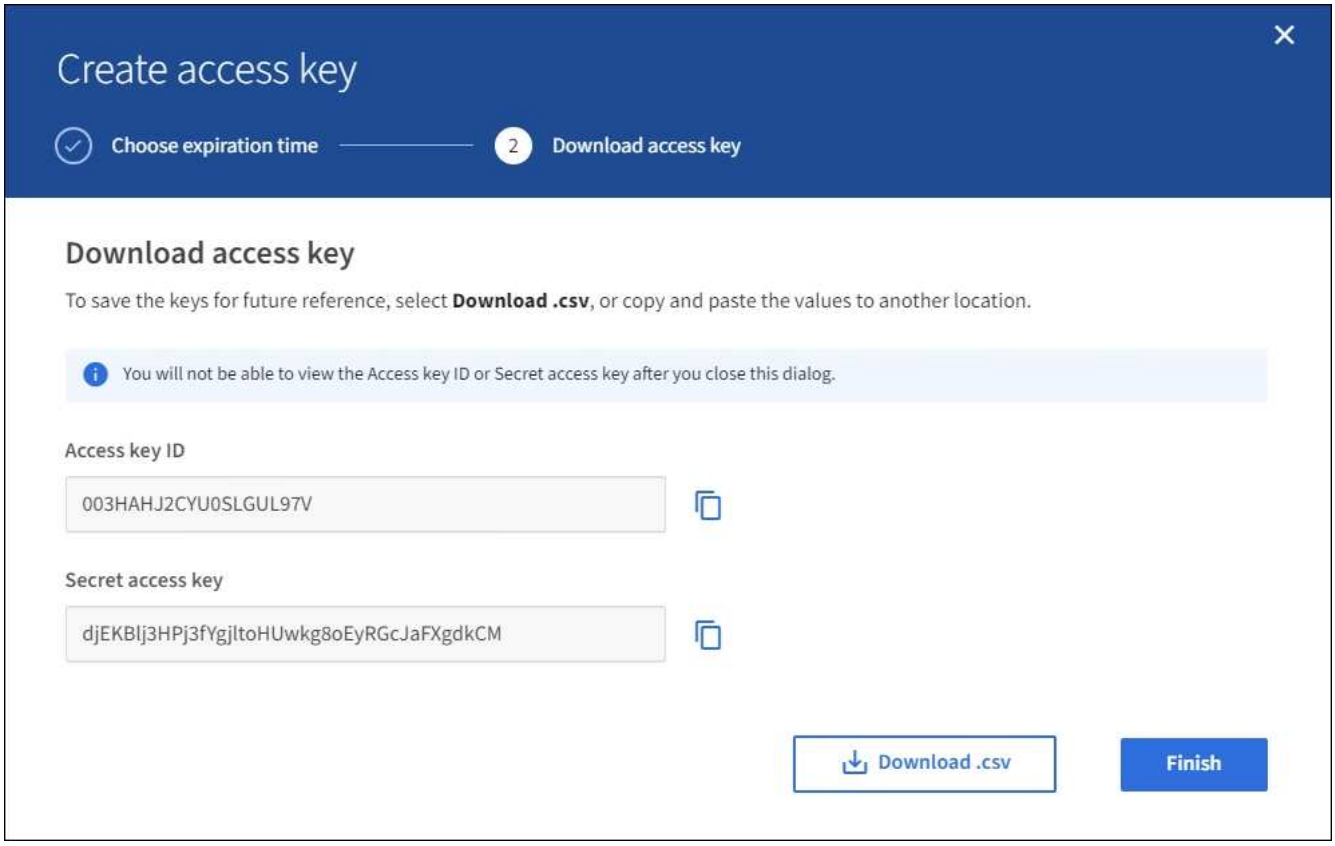


5. Seleccione **Crear clave de acceso**.

   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. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Información relacionada

Permisos de gestión de inquilinos

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.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe tener el permiso 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

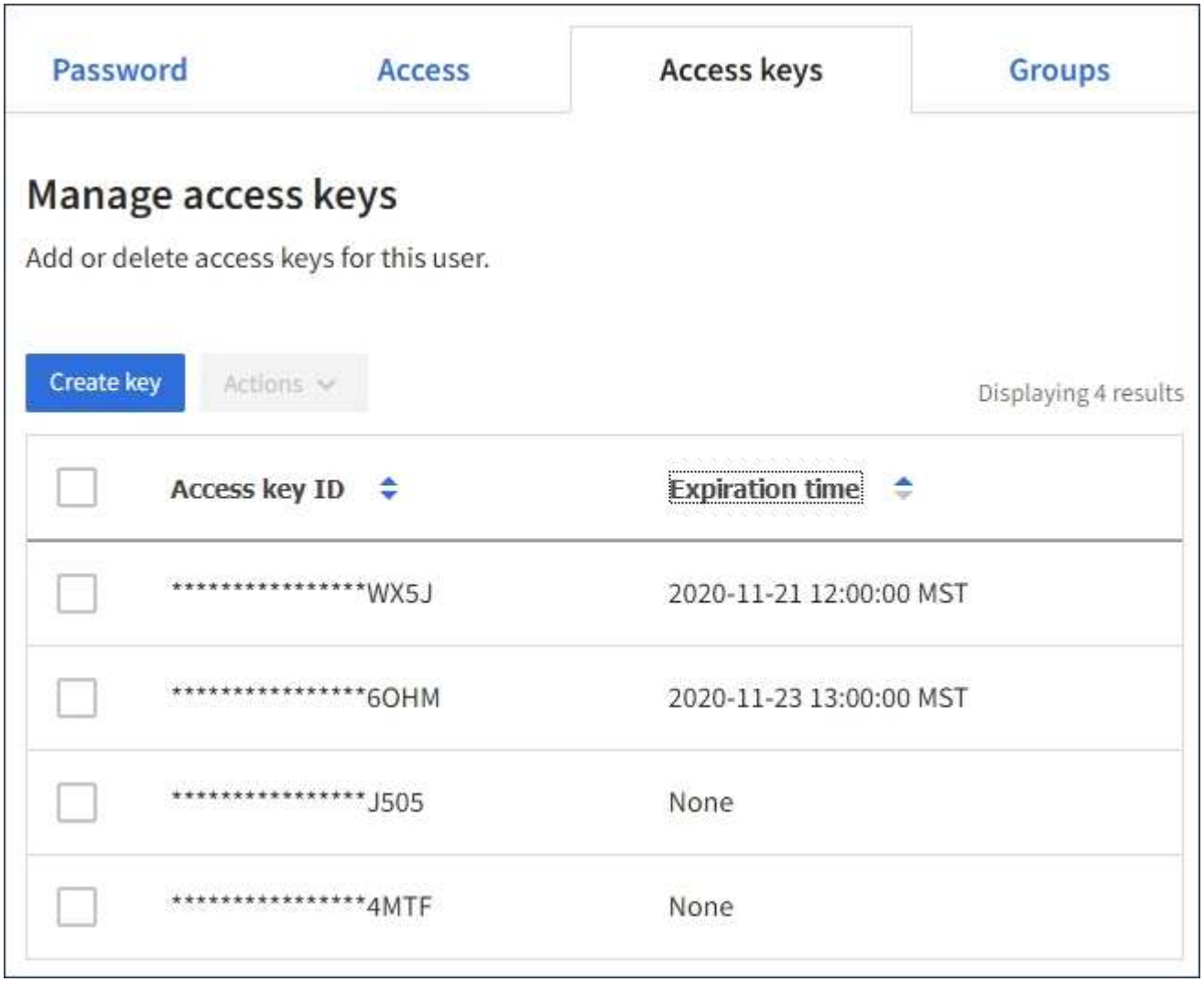
1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.

   Aparece la página Users (usuarios) y enumera los usuarios existentes.

2. Seleccione el usuario cuyas claves de acceso de S3 desee ver.

   Aparece la página de detalles de usuario.

3. Seleccione **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.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe tener el permiso acceso raíz. Consulte Permisos de gestión de inquilinos.

> 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**.

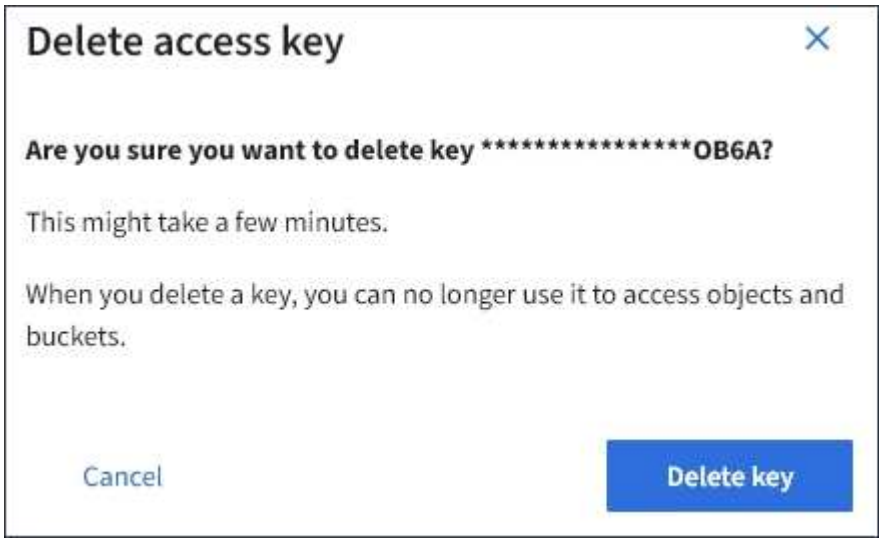
   Aparece la página Users (usuarios) y enumera los usuarios existentes.

2. Seleccione el usuario cuyas claves de acceso de S3 desee gestionar.

   Aparece la página de detalles de usuario.

3. Seleccione **teclas de acceso** y, a continuación, active la casilla de verificación de cada clave de acceso que desee eliminar.
4. Seleccione **acciones** > **Borrar clave seleccionada**.

   Se muestra un cuadro de diálogo de confirmación.



5. Seleccione **tecla Eliminar**.

   Aparecerá un mensaje de confirmación en la esquina superior derecha de la página. Los cambios pueden tardar hasta 15 minutos en surtir efecto debido al almacenamiento en caché.

Gestión de bloques S3

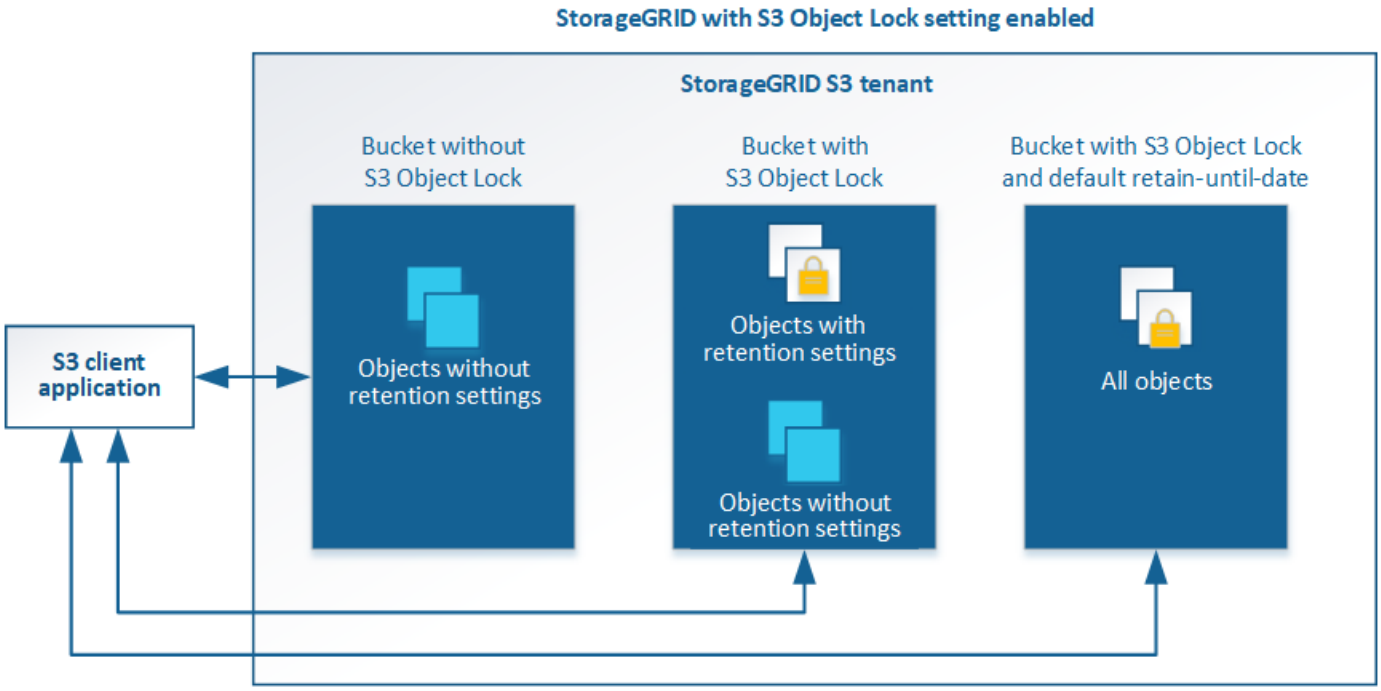
Use el bloqueo de objetos de S3 con inquilinos

Puede usar la función de bloqueo de objetos S3 en StorageGRID si los objetos deben cumplir 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 bloque tiene habilitada la función S3 Object Lock, las aplicaciones cliente S3 pueden especificar, opcionalmente, la configuración de retención para cualquier versión del objeto en ese bloque. Una versión de objeto debe tener la configuración de retención especificada para estar protegida por S3 Object Lock.



La función de bloqueo de objetos StorageGRID S3 ofrece un único modo de retención equivalente al modo de cumplimiento de normativas Amazon S3. De forma predeterminada, cualquier usuario no puede sobrescribir ni eliminar una versión de objeto protegido. La función de bloqueo de objetos StorageGRID S3 no es compatible con un modo de gobierno y no permite a los usuarios con permisos especiales omitir la configuración de retención o eliminar objetos protegidos.

Si un bloque tiene habilitado el bloqueo de objetos S3, la aplicación cliente S3 puede especificar, de manera opcional, la siguiente configuración de retención a nivel de objeto al crear o actualizar un objeto:

- **Retener-hasta-fecha**: Si la fecha retener-hasta-fecha de una versión de objeto es en el futuro, el objeto puede ser recuperado, pero no puede ser modificado o eliminado. Según sea necesario, se puede aumentar la fecha de retención hasta de un objeto, pero esta fecha no se puede disminuir.
- **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.

También puede hacerlo especifique un modo de retención predeterminado y un período de retención predeterminado para el bloque. Estos se aplican a cada objeto agregado al bloque que no especifica su propia configuración de retención.

Para obtener información detallada sobre estos ajustes, consulte Use el bloqueo de objetos de S3.

Gestione bloques que cumplen las normativas heredadas

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 obtener instrucciones, consulte el artículo de la base de conocimientos de NetApp.

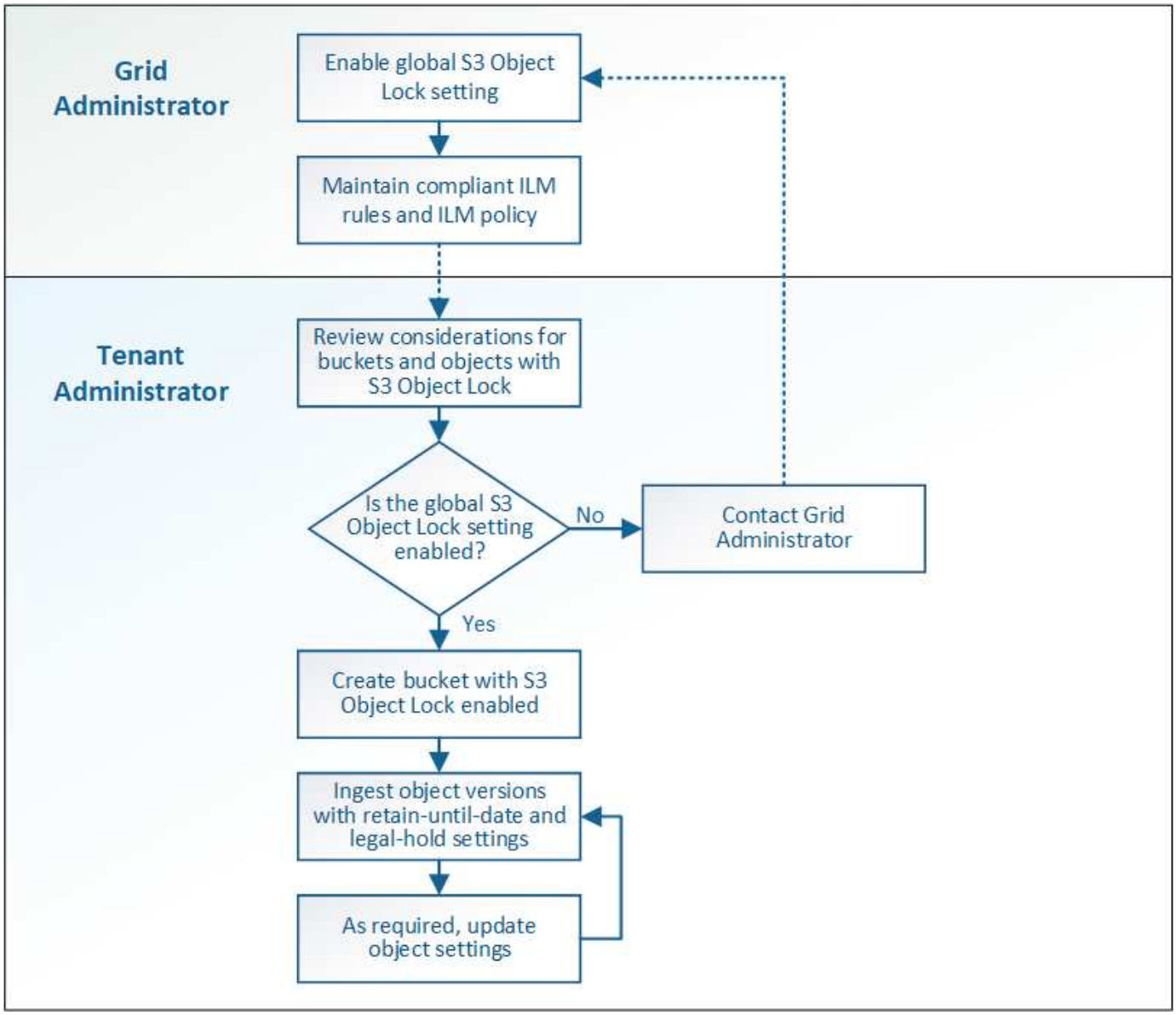
"Base de conocimientos de NetApp: Cómo gestionar bloques heredados que cumplen con la normativa StorageGRID 11.5"

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 el Política de gestión de la vida útil de la información (ILM) Es «"compatible"»; debe cumplir los requisitos de los depósitos con el bloqueo de objetos S3 activado. Para obtener más información, póngase en contacto con el administrador de grid o consulte las instrucciones para gestionar objetos con la gestión del ciclo de vida de la información.

Una vez que se habilita la opción global de bloqueo de objetos S3, se pueden crear bloques con el bloqueo de objetos S3 habilitado. Posteriormente, puede usar la aplicación cliente S3 para especificar opcionalmente la configuración de retención para cada versión del objeto.



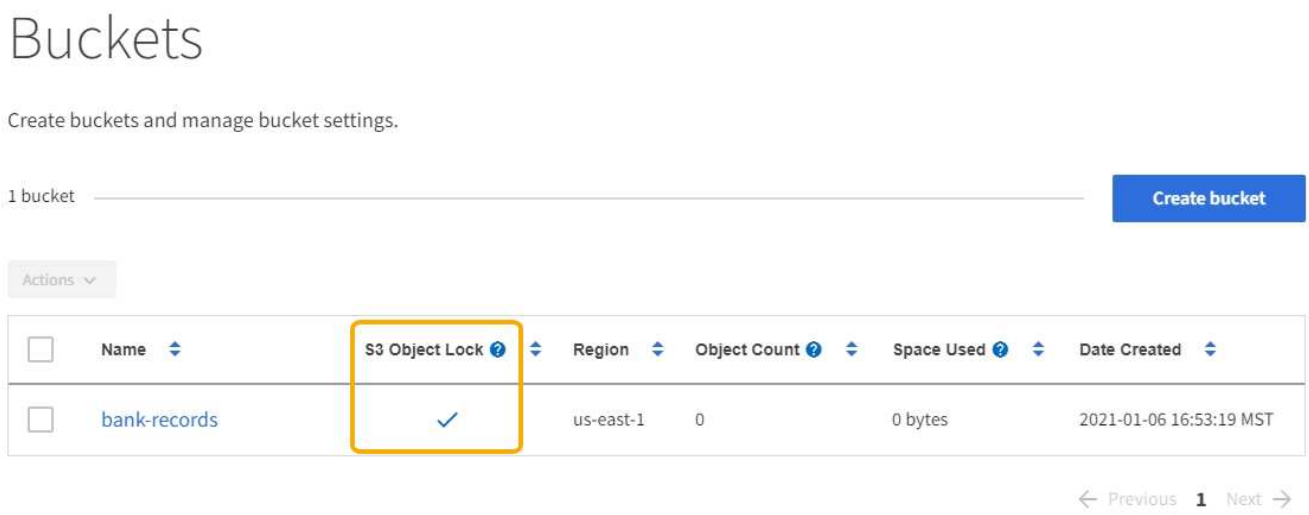
Requisitos para el bloqueo de objetos de S3

Antes de habilitar S3 Object Lock para un bloque, revise los requisitos para los bloques y objetos de S3 Object Lock y el ciclo de vida de los objetos en bloques con S3 Object Lock habilitado.

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.

  Este ejemplo del Administrador de inquilinos muestra un bloque 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 es posible habilitar el bloqueo de objetos de S3 para un bloque existente.
- Se requiere el versionado de bloques con S3 Object Lock. Cuando se habilita el bloqueo de objetos S3 para un bloque, StorageGRID habilita automáticamente el control de versiones para ese bloque.
- Después de crear un bloque con el bloqueo de objetos S3 habilitado, no se puede deshabilitar el bloqueo de objetos S3 ni suspender el control de versiones de ese bloque.
- Si lo desea, puede configurar la retención predeterminada para un bloque. Cuando se carga una versión de objeto, la retención predeterminada se aplica a la versión del objeto. Puede anular el valor predeterminado de bloque especificando un modo de retención y retener hasta la fecha en la solicitud para cargar una versión de objeto.
- Se admite la configuración del ciclo de vida de bloques para los bloques del ciclo de vida de objetos S3.
- 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, la aplicación cliente S3 debe configurar la retención predeterminada de bloques o especificar la configuración de retención en cada solicitud de carga.
- Puede aumentar la fecha de retención hasta una versión de objeto, pero nunca puede disminuir este valor.
- Si recibe una notificación de una acción legal pendiente o una investigación normativa, puede conservar la información relevante colocando una retención legal en una versión del objeto. Cuando una versión de objeto se encuentra bajo una retención legal, ese objeto no se puede eliminar de StorageGRID, aunque haya alcanzado su fecha de retención. Tan pronto como se levante la retención legal, la versión del objeto se puede eliminar si se ha alcanzado la fecha de retención.
- El bloqueo de objetos de S3 requiere el uso de bloques con versiones. 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 bloque con el bloqueo de objetos S3 habilitado atraviesa tres etapas:

1. **Procesamiento de objetos**

- Al añadir una versión de objeto a un bloque con el bloqueo de objetos S3 habilitado, la aplicación cliente S3 puede especificar, de manera opcional, la configuración de retención del objeto (retener hasta la fecha, la conservación legal o ambos). A continuación, StorageGRID genera metadatos para ese objeto, que incluye un identificador de objeto (UUID) único y la fecha y la hora de procesamiento.
- Después de procesar una versión de objeto con configuración de retención, sus datos y los metadatos definidos por el usuario de S3 no se pueden modificar.
- StorageGRID almacena los metadatos del objeto de forma independiente de los datos del objeto. Mantiene tres copias de todos los metadatos de objetos en cada sitio.

2. **Retención de objetos**
   - StorageGRID almacena varias copias del objeto. El número y el tipo exactos de copias y las ubicaciones del almacenamiento se determinan según las reglas conformes de la política de ILM activa.
3. **Eliminación de objetos**
   - Un objeto se puede eliminar cuando se alcanza su fecha de retención.
   - No se puede eliminar un objeto que se encuentra bajo una retención legal.

Crear bloque de S3

Puede usar el administrador de inquilinos para crear bloques S3 para los datos de objetos. Al crear un bloque, debe especificar el nombre y la región del bloque. Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, de manera opcional, puede habilitar el bloqueo de objetos S3 para el bloque.

Lo que necesitará

- Ha iniciado sesión en el administrador de inquilinos mediante un navegador web compatible.
- Pertenece a un grupo de usuarios que tiene el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

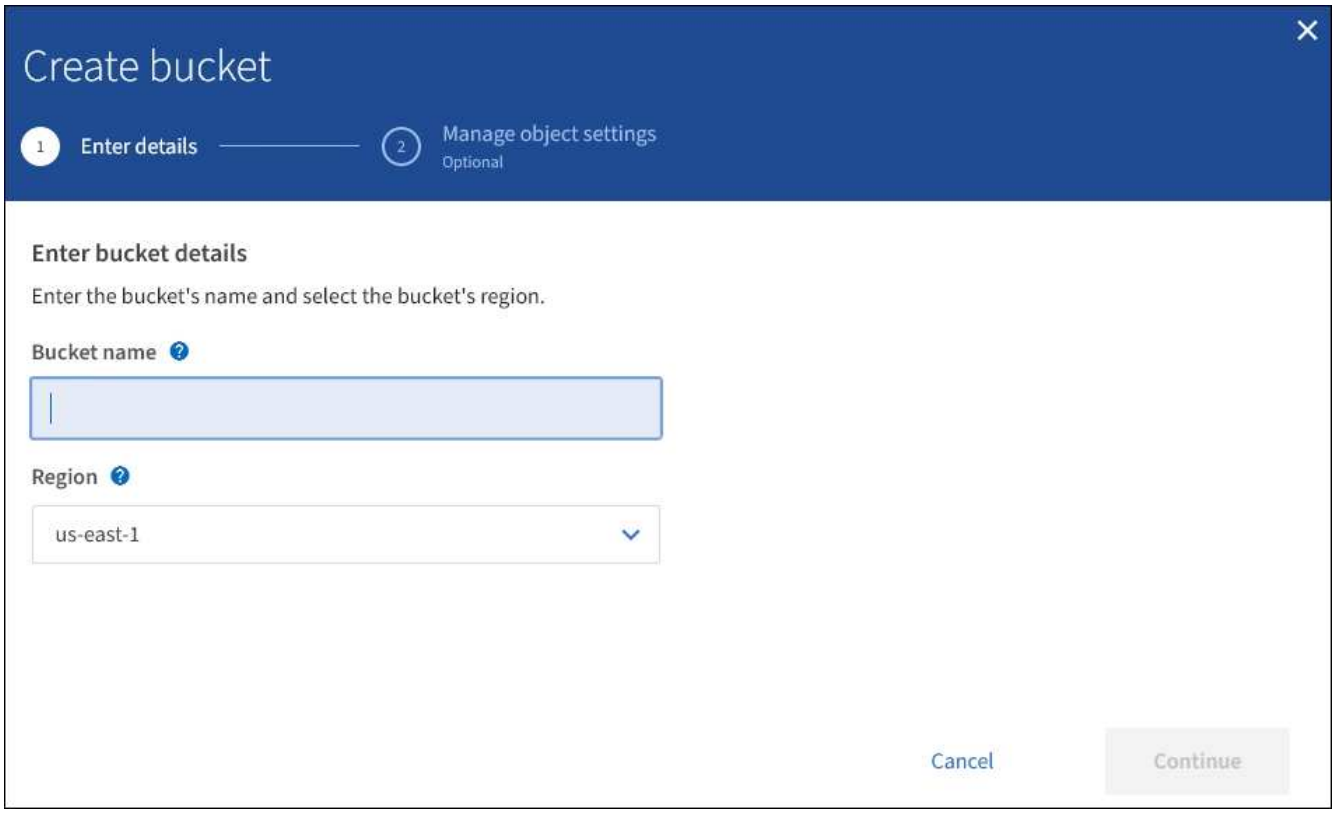
  > Los permisos para establecer o modificar las propiedades de Object Lock de grupos o objetos de S3 pueden ser concedidos por política de bloques o política de grupo.

- Si tiene pensado crear un bloque con S3 Object Lock, ha habilitado la configuración global de S3 Object Lock para el sistema StorageGRID y ha revisado los requisitos para bloques y objetos de S3 Object Lock.

  Utilice el bloqueo de objetos de S3

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
2. Seleccione **Crear cucharón**.



3. Introduzca un nombre único para el bloque.

> No se puede cambiar el nombre del bloque después de crear el bloque.

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.
- 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".

4. Seleccione la región para este segmento.

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.

> No se puede cambiar la región después de crear el bloque.

5. Seleccione **continuar**.
6. 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.

7. Si aparece la sección S3 Object Lock, de forma opcional, habilite S3 Object Lock para el bloque.

   No se puede habilitar o deshabilitar S3 Object Lock después de crear el bloque.

   La sección S3 Object Lock aparece solo si se habilita la configuración global de S3 Object Lock.

   El bloqueo de objetos S3 debe estar habilitado para el bloque antes de que una aplicación cliente S3 pueda especificar la configuración de retención legal y hasta la fecha para los objetos agregados al bloque.

   Si habilita S3 Object Lock para un bloque, el control de versiones de bloques se habilita automáticamente. También puede hacerlo especifique un modo de retención predeterminado y un período de retención predeterminado para el bloque que se aplican a cada objeto ingerido en el bloque que no especifica su propia configuración de retención.

8. Seleccione **Crear cucharón**.

   El cucharón se crea y se agrega a la tabla de la página Cuches.

Información relacionada

Gestión de objetos con ILM

Comprender la API de gestión de inquilinos

Use S3

Ver detalles de bloques de S3

Puede ver una lista de las configuraciones de bloques y bloques en su cuenta de inquilino.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.

   Aparece la página Cuchos y enumera todos los cucharones de la cuenta de arrendatario.

2. Revisar la información de cada bloque.

   Según sea necesario, puede ordenar la información por cualquier columna o puede avanzar y retroceder por la lista.

   - Nombre: Nombre único del bloque, que no se puede cambiar.
   - S3 Object Lock: Si está habilitado el bloqueo de objetos de S3 para este bloque.

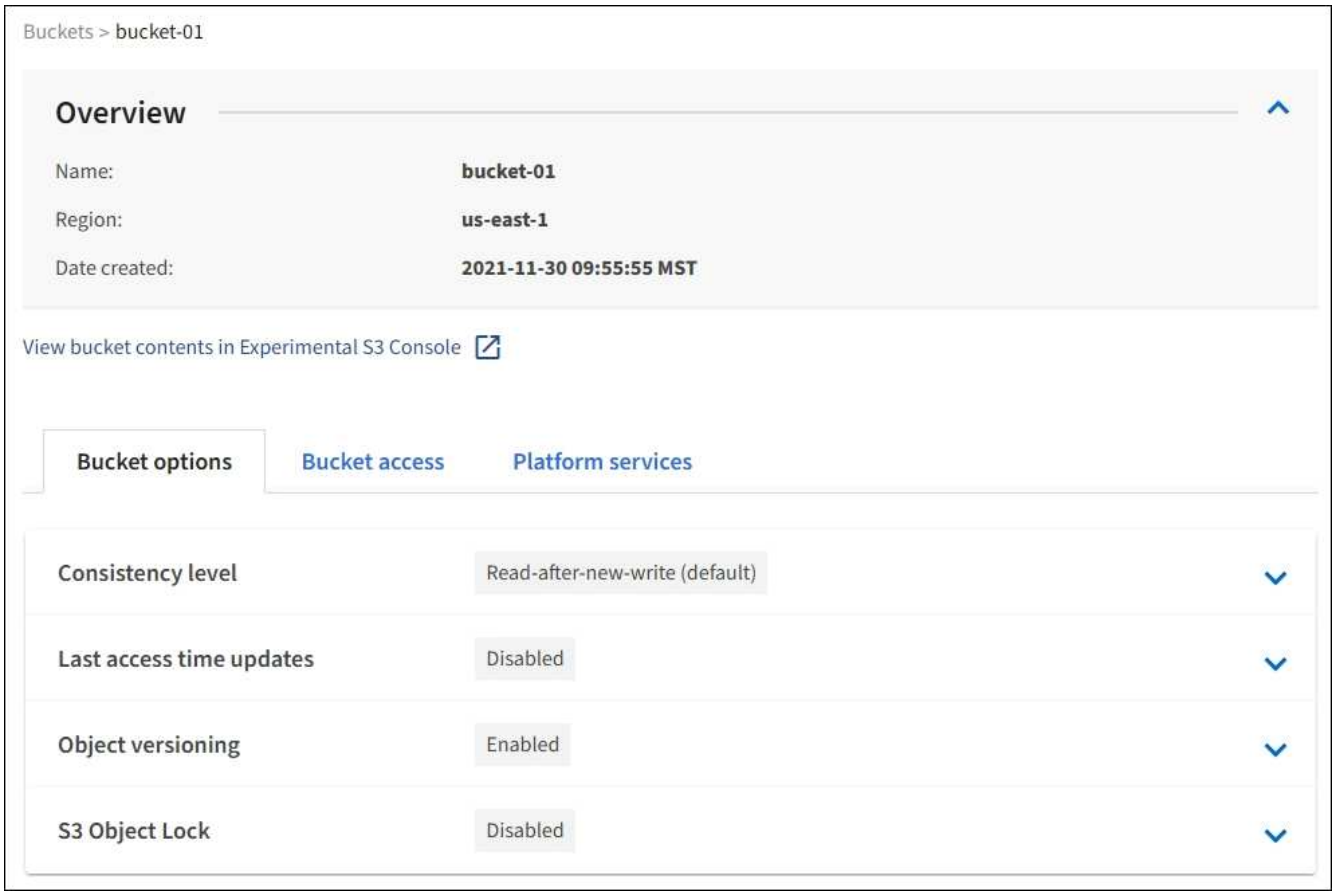
     Esta columna no se muestra si la configuración global de bloqueo de objetos S3 está deshabilitada. Esta columna también muestra información para todos los segmentos compatibles anteriores.

   - Región: La región del cucharón, que no se puede cambiar.
   - Recuento de objetos: El número de objetos de este bloque.
   - Espacio utilizado: Tamaño lógico de todos los objetos de este 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 que se creó el segmento.

   > 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. Para ver y gestionar la configuración de un bloque, seleccione el nombre del bloque.

   La página de detalles bucket permite ver y editar la configuración de las opciones de bloques, el acceso a bloques y servicios de plataforma.



Cambie el nivel de coherencia

Si usa un inquilino de S3, puede usar el administrador de inquilinos o la API de gestión de inquilinos para cambiar el control de coherencia para las operaciones realizadas en los objetos en los bloques S3.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque. Consulte Permisos de gestión de inquilinos.

Acerca de esta tarea

El nivel de consistencia proporciona un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en distintos nodos de almacenamiento y sitios. En general, debe utilizar el nivel de consistencia de **lectura tras escritura nueva** para sus cucharones.

Si el nivel de consistencia de **lectura tras escritura nueva** no cumple los requisitos de la aplicación cliente, puede cambiar el nivel de consistencia estableciendo el nivel de consistencia de la cuchara o utilizando la `Consistency-Control` encabezado. La `Consistency-Control` el encabezado anula el nivel de consistencia del cucharón.

> Cuando se cambia el nivel de consistencia de un cubo, solo se garantiza que los objetos que se ingieren después del cambio alcancen el nivel revisado.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
2. Seleccione el nombre del bloque de la lista.

   Aparece la página de detalles bucket.

3. Seleccione **Opciones de bloque** > **nivel de coherencia**.
4. Seleccione un nivel de 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 depósitos S3, utilice sólo según sea necesario (por ejemplo, para un depósito que contiene valores de log 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**.

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 sólo se aplican a los sistemas StorageGRID que incluyen al menos una regla de ILM que utiliza la opción **última hora de acceso** en sus instrucciones de colocación. Puede ignorar estas instrucciones si el sistema StorageGRID no incluye dicha regla.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque. Consulte Permisos de gestión de inquilinos.

Last Access Time es una de las opciones disponibles para la instrucción de colocación **Reference Time** para una regla de ILM. Si se establece el tiempo de referencia de una regla en tiempo de último acceso, los administradores de la cuadrícula pueden especificar que los objetos se coloquen en determinadas ubicaciones de almacenamiento en función de cuándo se recuperaron por última vez esos objetos (se leen o se visualizan).

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.

> Consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

De forma predeterminada, las actualizaciones de la hora del último acceso están desactivadas. Si el sistema StorageGRID incluye una regla de ILM que utiliza la opción **Hora de último acceso** y desea que esta opción se aplique a los objetos de este bloque, debe habilitar las actualizaciones para el último tiempo de acceso para los bloques S3 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

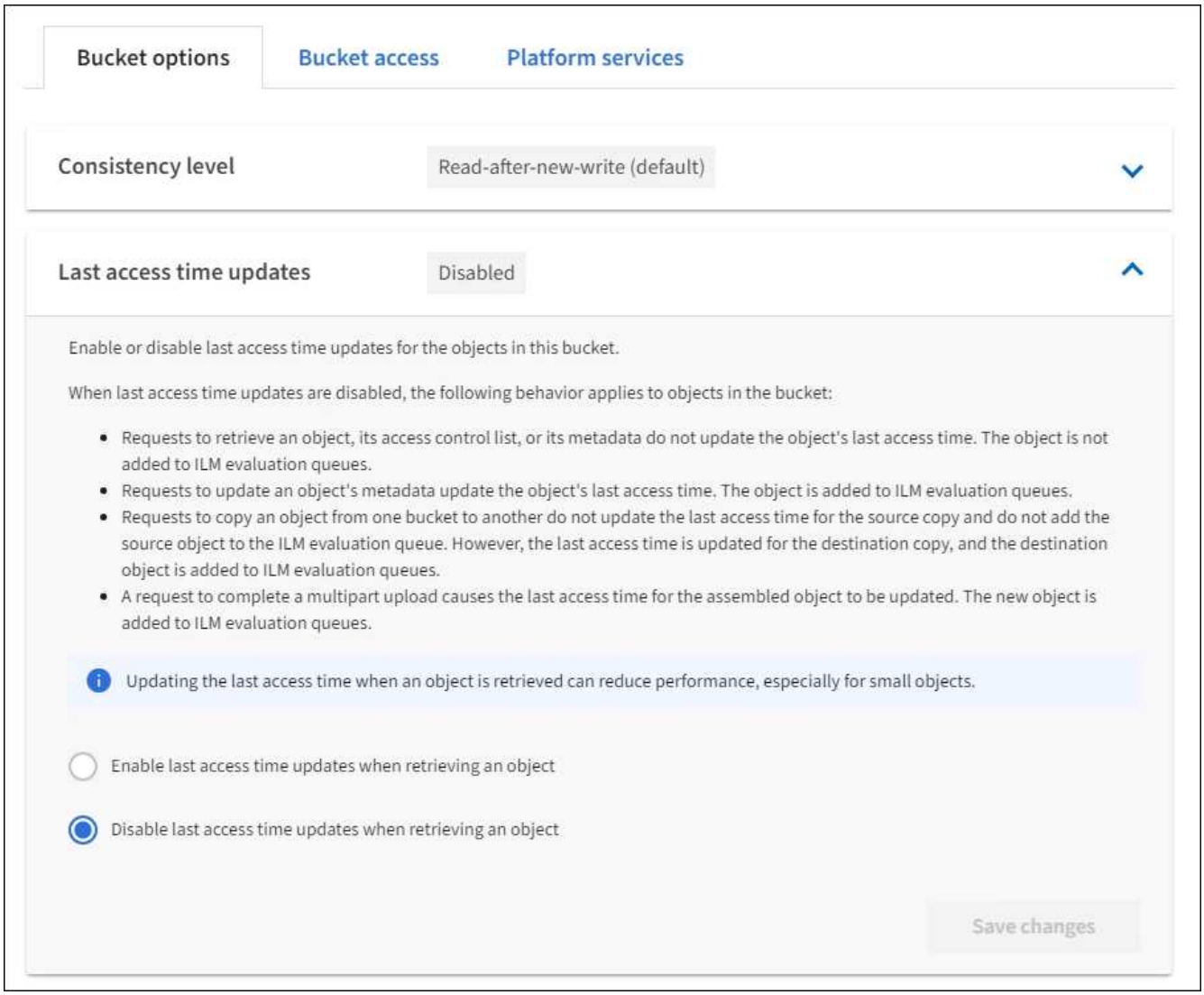
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
2. Seleccione el nombre del bloque de la lista.

   Aparece la página de detalles bucket.

3. Seleccione **Opciones de bloque** > **actualizaciones del último tiempo de acceso**.
4. Seleccione el botón de opción adecuado para activar o desactivar las actualizaciones de la hora del último acceso.



5. Seleccione **Guardar cambios**.

Información relacionada

Permisos de gestión de inquilinos

Cambiar el control de versiones del objeto para un bloque

Si usa un inquilino de S3, puede usar el administrador de inquilinos o la API de gestión de inquilinos para cambiar el estado de versionado de los bloques de S3.

Lo que necesitará

- Ha iniciado sesión en el administrador de inquilinos mediante un navegador web compatible.
- Pertenece a un grupo de usuarios que tiene el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque.

  Permisos de gestión de inquilinos

Acerca de esta tarea

Puede habilitar o suspender el control de versiones de objetos de un bloque. Una vez que habilita el control de versiones de un bloque, no puede volver a un estado sin versiones. Sin embargo, puede suspender el control de versiones del bloque.

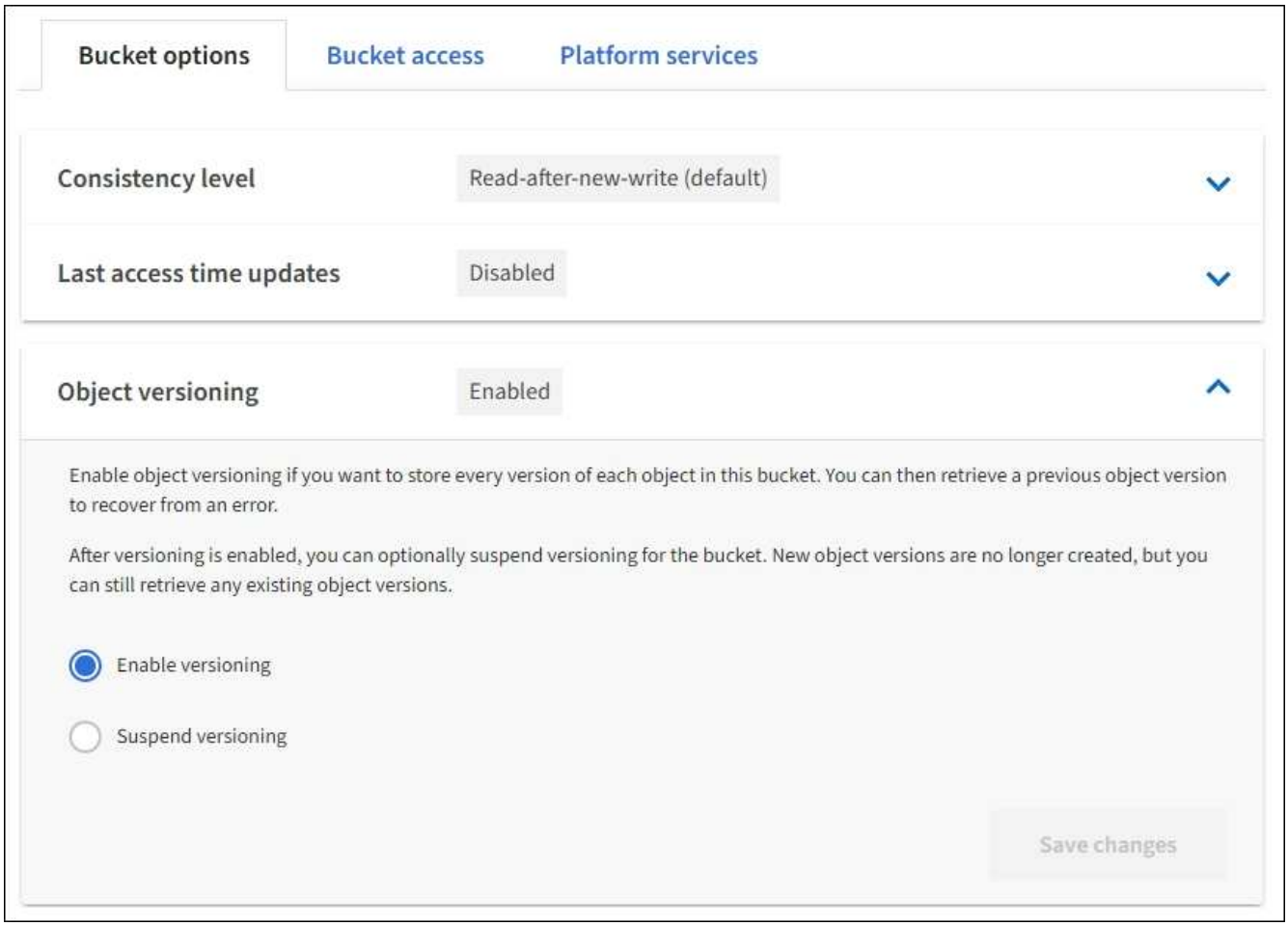
- Desactivado: El control de versiones no se ha activado nunca
- Activado: El control de versiones está activado
- Suspendido: El control de versiones se ha habilitado anteriormente y se ha suspendido

Versionado de objetos de S3

Reglas de ILM y políticas para objetos con versiones de S3 (ejemplo 4)

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
2. Seleccione el nombre del bloque de la lista.
3. Seleccione **Opciones de bloque** > **versiones de objeto**.



4. Seleccione un estado de control de versiones para los objetos de este bloque.

> 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**.

Configurar el uso compartido de recursos de origen cruzado (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un bloque de S3 si desea que dicho bloque y los objetos de ese bloque sean accesibles a

las aplicaciones web de otros dominios.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o 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 que las aplicaciones web de cliente de un dominio accedan 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`.

Pasos

1. Utilice un editor de texto para crear el XML necesario para habilitar CORS.

   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>
   ```

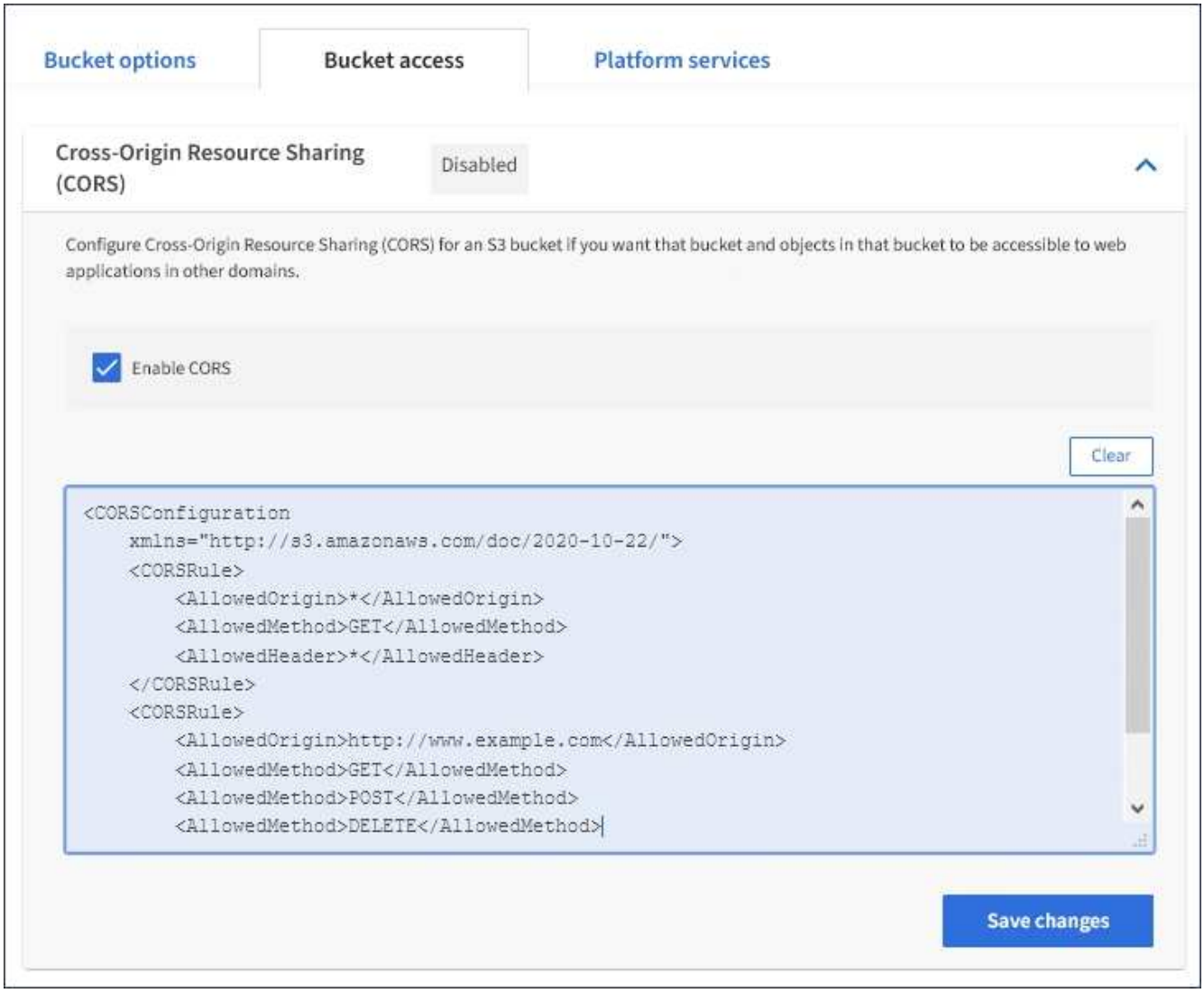
   Para obtener más información acerca del XML de configuración de CORS, consulte "Documentación de Amazon Web Services (AWS): Guía para desarrolladores de Amazon simple Storage Service".

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.
3. Seleccione el nombre del bloque de la lista.

   Aparece la página de detalles bucket.

4. Seleccione **acceso a bloque** > **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 y seleccione **Guardar cambios**.



7. Para modificar la configuración de CORS para el bloque, actualice el XML de configuración de CORS en el cuadro de texto o seleccione **Borrar** para volver a empezar. A continuación, seleccione **Guardar cambios**.
8. Para desactivar CORS para el cucharón, desactive la casilla de verificación **Activar CORS** y, a continuación, seleccione **Guardar cambios**.

Eliminar bloque de S3

Puede usar el administrador de inquilinos para eliminar uno o varios bloques de S3 vacíos.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz. Estos permisos anulan la configuración de los permisos en las políticas de grupo o bloque. Consulte Permisos de gestión de inquilinos.
- Los cucharones que desea eliminar están vacíos.

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 puede eliminar un bloque de S3 si contiene objetos o versiones de objetos no actuales. Para obtener información sobre cómo se eliminan los objetos con versiones S3, consulte instrucciones para gestionar objetos con la gestión del ciclo de vida de la información.

Pasos

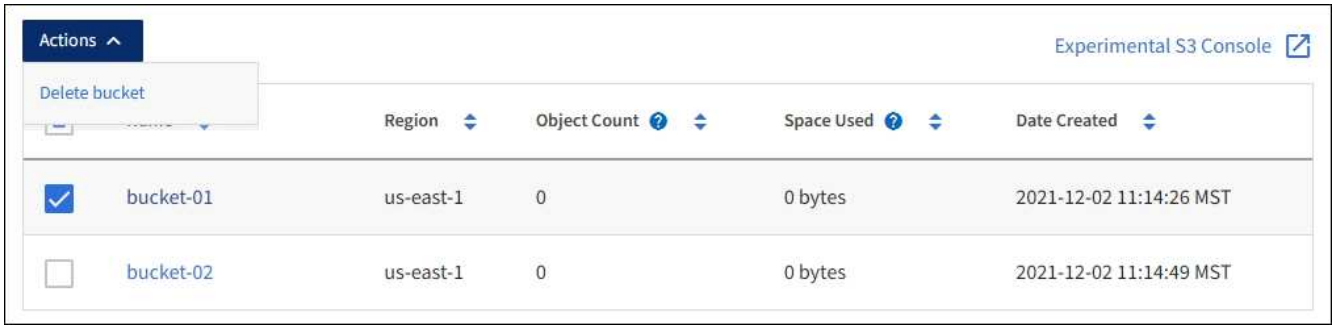
1. Seleccione **ALMACENAMIENTO (S3)** > **Cuchos**.

   Aparece la página Buckets y muestra todos los bloques S3 existentes.

2. Seleccione la casilla de verificación para el segmento vacío que desea eliminar. Puede seleccionar más de un bloque a la vez.

   El menú acciones está activado.

3. En el menú acciones, seleccione **Eliminar cubo** (o **Eliminar cubos** si ha elegido más de uno).



4. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí** para eliminar todos los segmentos que haya elegido.

   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 eliminar todos los objetos antes de

poder eliminar un bloque.

Utilice la consola Experimental S3

Puede usar la consola de S3 para ver los objetos de un bloque de S3.

También puede usar la consola de S3 para hacer lo siguiente:

- Agregar y eliminar objetos, versiones de objetos y carpetas
- Cambie el nombre de los objetos
- Mueva y copie objetos entre bloques y carpetas
- Administrar etiquetas de objetos
- Ver los metadatos de objetos
- Descargar objetos

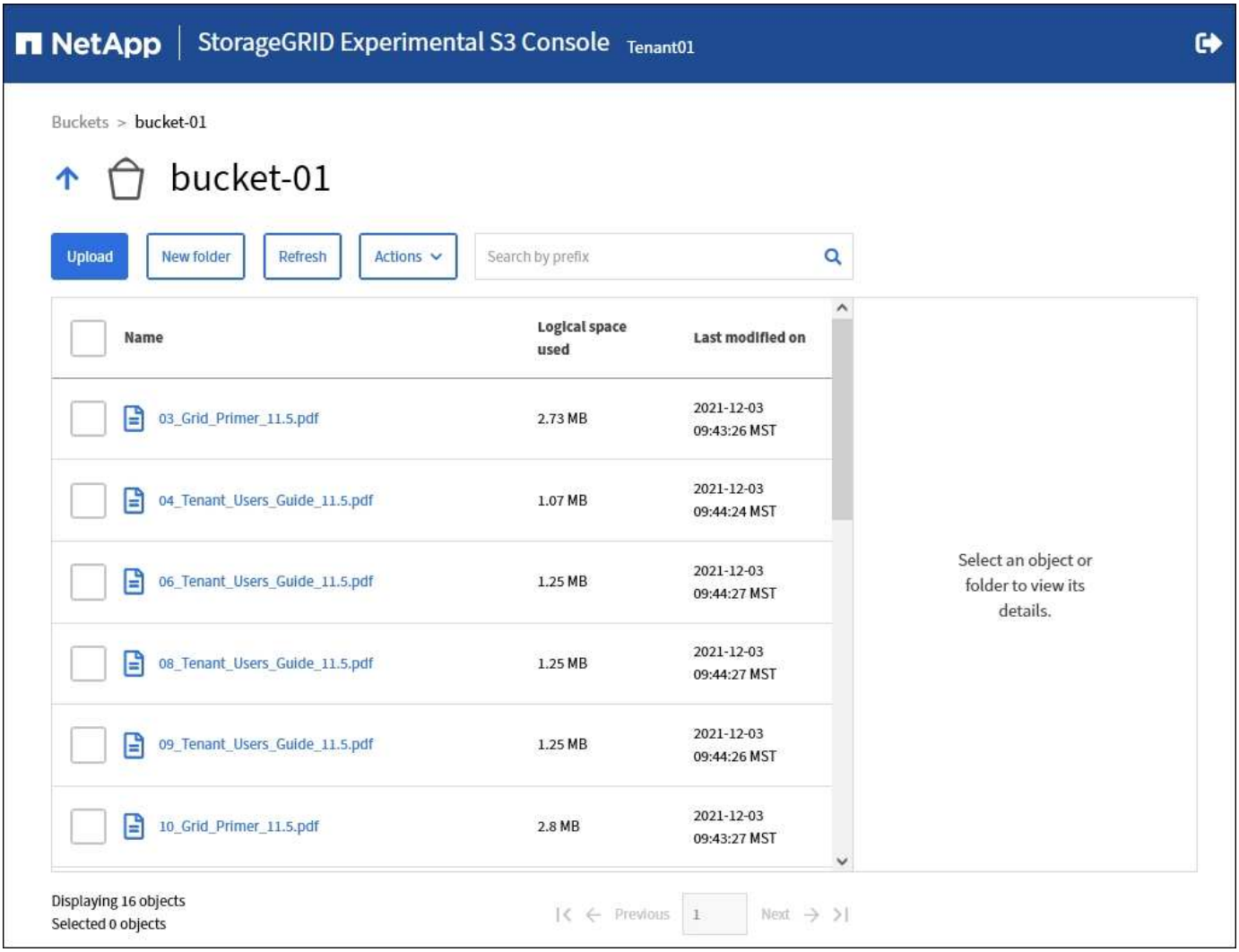
> La consola de S3 no se ha probado completamente y se Marca como “experimental”. No está diseñado para la gestión masiva de objetos ni para su uso en un entorno de producción. Los inquilinos solo deben usar S3 Console cuando se realicen funciones para un pequeño número de objetos, como cuando se cargan objetos para simular una nueva política de ILM, solución de problemas de ingesta, o bien mediante grids de prueba de concepto o no de producción.

Lo que necesitará

- Ha iniciado sesión en el administrador de inquilinos mediante un navegador web compatible.
- Tiene el permiso gestionar sus propias credenciales de S3.
- Ha creado un bucket.
- 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 **Cuchos**.
2. Seleccione Experimental S3 Console . También puede acceder a este enlace desde la página de detalles de la cuchara.
3. En la página de inicio de sesión de Experimental S3 Console, 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. Gestione los objetos que sea necesario.



Gestione servicios de plataformas S3

¿Qué son los servicios de plataforma?

Los servicios de plataforma de StorageGRID pueden ayudarle a implementar una estrategia de cloud híbrido.

Si se permite el uso de servicios de plataforma para su cuenta de inquilino, puede configurar los siguientes servicios para cualquier bloque de S3:

- **Duplicación CloudMirror**: La Servicio de replicación CloudMirror de StorageGRID Se utiliza 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**: Notificaciones de eventos por bloque Se utilizan para enviar notificaciones sobre acciones específicas realizadas en objetos a un Amazon simple Notification Service™ (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**: El servicio de integración de búsqueda Se usa para enviar metadatos de objetos de S3 a un índice de Elasticsearch especificado donde los metadatos se pueden buscar o analizar 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.

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 extremos externos que se configuran mediante el administrador de inquilinos o la API de gestión de inquilinos. Cada extremo representa un destino externo, como un bloque de StorageGRID S3, un bloque de Amazon Web Services, un tema de servicio de notificación simple (SNS) o un clúster de Elasticsearch alojado localmente, en AWS u otros lugares.

Después de crear un extremo, puede habilitar un servicio de plataforma para un bloque agregando la 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:

1. 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.
2. Si también desea enviar notificaciones cuando estos objetos están almacenados en el bloque, debe añadir

una configuración de notificaciones.

3. 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
Replicación de CloudMirror	• OBTENGA la replicación de Bucket • PUT Bucket replication
Notificaciones	• OBTENGA la notificación DE BUCKET • NOTIFICACIÓN DE PUT Bucket
Integración de búsqueda	• OBTENGA la configuración de notificación de metadatos del bloque de datos • PUT bucket metadata notification Configuration Estas operaciones están personalizadas en StorageGRID.

Consulte las instrucciones para implementar aplicaciones cliente de S3 para obtener detalles sobre cómo StorageGRID implementa estas API.

Información relacionada

Consideraciones sobre el uso de servicios de plataforma

Use S3

Servicio de replicación de CloudMirror

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 opera con independencia de la política de ILM activa de la cuadrícula. 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.

Si habilita la replicación de CloudMirror para un bloque existente, solo se replican los nuevos objetos agregados a ese bloque. No se replican ningún objeto existente en el bloque. Para forzar la replicación de objetos existentes, puede actualizar los metadatos del objeto existente ejecutando una copia de objeto.

> Si va a usar la replicación de CloudMirror para copiar objetos en un destino de AWS S3, tenga en cuenta que Amazon S3 limita el tamaño de los metadatos definidos por el usuario en 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 se 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 segmento de destino, StorageGRID los Marca como «réplicas». Un bloque 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 admite un CloudMirror bidireccional entre dos grids.

La singularidad y el orden de los eventos en el segmento 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

Es posible habilitar la notificación de eventos para un bloque de S3 si desea que StorageGRID envíe notificaciones sobre eventos especificados a un servicio de notificación simple (SNS) de destino.

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 las notificaciones de bloques, con el tema SNS de destino especificado como URN de un extremo.

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 las siguientes limitaciones:

- No es posible configurar una notificación para los siguientes tipos de eventos. 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 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. Una vez indizado un documento, no se pueden 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, las notificaciones no se envían para ningún objeto que ya estaba 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 el uso de 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 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 que coincida con el comportamiento de eliminación de los servicios CRR y SNS de AWS, las solicitudes de notificación de CloudMirror y eventos no se envían cuando se elimina un objeto del bloque de origen debido a las reglas de ILM 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.

Consideraciones sobre el uso del servicio de replicación de CloudMirror

Consideración	Detalles
Estado de replicación	StorageGRID no admite el `x-amz-replication-status` encabezado.

Consideración	Detalles
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 *recomendado* para una operación PUT Object 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 cucharón de origen en StorageGRID no están relacionados con los ID de versión para el cubo de destino.
Etiquetado para versiones de objetos	El servicio CloudMirror no replica ninguna solicitud DE etiquetado de objetos PUT ni ELIMINA solicitudes de etiquetado de objetos que proporcionen un ID de versión, debido a las limitaciones en el protocolo S3. Como los ID de versión del origen y del destino no están relacionados, no hay manera de garantizar que se replique una actualización de etiqueta a un ID de versión específico. Por el contrario, el servicio CloudMirror replica las solicitudes DE etiquetado PUT Object o ELIMINA las solicitudes de etiquetado de objetos 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 bloque de destino S3 para la replicación de CloudMirror tiene la función S3 Object Lock habilitada, el intento de configurar la replicación de bucket (PUT Bucket replication) producirá 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 extremo de servicios de plataforma, debe ser un usuario inquilino con permiso Administrar extremos o acceso raíz, en una cuadrícula cuya red se haya configurado para permitir que los nodos de almacenamiento accedan a recursos de extremo externos. 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 bloque de StorageGRID en un bloque de AWS S3, debe crear un extremo de servicios de plataforma que incluya la información y las credenciales que StorageGRID necesita para acceder al bloque de destino en AWS.

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 es posible configurar un bloque de origen para que use más de un extremo como destino, lo que permite hacer cosas como enviar notificaciones sobre la creación de objetos a un tema de SNS y notificaciones sobre la eliminación de objetos a un segundo tema 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 admite los extremos del servicio de notificación simple (SNS). No se admiten extremos de AWS Lambda o simple Queue Service (SQS).

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 en los clouds de AWS u otros lugares.

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 extremo. 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 extremo cuando cree 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
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	nombre del bloque
Notificaciones	sns-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:

```
urn:mysite:sns:optional:optional:sns-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.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar endpoints.
- Se debe haber creado el recurso al que hace referencia el extremo de servicios de la plataforma:
  - Replicación de CloudMirror: Bloque de S3
  - Notificación de eventos: Tema SNS
  - Notificación de búsqueda: Índice de Elasticsearch, si el clúster de destino no está configurado para crear índices automáticamente.
- Debe tener 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)

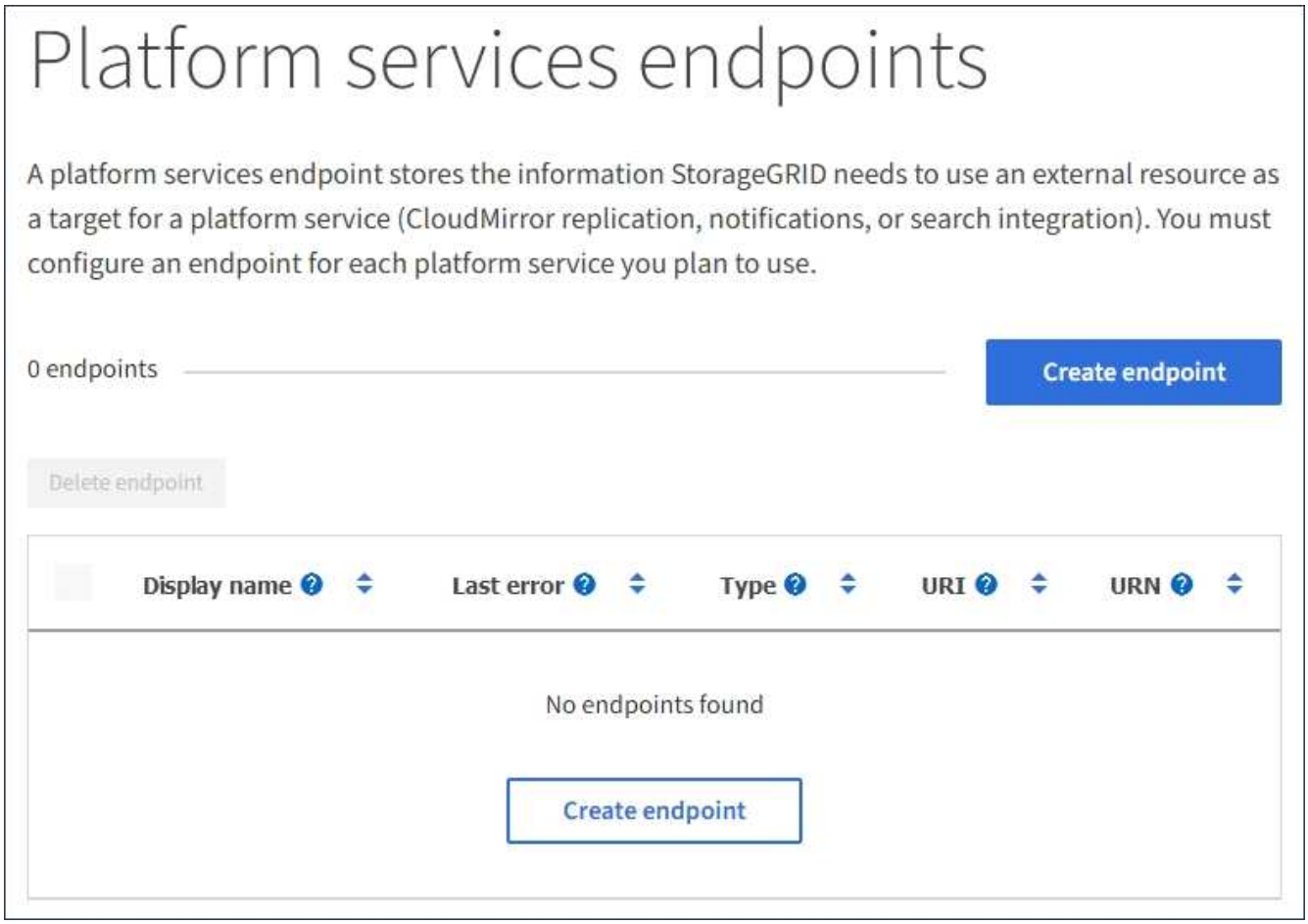
    Especifique URN para el extremo de servicios de la plataforma

  - Credenciales de autenticación (si es necesario):
    - 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.
  - Certificado de seguridad (si se utiliza un certificado de CA personalizado)

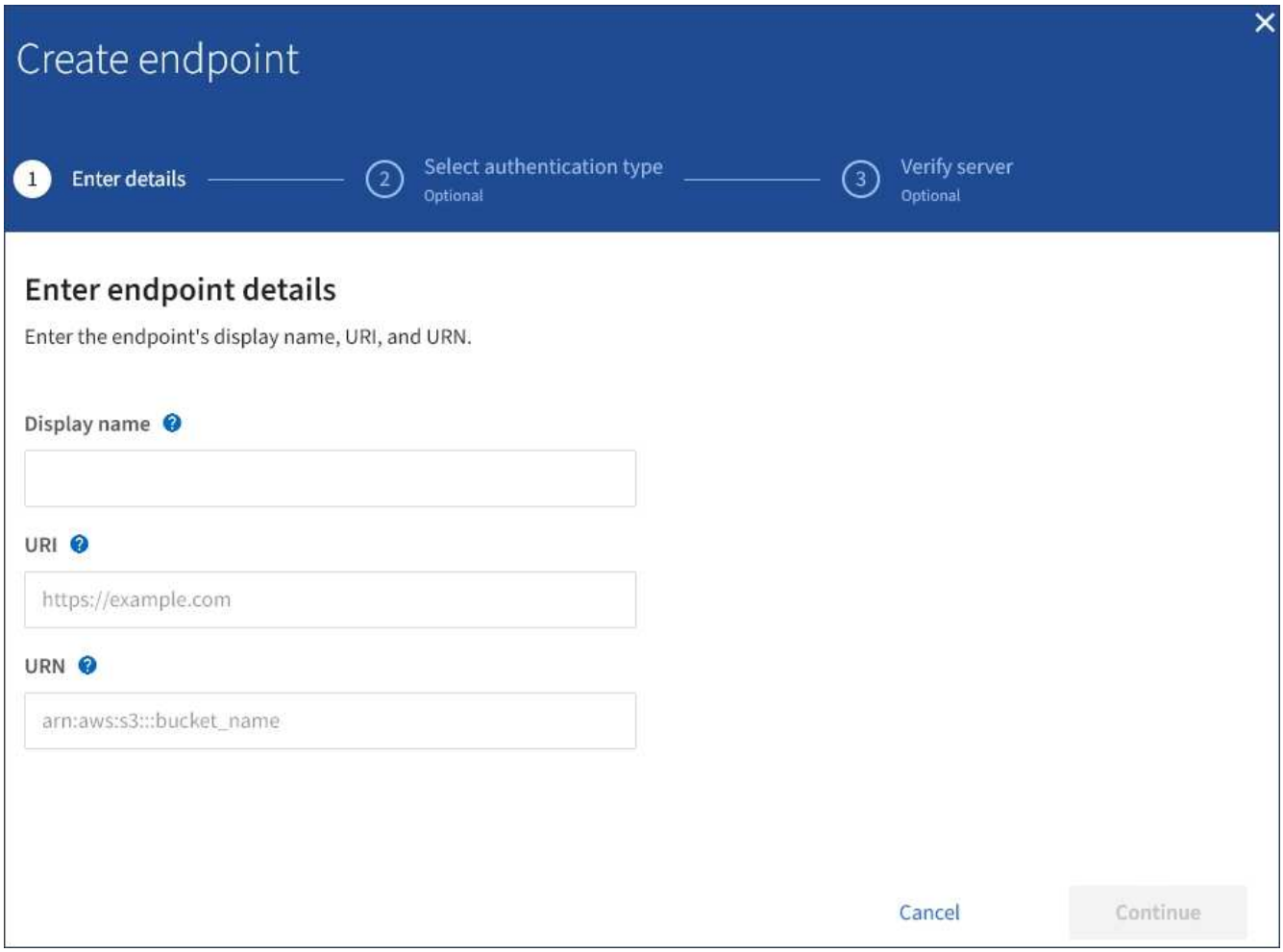
Pasos

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 admite el extremo se muestra junto al nombre del extremo cuando se muestra en la página de extremos, 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, el puerto 443 se utiliza para los URI HTTPS y el puerto 80 se utiliza para los URI HTTP.

   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:

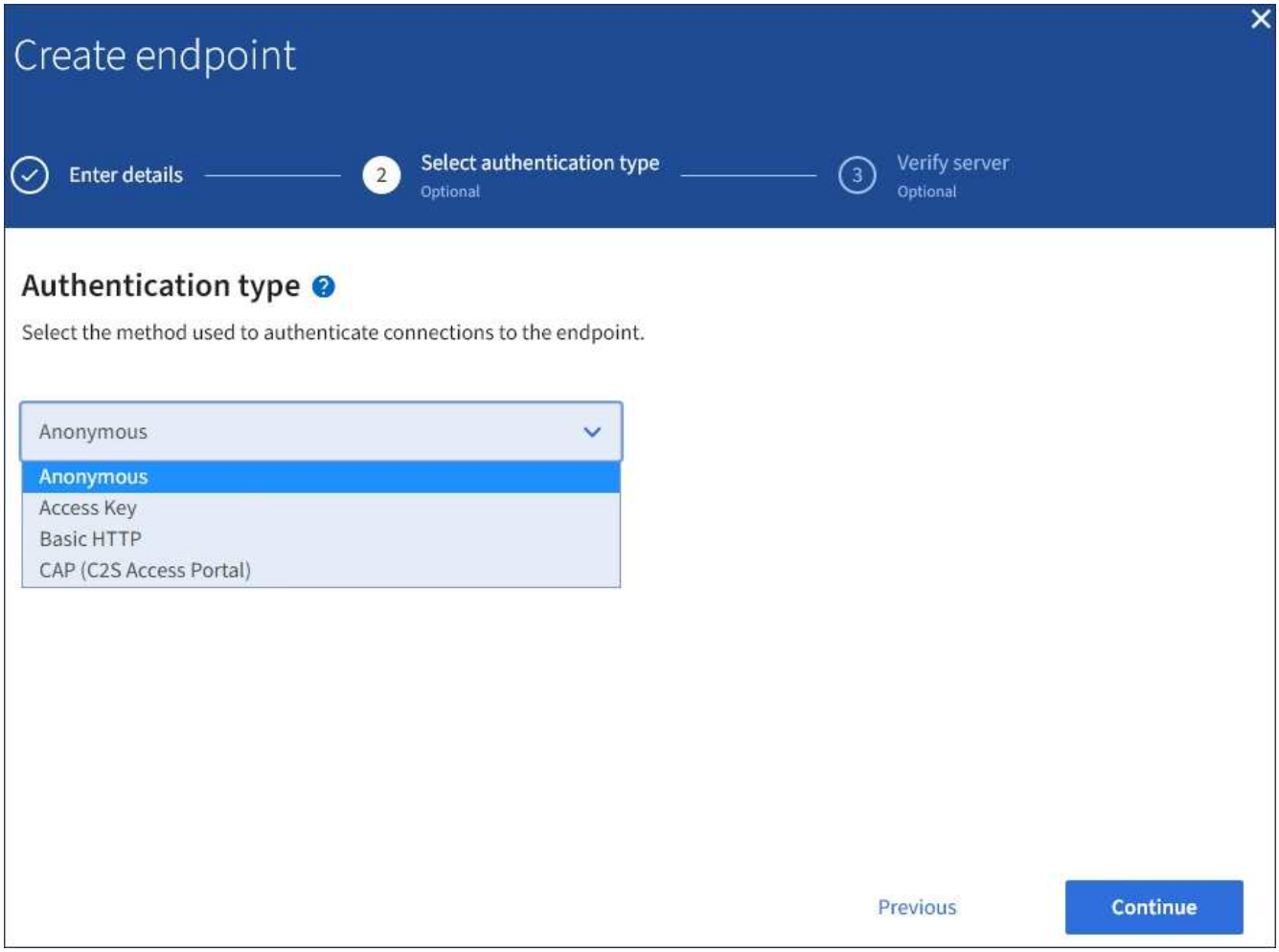
```
https://s3-aws-region.amazonaws.com
```

> Si se utiliza el extremo para el servicio de replicación de CloudMirror, no incluya el nombre de 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 es posible cambiar el URN de un extremo una vez que se creó el extremo.

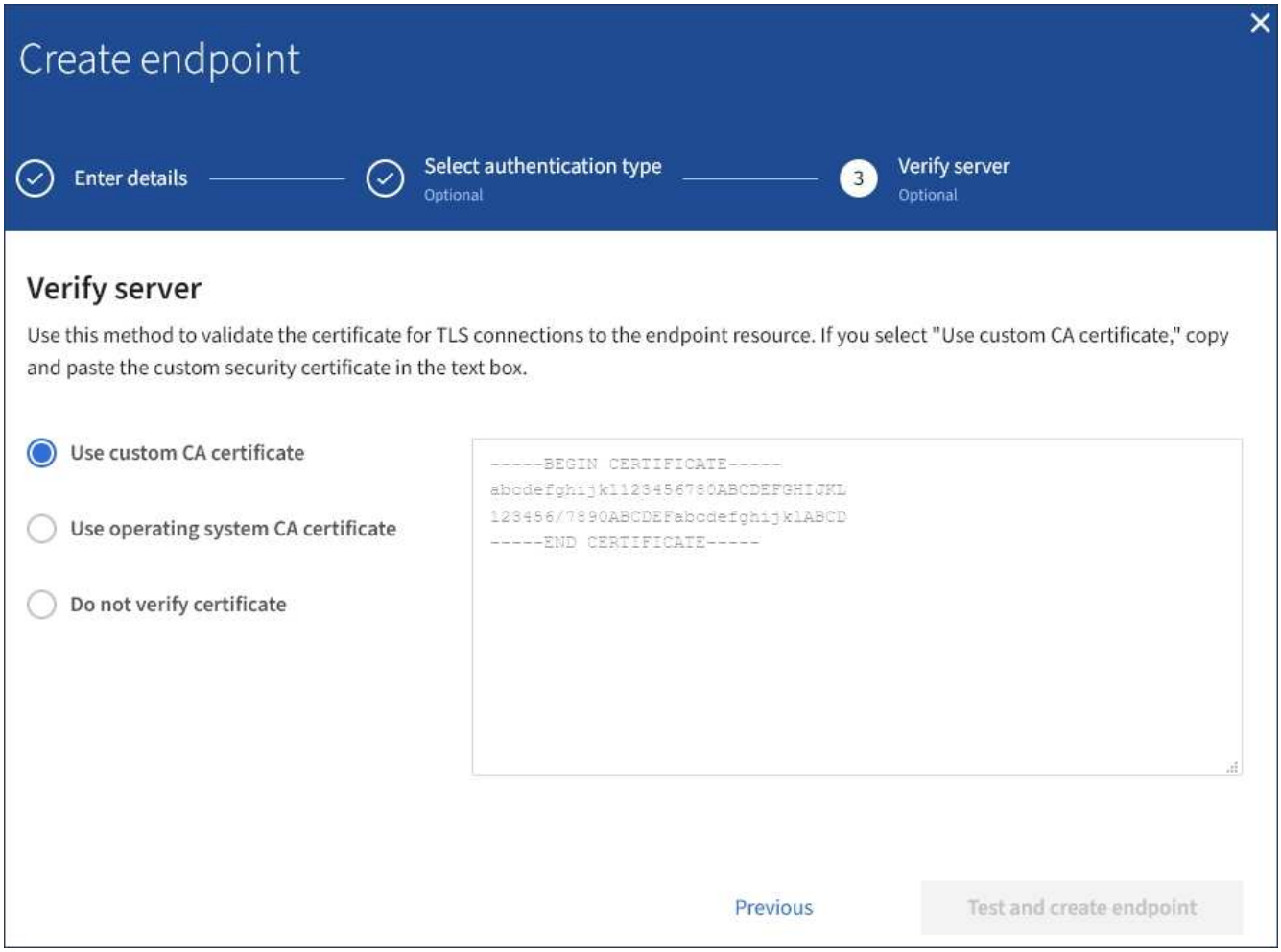
6. Seleccione **continuar**.
7. Seleccione un valor para **Tipo de autenticación** y, a continuación, introduzca o cargue las credenciales necesarias.



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)

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**.

> Se produce un error en la creación de extremos si los servicios de plataforma no están habilitados 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.

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar endpoints.

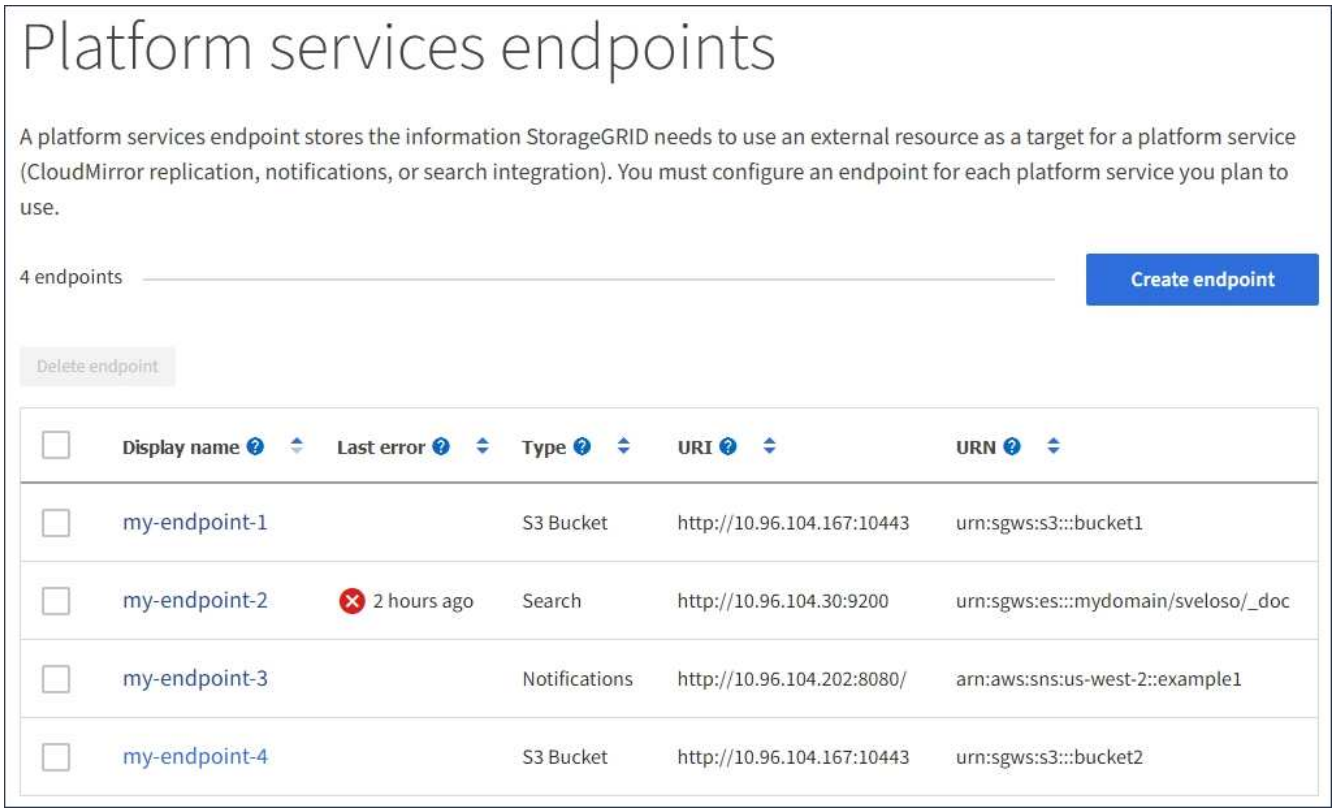
Acerca de esta tarea

StorageGRID no valida que las credenciales tengan los permisos correctos.

Pasos

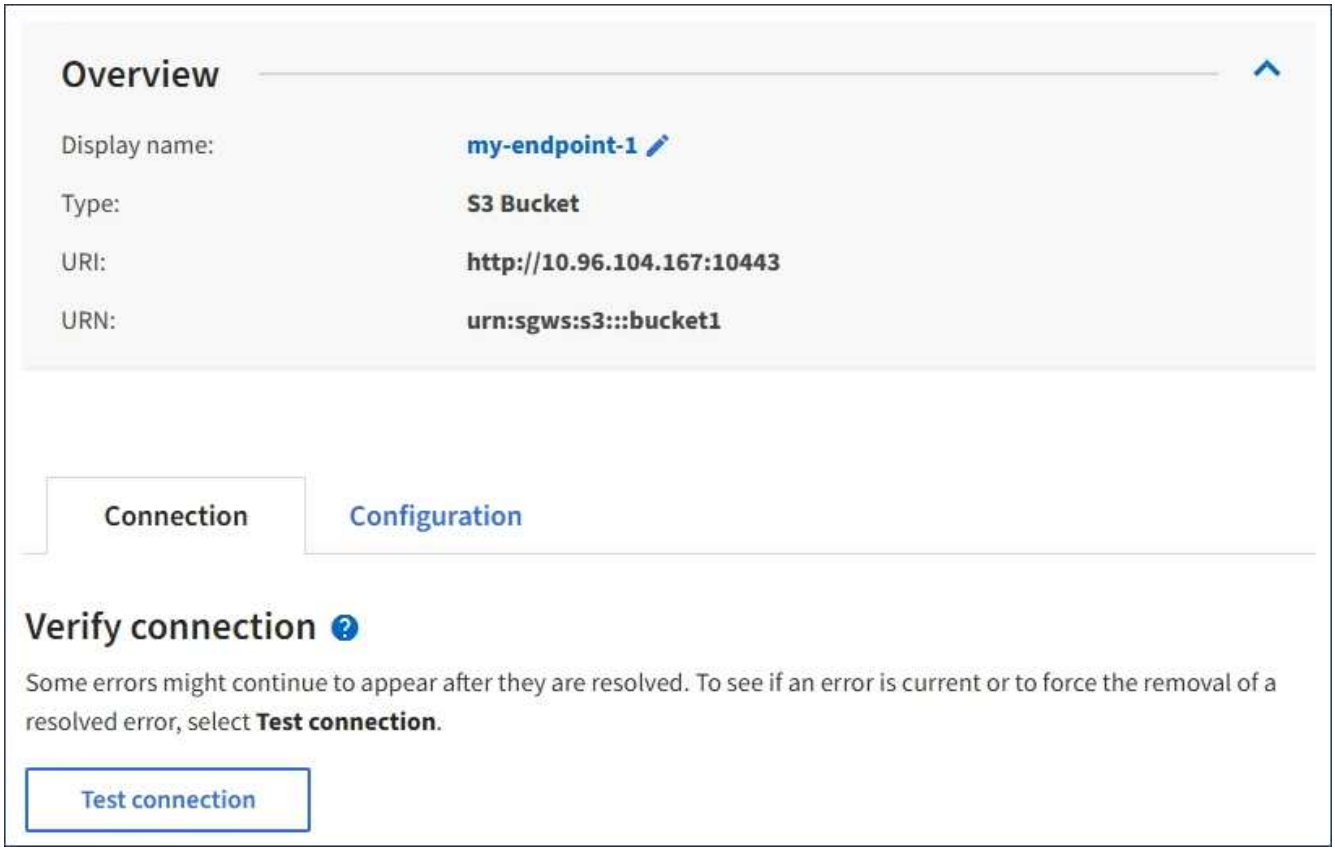
1. Seleccione **STORAGE (S3)** > **Platform Services Endpoints**.

   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 se puede cambiar el URN de un extremo de servicios de plataforma.

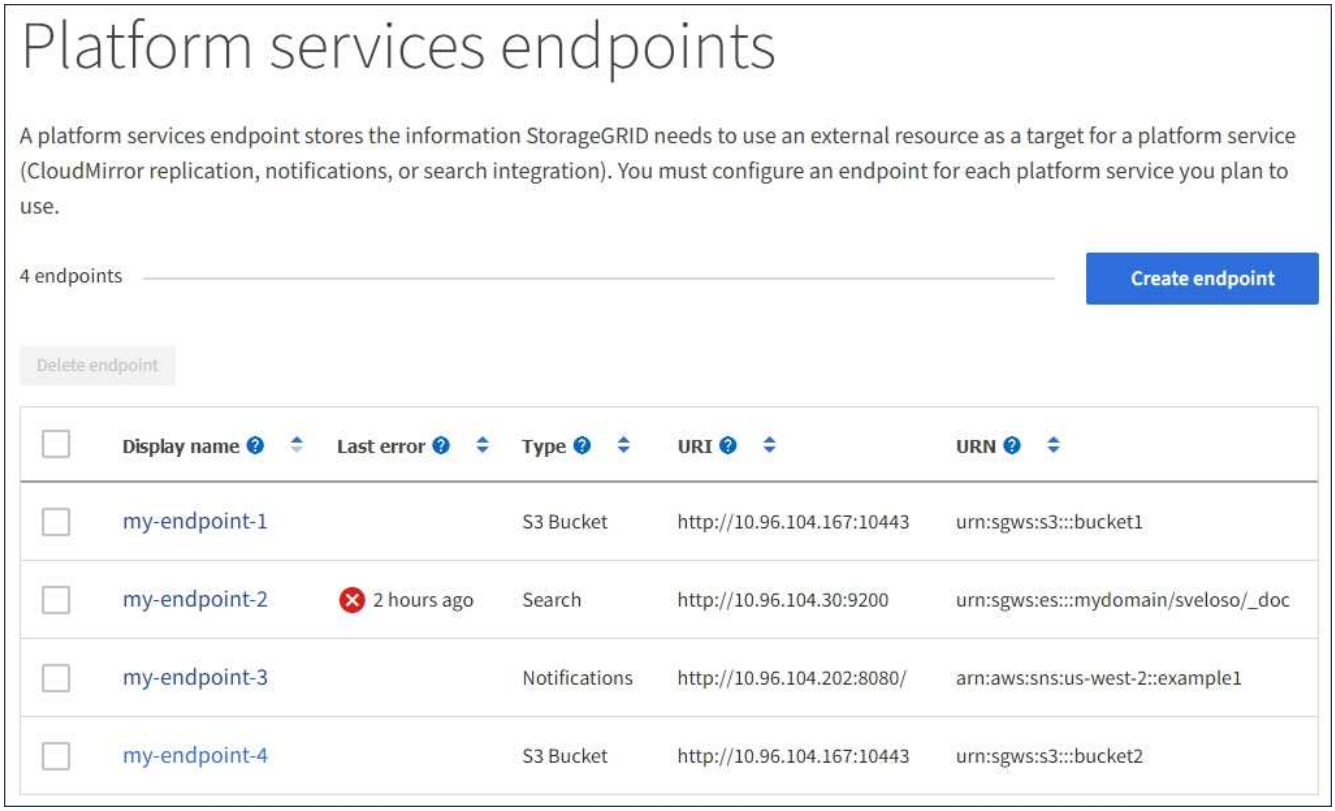
Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar endpoints. Consulte Permisos de gestión de inquilinos.

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**.

Overview

Display name: my-endpoint-3

Type: Notifications

URI: http://10.96.104.202:8080/

URN: arn:aws:sns:us-west-2::example1

Connection | Configuration

Edit configuration

Endpoint details

URI

http://10.96.104.202:8080/

URN

arn:aws:sns:us-west-2::example1

Authentication type

Basic HTTP

Username

testme

Password

••••••••

Edit password

Verify server

- Use custom CA certificate
- Use operating system CA certificate
- Do not verify certificate

```
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
```

Test and save changes

4. Según sea necesario, cambie la configuración del extremo.

> No es posible cambiar el URN de un extremo una vez que se creó el extremo.

   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 HTTP básica, cambie el nombre de usuario según sea necesario. Cambie la contraseña según sea necesario; para ello, seleccione **Editar contraseña** e introduzca la nueva contraseña. Si necesita cancelar los cambios, seleccione **Revert password 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.

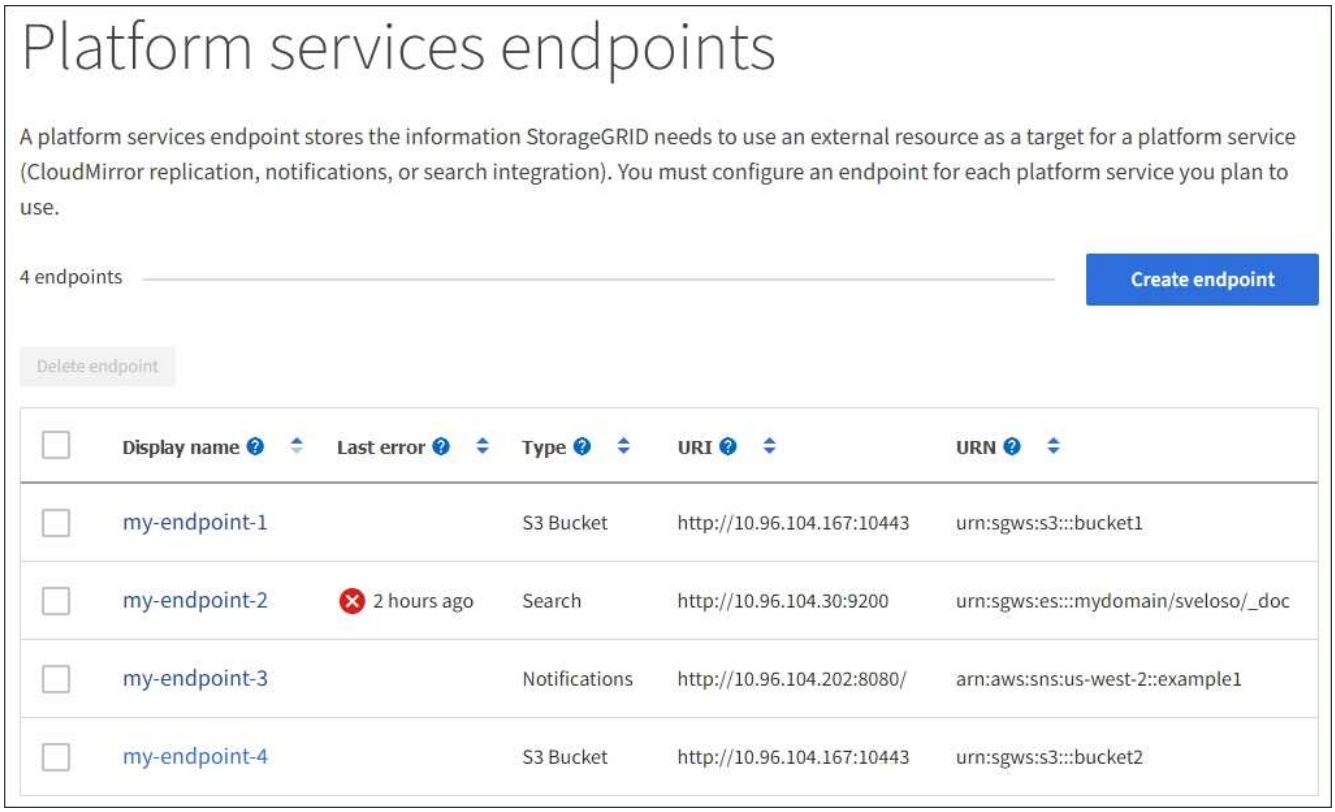
Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un navegador web compatible.
- Debe pertenecer a un grupo de usuarios que tenga el permiso **Administrar endpoints**. Consulte Permisos de gestión de inquilinos.

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.

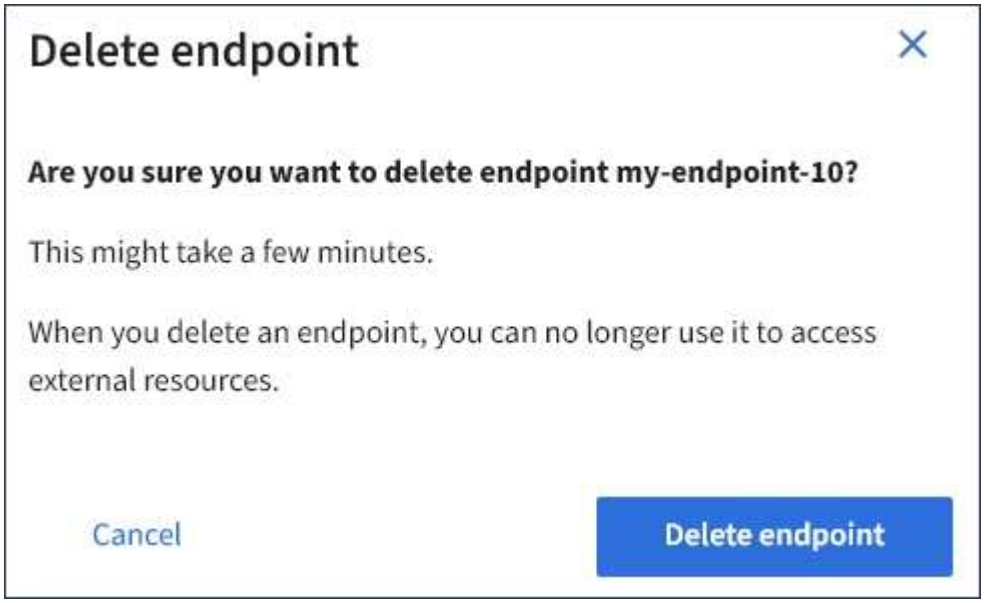


2. Seleccione la casilla de comprobación de cada extremo que desea eliminar.

> 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.



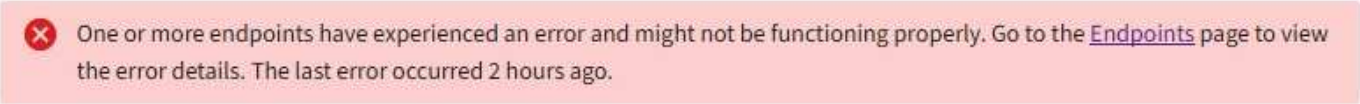
4. Seleccione **Eliminar punto final**.

Solucionar errores de extremos de servicios de plataforma

Si se produce un error cuando StorageGRID intenta comunicarse con un extremo 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

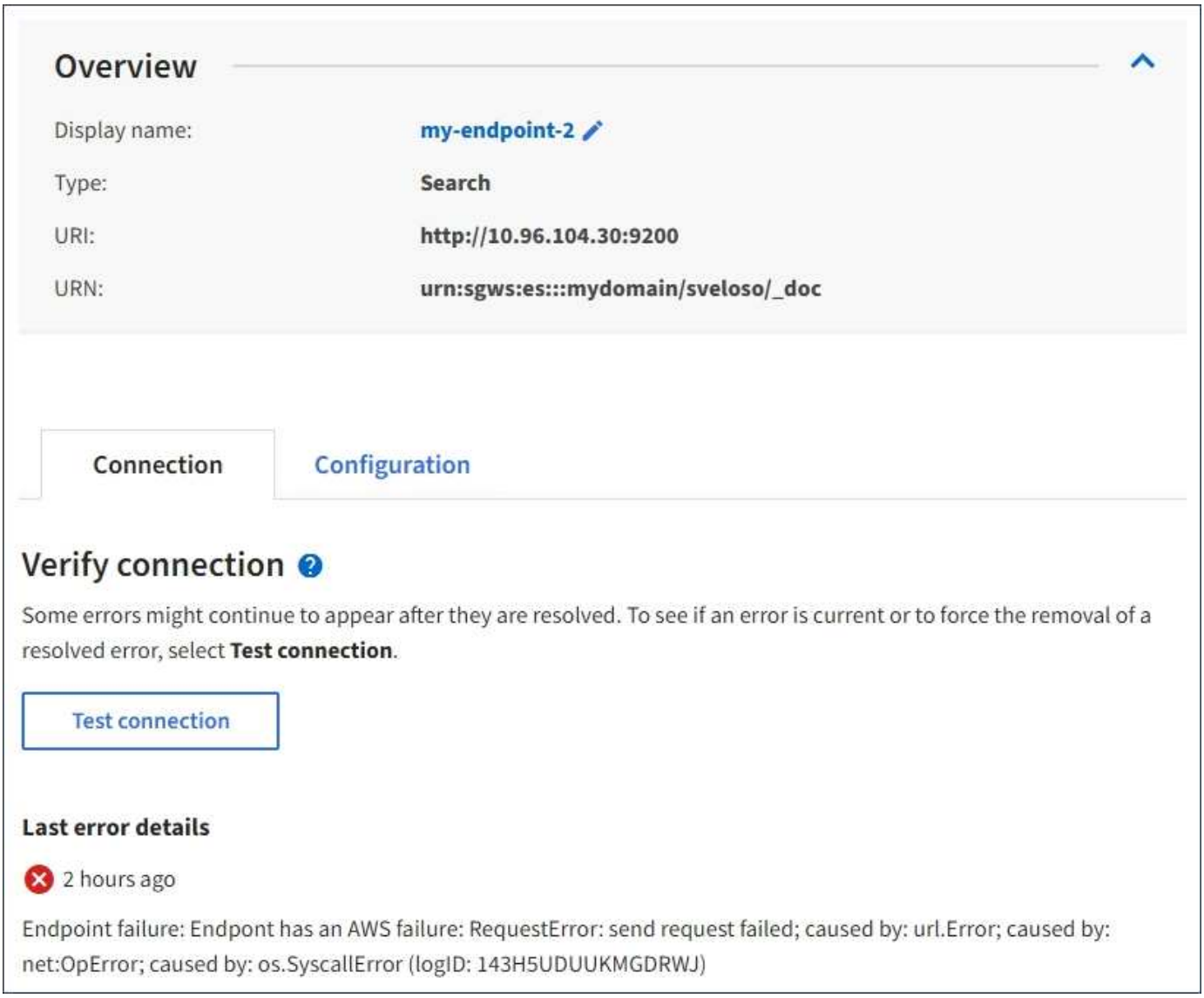
Si se han producido errores de extremo de servicios de plataforma en los últimos 7 días, la consola del administrador de inquilinos muestra un mensaje de alerta. Puede ir a la página de extremos de servicios de plataforma para ver más detalles sobre el error.



El mismo error que aparece en el panel también aparece en la parte superior de la página de extremos 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 "'es necesario actualizar las credenciales del punto final o el acceso al destino'" 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 Prohibido'"), compruebe los permisos asociados con las credenciales del punto final.

Solución de problemas de servicios de plataforma adicionales

Para obtener información adicional sobre la solución de problemas de los servicios de la plataforma, consulte las instrucciones para administrar StorageGRID.

Administre StorageGRID

Información relacionada

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.

Lo que necesitará

- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe haber creado un bloque para actuar como origen de replicación.
- El extremo que pretende usar como destino de la replicación de CloudMirror ya debe existir y debe tener su URN.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz, que le permite administrar la configuración de todos los segmentos S3 de su cuenta de inquilino. 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. Para habilitar la replicación de CloudMirror en un bloque, debe crear y aplicar un XML de configuración de replicación de bloques 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 la documentación de Amazon simple Storage Service (S3) sobre la replicación entre regiones (CRR). Para obtener más información sobre cómo StorageGRID implementa la API de configuración de la replicación de bloques de S3, consulte Instrucciones para implementar aplicaciones cliente de S3.

Si habilita la replicación de CloudMirror en un bloque que contiene objetos, se replican los objetos nuevos agregados al bloque, pero no los objetos existentes en el bloque. 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:

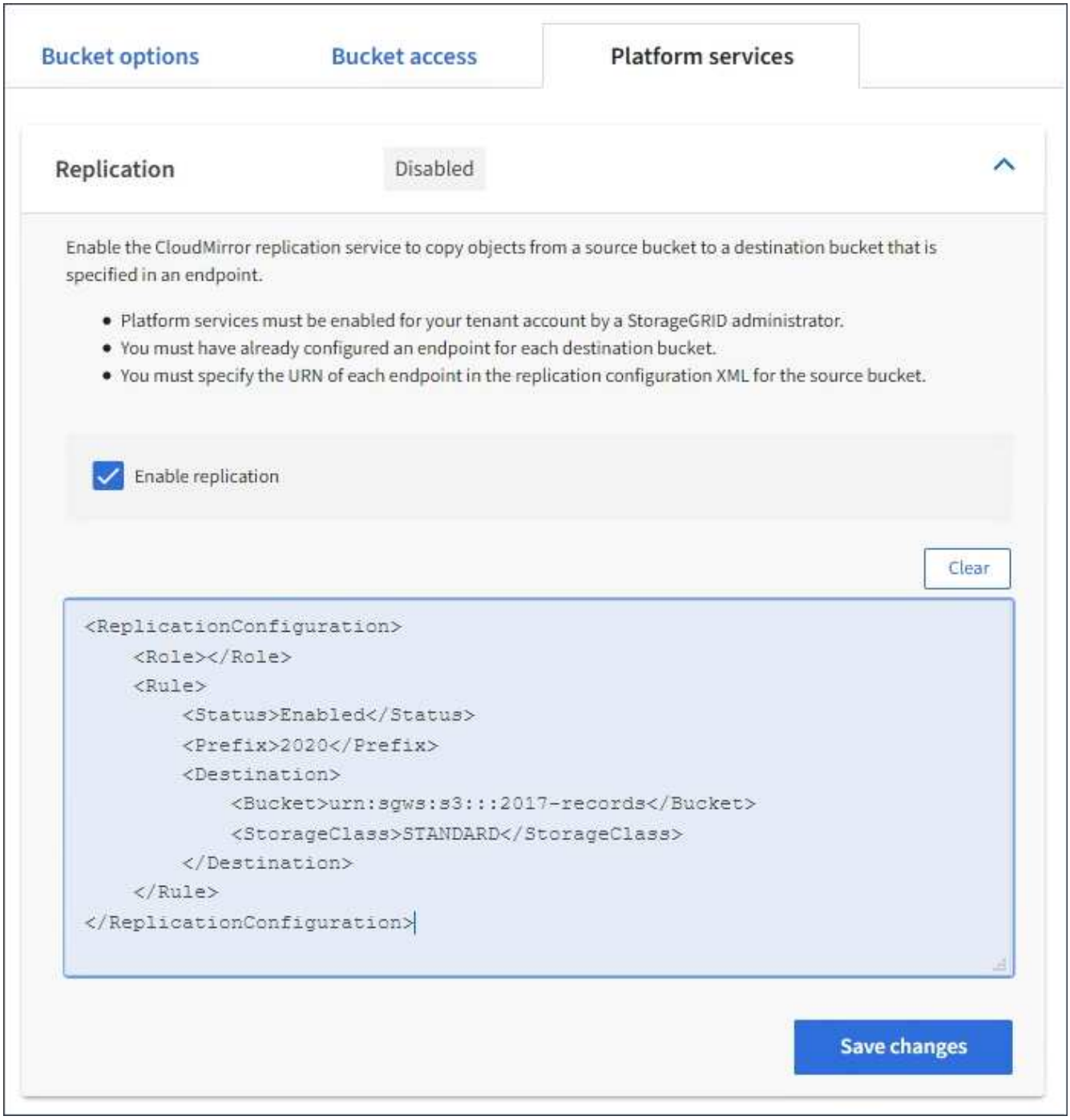
   - Tenga en cuenta que StorageGRID solo admite V1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso de `Filter` Elemento para reglas y sigue las convenciones V1 para eliminar versiones de objetos. Consulte la documentación de Amazon sobre la configuración de replicación 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 se 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. 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** > **replicación**.
5. Active la casilla de verificación **Activar 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

Use S3

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 bloque para enviar información acerca de los eventos especificados a un servicio de destino que admita AWS simple Notification Service™ (SNS).

Lo que necesitará

- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe haber creado un bloque para que actúe como el origen de las notificaciones.
- Debe haber el extremo que se pretende usar como destino de las notificaciones de eventos y su URN debe estar presente.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz, que le permite administrar la configuración de todos los segmentos S3 de su cuenta de inquilino. 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 especificado para un objeto del bloque de origen, se genera una notificación y se envía al tema Servicio de notificación simple (SNS) que se utiliza como extremo 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 más información sobre cómo StorageGRID implementa la API de configuración de notificaciones de bloques de S3, consulte las instrucciones para implementar aplicaciones de cliente 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

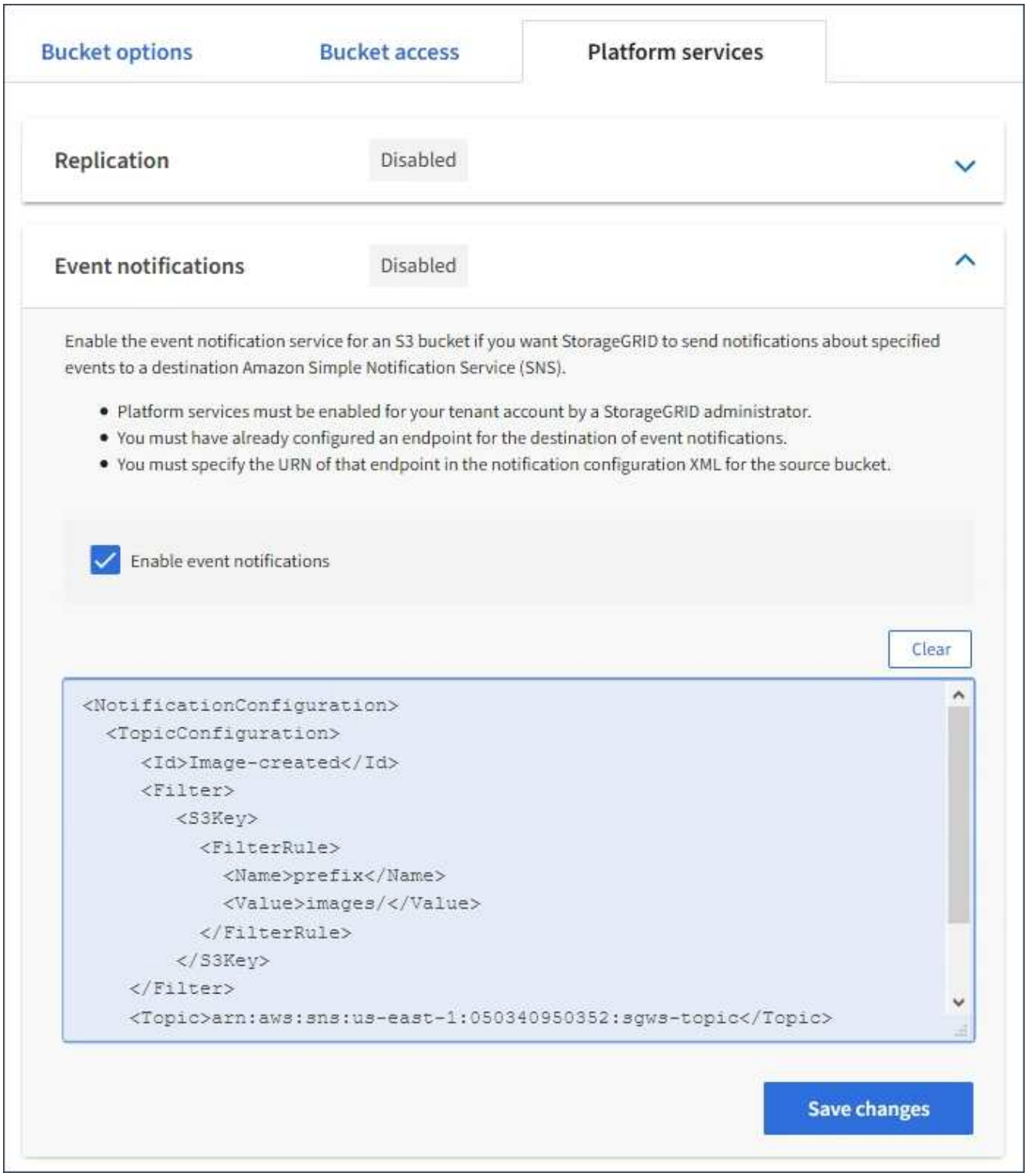
1. Habilite las notificaciones para su bloque de origen:
    - Use un editor de texto para crear el XML de configuración de notificaciones necesario para habilitar las notificaciones de eventos, como se especifica en la API de notificación de S3.
    - Al configurar XML, utilice URN de un extremo de 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. Active la casilla de verificación **Activar 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 SNS de destino.

Por ejemplo, si el tema de destino está alojado en el servicio de notificación simple (SNS) de AWS, puede configurar el servicio para que le envíe un correo electrónico cuando se entrega la notificación.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"1111111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"1111111111111111111"
               },
               "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 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 solicitud de configuración de notificación de metadatos del bloque
- PUT bucket metadata notification Configuration

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 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 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.

Lo que necesitará

- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe haber creado un bloque de S3 cuyo contenido desea indexar.
- El extremo que pretende usar como destino del servicio de integración de búsqueda ya debe existir y debe tener su URN.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz, que le permite administrar la configuración de todos los segmentos S3 de su cuenta de inquilino. 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 bloque 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.

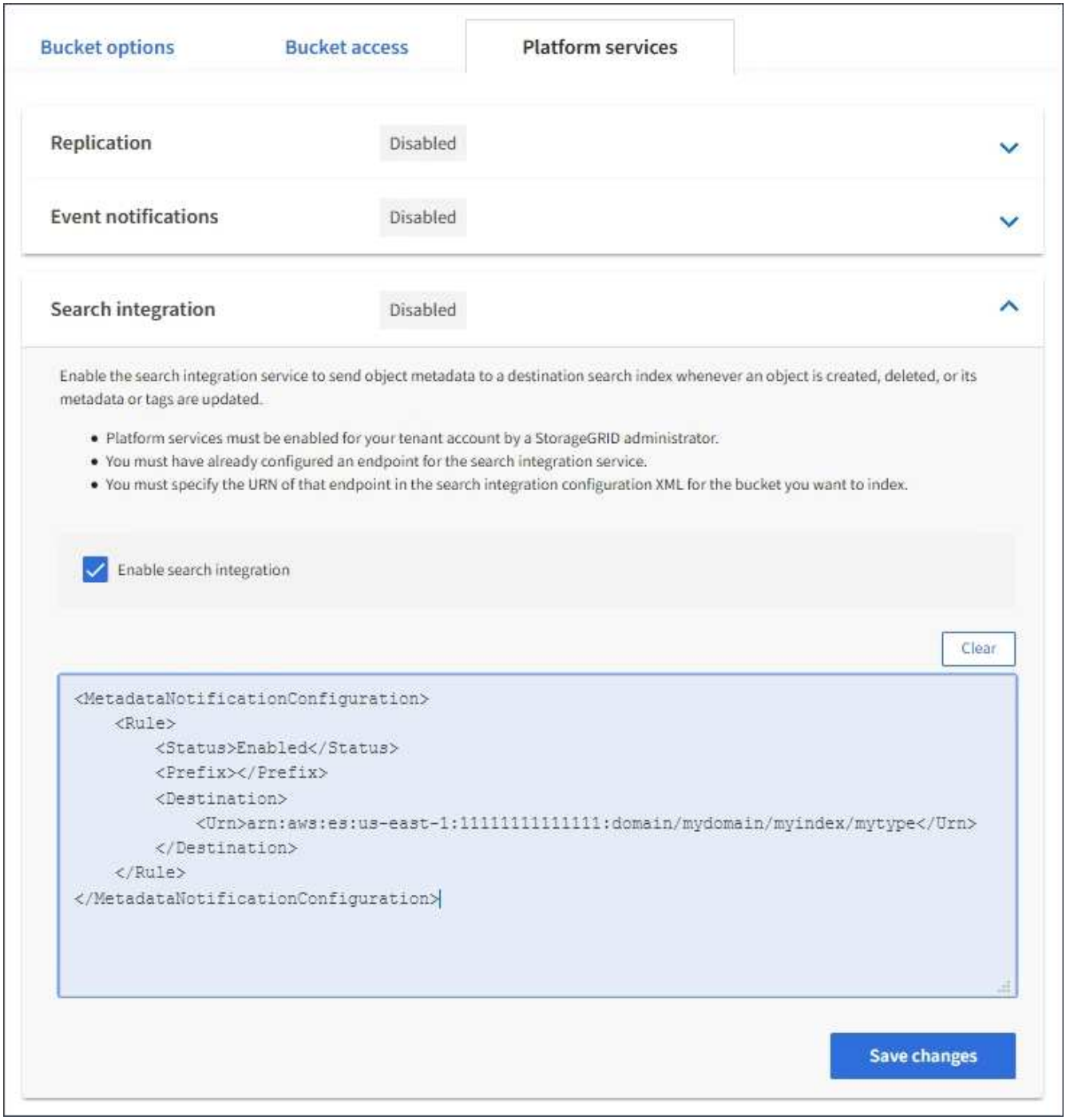
   ```
   <MetadataNotificationConfiguration>
    <Rule>
       <Status>Enabled</Status>
       <Prefix></Prefix>
       <Destination>
          <Urn>arn:aws:es:us-east-
   1:1111111111111:domain/mydomain/myindex/mytype</Urn>
          </Destination>
    </Rule>
   </MetadataNotificationConfiguration>
   ```

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. Active la casilla de verificación **Activar 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 anule la selección de 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 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. Una vez indizado un documento, no se pueden editar los tipos de campo del documento en el índice.

Use S3

Utilice S3: Descripción general

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 aplicaciones orientadas a los servicios desarrolladas para los servicios web S3 con un almacenamiento de objetos en las instalaciones que usa el sistema StorageGRID. Esto requiere cambios mínimos en el uso actual de llamadas API DE REST de S3 por parte de una aplicación cliente.

Cambios en la compatibilidad con la API DE REST de S3

Debe estar al tanto de los cambios en la compatibilidad del sistema StorageGRID con la API DE REST de S3.

Liberar	Comentarios
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. • El tamaño máximo *recommended* para una única operación PUT Object es ahora 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. En StorageGRID 11.6, el tamaño máximo *admitido* para una única operación PUT Object sigue siendo de 5 TIB (5,497,558,138,880 bytes). Sin embargo, la alerta * S3 PUT Object size demasiado grande* se activará si intenta cargar un objeto que supere los 5 GIB.
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. • Se ha agregado compatibilidad con TLS 1.3 y se ha actualizado la lista de conjuntos de cifrado TLS compatibles. • El servicio CLB está obsoleto.

Liberar	Comentarios
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. • Lista actualizada de conjuntos de cifrado TLS admitidos. 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 agregado soporte para uso compartido de recursos de origen cruzado (CORS), conexiones de clientes HTTP para S3 a nodos de grid y configuración de cumplimiento en bloques.
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 añadió compatibilidad con las restricciones de ubicación del etiquetado de objetos para bloques y la configuración de control de 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.

Versiones compatibles

StorageGRID admite las siguientes versiones específicas de S3 y HTTP.

Elemento	Versión
Especificación de S3	*Simple Storage Service referencia de API* 2006-03-01
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

"RFC de IETF 2616: Protocolo de transferencia de hipertexto (HTTP/1.1)"

"Documentación de Amazon Web Services (AWS): Referencia de API de Amazon simple Storage Service"

Soporte para servicios de plataforma StorageGRID

Los servicios de plataforma StorageGRID permiten que las cuentas de inquilinos StorageGRID aprovechen servicios externos, como un bloque de S3 remoto, un extremo de servicio de notificación simple (SNS) o un clúster de Elasticsearch para ampliar los servicios que ofrece un grid.

La tabla siguiente resume los servicios de plataforma disponibles y las API S3 que se utilizan para configurarlos.

Servicio de plataforma	Específico	API de S3 que se utiliza para configurar el servicio
Replicación de CloudMirror	Replica objetos de un bloque StorageGRID de origen en el bloque S3 remoto configurado.	PUT Bucket replication
Notificaciones	Envía notificaciones acerca de eventos en un bloque de StorageGRID de origen a un extremo de servicio simple de notificación (SNS) configurado.	NOTIFICACIÓN DE PUT Bucket
Integración de búsqueda	Envía metadatos de objetos para los objetos almacenados en un bloque de StorageGRID a un índice de Elasticsearch configurado.	PUT bucket metadata notification **Nota:** se trata de una API StorageGRID S3 personalizada.

Un administrador de grid debe habilitar el uso de los servicios de plataforma para una cuenta de inquilino

antes de poder utilizarlos. A continuación, un administrador de arrendatarios debe crear un extremo que represente el servicio remoto en la cuenta de arrendatario. Este paso es necesario para poder configurar un servicio.

Recomendaciones para el uso de servicios de plataformas

Antes de utilizar los servicios de plataforma, debe tener en cuenta las siguientes recomendaciones:

- NetApp recomienda que no permita 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.
- Si un bloque de S3 en el sistema StorageGRID tiene habilitadas las versiones y la replicación de CloudMirror, NetApp recomienda que el extremo de destino también tenga habilitada el control de versiones de bloque de S3. Esto permite que la replicación de CloudMirror genere versiones de objetos similares en el extremo.
- La replicación de CloudMirror no es compatible si el bloque de origen tiene la función S3 Object Lock habilitada.
- La replicación de CloudMirror generará un error ACCESSDENIED si el bloque de destino tiene activada la conformidad heredada.

Información relacionada

Usar cuenta de inquilino

Administre StorageGRID

Operaciones en bloques

PUT bucket metadata notification Configuration

Configure las conexiones y las cuentas de inquilino

Para configurar StorageGRID para aceptar conexiones desde aplicaciones cliente, es necesario crear una o más cuentas de inquilino y configurar las conexiones.

Cree y configure cuentas de inquilino de S3

Se requiere una cuenta de inquilino de S3 para que los clientes de la API de S3 puedan almacenar y recuperar objetos en StorageGRID. Cada cuenta de inquilino tiene su propio ID de cuenta, grupos y usuarios, y contenedores y objetos.

Las cuentas de inquilino S3 las crea un administrador de grid de StorageGRID mediante Grid Manager o la API de gestión de grid. Al crear una cuenta de inquilino de S3, el administrador de grid especifica la siguiente información:

- Nombre para mostrar del arrendatario (el ID de cuenta del arrendatario se asigna automáticamente y no se puede modificar).
- Si la cuenta de inquilino tiene permiso para utilizar los servicios de plataforma. Si se permite el uso de servicios de plataforma, la cuadrícula debe configurarse para que admita su uso.
- Opcionalmente, una cuota de almacenamiento para la cuenta de inquilino: El número máximo de gigabytes, terabytes o petabytes disponibles para los objetos del inquilino. La cuota de almacenamiento de un inquilino representa una cantidad lógica (tamaño de objeto), no una cantidad física (tamaño en disco).

- Si está habilitada la federación de identidades para el sistema StorageGRID, el grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.
- Si el sistema StorageGRID no utiliza el inicio de sesión único (SSO), tanto si la cuenta de inquilino usará su propio origen de identidad como si comparte el origen de identidad de la cuadrícula, así como la contraseña inicial del usuario raíz local del inquilino.

Una vez creada una cuenta de inquilino de S3, los usuarios de inquilinos pueden acceder al administrador de inquilinos para realizar tareas como las siguientes:

- Configure la federación de identidades (a menos que el origen de identidades se comparta con la cuadrícula) y cree grupos y usuarios locales
- Gestión de claves de acceso de S3
- Cree y gestione bloques de S3, incluidos los bloques con el bloqueo de objetos S3 habilitado
- Utilizar servicios de plataforma (si están habilitados)
- Supervise el uso del almacenamiento

> Los usuarios inquilinos S3 pueden crear y gestionar bloques de S3 con el administrador de inquilinos, pero deben tener claves de acceso S3 y usar la API REST de S3 para procesar y gestionar objetos.

Información relacionada

Administre StorageGRID

Usar cuenta de inquilino

Cómo se pueden configurar las conexiones de clientes

Un administrador de grid toma opciones de configuración que afectan a la forma en que los clientes S3 se conectan a StorageGRID para almacenar y recuperar datos. La información específica que necesita para realizar una conexión depende de la configuración elegida.

Las aplicaciones cliente pueden almacenar o recuperar objetos conectándose a cualquiera de los siguientes elementos:

- El servicio Load Balancer en los nodos de administrador o de puerta de enlace, o bien, de forma opcional, la dirección IP virtual de un grupo de alta disponibilidad (ha) de nodos de administración o nodos de puerta de enlace
- El servicio CLB en los nodos de puerta de enlace o, opcionalmente, la dirección IP virtual de un grupo de nodos de puerta de enlace de alta disponibilidad

> El servicio CLB está obsoleto. Los clientes configurados antes de la versión StorageGRID 11.3 pueden seguir utilizando el servicio CLB en los nodos de puerta de enlace. El resto de aplicaciones cliente que dependen de StorageGRID para proporcionar equilibrio de carga se deben conectar mediante el servicio Load Balancer.

- Nodos de almacenamiento, con o sin un equilibrador de carga externo

Al configurar StorageGRID, un administrador de grid puede utilizar Grid Manager o la API de gestión de grid para realizar los siguientes pasos, todos ellos opcionales:

1. Configure los extremos para el servicio Load Balancer.

Debe configurar los extremos para usar el servicio Load Balancer. El servicio Load Balancer en los nodos de administrador o de puerta de enlace distribuye conexiones de red entrantes desde aplicaciones cliente hasta los nodos de almacenamiento. Al crear un extremo de equilibrio de carga, el administrador de StorageGRID especifica un número de puerto, tanto si el extremo acepta conexiones HTTP o HTTPS, como el tipo de cliente (S3 o Swift) que utilizará el extremo y el certificado que se utilizará para las conexiones HTTPS (si procede).

2. Configure redes de cliente no fiables.

   Si un administrador de StorageGRID configura la red cliente de un nodo para que no sea de confianza, el nodo sólo acepta conexiones entrantes en la red cliente en puertos que se configuran explícitamente como extremos equilibradores de carga.

3. Configuración de grupos de alta disponibilidad.

   Si un administrador crea un grupo de alta disponibilidad, las interfaces de red de varios nodos de administrador o nodos de puerta de enlace se colocan en una configuración de backup activo. Las conexiones de clientes se realizan mediante la dirección IP virtual del grupo de alta disponibilidad.

Para obtener más información acerca de cada opción, consulte las instrucciones para administrar StorageGRID.

Información relacionada

Administre StorageGRID

Resumen: Direcciones IP y puertos para conexiones cliente

Las aplicaciones cliente se conectan a StorageGRID mediante la dirección IP de un nodo de grid y el número de puerto de un servicio en ese nodo. Si se configuran los grupos de alta disponibilidad, las aplicaciones cliente se pueden conectar mediante la dirección IP virtual del grupo de alta disponibilidad.

Información necesaria para realizar conexiones de cliente

La tabla resume las distintas maneras en que los clientes pueden conectarse a StorageGRID y las direcciones IP y los puertos que se utilizan para cada tipo de conexión. Póngase en contacto con el administrador de StorageGRID para obtener más información o consulte las instrucciones para administrar StorageGRID para obtener una descripción de cómo encontrar esta información en el administrador de grid.

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 de punto final del equilibrador de carga
Grupo de ALTA DISPONIBILIDAD	CLB **Nota:** el servicio CLB está en desuso.	La dirección IP virtual de un grupo de alta disponibilidad	Puertos S3 predeterminados: • HTTPS: 8082 • HTTP: 8084

Dónde se realiza la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
Nodo de administración	Equilibrador de carga	La dirección IP del nodo de administrador	• Puerto de punto final del equilibrador de carga
Nodo de puerta de enlace	Equilibrador de carga	La dirección IP del nodo de puerta de enlace	• Puerto de punto final del equilibrador de carga
Nodo de puerta de enlace	CLB **Nota:** el servicio CLB está en desuso.	La dirección IP del nodo de puerta de enlace **Nota:** de forma predeterminada, los puertos HTTP para CLB y LDR no están habilitados.	Puertos S3 predeterminados: • HTTPS: 8082 • HTTP: 8084
Nodo de almacenamiento	LDR	La dirección IP del nodo de almacenamiento	Puertos S3 predeterminados: • HTTPS: 18082 • HTTP: 18084

Ejemplo

Para conectar un cliente S3 al extremo de equilibrio de carga de un grupo ha de nodos de puerta de enlace, 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 de alta disponibilidad es 192.0.2.5 y el número de puerto de un extremo de equilibrio de carga de S3 es 10443, un cliente de S3 puede usar la siguiente URL para conectarse a StorageGRID:

- `https://192.0.2.5:10443`

Es posible configurar un nombre DNS para la dirección IP que utilizan los clientes para conectarse a StorageGRID. Póngase en contacto con el administrador de red local.

Información relacionada

Administre StorageGRID

Decidir usar conexiones HTTPS o HTTP

Cuando se realizan conexiones de cliente mediante un extremo de equilibrio de carga, es necesario realizar conexiones mediante el protocolo (HTTP o HTTPS) especificado para ese extremo. Para utilizar HTTP para las conexiones de clientes a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace, debe habilitar su uso.

De forma predeterminada, cuando las aplicaciones cliente se conectan a nodos de almacenamiento o al

servicio CLB en nodos de puerta de enlace, deben utilizar HTTPS cifrado para todas las conexiones. Opcionalmente, puede habilitar conexiones HTTP menos seguras seleccionando la opción de cuadrícula **Activar conexión HTTP** en el Administrador de grid. Por ejemplo, una aplicación cliente puede utilizar HTTP al probar la conexión a un nodo de almacenamiento en un entorno no de producción.

> Tenga cuidado al habilitar HTTP para una cuadrícula de producción, ya que las solicitudes se enviarán sin cifrar.

> El servicio CLB está obsoleto.

Si se selecciona la opción **Activar conexión HTTP**, los clientes deben utilizar puertos diferentes para HTTP que los que utilizan para HTTPS. Consulte las instrucciones para administrar StorageGRID.

Información relacionada

Administre StorageGRID

Ventajas de las conexiones HTTP activas, inactivas y simultáneas

Nombres de dominio extremo para solicitudes de S3

Para poder utilizar los nombres de dominio S3 para las solicitudes de cliente, un administrador de StorageGRID debe configurar el sistema para aceptar conexiones que usen nombres de dominio S3 en solicitudes de estilo de ruta de acceso S3 y de estilo virtual alojado S3.

Acerca de esta tarea

Para permitir utilizar solicitudes de estilo alojadas virtuales de S3, un administrador de grid debe realizar las siguientes tareas:

- Use Grid Manager para añadir los nombres de dominio de extremo S3 al sistema StorageGRID.
- Asegúrese de que el certificado que utiliza el cliente para las conexiones HTTPS a StorageGRID esté firmado para todos los nombres de dominio que el cliente necesita.

  Por ejemplo, si el extremo es `s3.company.com`, El administrador de grid 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 utilizado por el cliente para incluir registros DNS que coincidan con los nombres de dominio de extremo, incluidos los registros comodín necesarios.

Si el cliente se conecta mediante el servicio Load Balancer, el certificado que el administrador de grid configura es el certificado para el extremo de equilibrio de carga que utiliza el cliente.

> Cada extremo de equilibrador de carga tiene su propio certificado y cada extremo se puede configurar para reconocer diferentes nombres de dominio de extremo.

Si el cliente se conecta a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace, el certificado que el administrador de grid configura es el único certificado de servidor personalizado utilizado para la cuadrícula.

> El servicio CLB está obsoleto.

Consulte las instrucciones para administrar StorageGRID si desea obtener más información.

Una vez completados estos pasos, puede utilizar solicitudes virtuales de estilo hospedado (por ejemplo, `bucket.s3.company.com`).

Información relacionada

Administre StorageGRID

Configure la seguridad de la API DE REST

Probar configuración de la API DE REST de S3

Puede utilizar la interfaz de línea de comandos (CLI de AWS) de Amazon Web Services para probar la conexión al sistema y verificar que puede leer y escribir objetos en el sistema.

Lo que necesitará

- Ha descargado e instalado la CLI de AWS desde "aws.amazon.com/cli".
- Creó una cuenta de inquilino de S3 en el sistema StorageGRID.

Pasos

1. Configure los ajustes de Amazon Web Services para que utilicen 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 AWS para la cuenta que creó.
   c. Introduzca la clave de acceso secreto de AWS para la cuenta que ha creado.
   d. Introduzca la región predeterminada que desea 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.

```
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"
```

1. 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.

2. 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
```

3. Elimine el objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

4. 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

Una aplicación cliente puede utilizar llamadas API DE REST de S3 para conectarse a StorageGRID y crear, eliminar y modificar bloques, así como almacenar y recuperar objetos.

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.

Controles de consistencia

Los controles 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.

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 objetos en un nivel de coherencia diferente, puede especificar un control de coherencia para cada bloque o para cada operación de API.

Controles de consistencia

El control de consistencia afecta a cómo los metadatos que utiliza StorageGRID para realizar un seguimiento de los objetos se distribuyen entre los nodos y, por lo tanto, la disponibilidad de los objetos para las solicitudes del cliente.

Puede establecer el control de coherencia de un bloque o una operación API en uno de los siguientes valores:

- **Todos**: Todos los nodos reciben los datos inmediatamente, o la solicitud fallará.
- **Strong-global**: Garantiza la coherencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios.
- **Strong-site**: Garantiza la coherencia de lectura después de escritura para todas las solicitudes de cliente dentro de un sitio.
- **Read-after-new-write**: (Predeterminado) 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 depósitos S3, utilice sólo según sea necesario (por ejemplo, para un depósito que contiene valores de log que rara vez se leen, o para operaciones HEAD u GET en claves que no existen). No se admite para bloques de FabricPool S3.

Utilizar controles de coherencia «reescritura tras escritura» y «disponibles»

Cuando una OPERACIÓN HEAD u GET utiliza el control de consistencia «relativamente una vez que una nueva escritura», StorageGRID realiza la búsqueda en varios pasos, como se indica a continuación:

- Primero busca el objeto con una baja consistencia.
- Si esa búsqueda falla, repite la búsqueda en el siguiente nivel de coherencia hasta que alcanza un nivel de coherencia equivalente al comportamiento de la búsqueda global.

Si una operación HEAD u GET utiliza el control de consistencia “READ-after-new-write”, pero el objeto no existe, la búsqueda de objetos siempre alcanzará un nivel de consistencia equivalente al comportamiento de strong-global. Debido a que este nivel de coherencia requiere que haya varias copias de los metadatos del objeto disponibles en cada sitio, puede recibir un número elevado de errores del servidor interno 500 si no están disponibles dos o más nodos de almacenamiento en el mismo sitio.

A menos que necesite garantías de coherencia similares a las de Amazon S3, podrá evitar estos errores en LAS operaciones DE CABEZA y OBTENER al establecer el control de coherencia en "'Available'". Cuando un CABEZAL o UNA operación DE OBTENER utiliza el control de consistencia "'disponible'", StorageGRID sólo proporciona consistencia eventual. No vuelve a intentar una operación fallida en los niveles de coherencia crecientes, por lo que no es necesario que haya disponibles varias copias de los metadatos de objeto.

Especifique el control de coherencia para la operación de API

Para configurar el control de coherencia para una operación de API individual, deben ser compatibles los controles de coherencia para la operación y debe especificar el control de coherencia en el encabezado de la solicitud. En este ejemplo se establece el control de coherencia en «punto de referencia» para una operación GET Object.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

Debe usar el mismo control de coherencia para las operaciones PUT Object y GET Object.

Especifique el control de coherencia para el bloque

Para establecer el control de consistencia para el bloque, puede utilizar StorageGRID la solicitud de consistencia PUT Bucket y LA solicitud DE consistencia GET Bucket. También puede usar el Administrador de inquilinos o la API de gestión de inquilinos.

Cuando configure los controles de coherencia para un cucharón, tenga en cuenta lo siguiente:

- La configuración del control de coherencia para un bloque determina el control de coherencia que se utiliza para las operaciones de S3 realizadas en los objetos del bloque o en la configuración de bloques. No afecta a las operaciones del propio cucharón.
- El control de coherencia de una operación API individual anula el control de coherencia del bloque.
- En general, los cucharones deben utilizar el control de coherencia predeterminado, «entre una y otra escritura». Si las solicitudes no funcionan correctamente, cambie el comportamiento del cliente de la aplicación, si es posible. O bien, configure el cliente para especificar el control de consistencia de cada solicitud API. Establecer el control de consistencia a nivel de cucharón únicamente como último recurso.

Cómo interactúan los controles de consistencia y las reglas de ILM para afectar a la protección de datos

Tanto la elección del control de coherencia como la regla de ILM afectan a la forma en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, el control de consistencia usado cuando se almacena un objeto afecta a la colocación inicial de los metadatos de objetos, mientras que el comportamiento de procesamiento seleccionado para la regla de ILM afecta a la colocación inicial de las copias de objetos. Dado que StorageGRID requiere acceso tanto a los metadatos de un objeto como a sus datos para cumplir con las solicitudes de los clientes, seleccionar los niveles de protección correspondientes para el nivel de coherencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas más predecibles del sistema.

Para las reglas de ILM hay disponibles los siguientes comportamientos de consumo:

- **Estricto**: Todas las copias especificadas en la regla ILM deben hacerse antes de que el éxito se devuelva al cliente.
- **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.
- **Commit doble**: StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Antes de seleccionar el comportamiento de ingesta para una regla de ILM, lea la descripción completa de estas opciones de configuración en Gestión de objetos con ILM.

Ejemplo de cómo puede interactuar el control de consistencia y la regla de ILM

Suponga que tiene una cuadrícula de dos sitios con la siguiente regla de ILM y la siguiente configuración de nivel de coherencia:

- **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.
- **Nivel de coherencia**: "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 su lugar usa la misma regla de ILM y el nivel de consistencia de «otrong-site», es posible que el cliente reciba un mensaje de éxito después de replicar los datos del objeto en el sitio remoto, pero antes de que los metadatos del objeto 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 los niveles de coherencia y las reglas del ILM puede ser compleja. Póngase en contacto con NetApp si necesita ayuda.

Información relacionada

OBTENGA la solicitud de consistencia de bloque

PONER solicitud de consistencia de bloque

Cómo gestionan las reglas de ILM de StorageGRID los objetos

El administrador de grid crea reglas de gestión del ciclo de vida de la información (ILM) para gestionar los datos de los objetos que se ingieren en el sistema StorageGRID desde aplicaciones cliente de la API REST S3. A continuación, estas reglas se añaden a la política de ILM para determinar cómo y dónde se almacenan los datos de objetos con el tiempo.

La configuración de ILM determina los siguientes aspectos de un objeto:

- **Geografía**

  La ubicación de los datos de un objeto, ya sea en el sistema StorageGRID (pool de almacenamiento) o en un pool de almacenamiento en el cloud.

- **Grado de almacenamiento**

  El tipo de almacenamiento utilizado para almacenar datos de objetos, como la tecnología flash o el disco giratorio.

- **Protección contra pérdidas**

Cuántas copias se hacen y los tipos de copias que se crean: Replicación, codificación de borrado o ambos.

- **Retención**

  Los cambios se producen a lo largo del tiempo en el modo en que se gestionan los datos de un objeto, dónde se almacenan y cómo se protegen de pérdidas.

- **Protección durante la ingesta**

  El método utilizado para proteger los datos de objetos durante el procesamiento: Colocación síncrona (utilizando las opciones equilibradas o estrictas para el comportamiento de ingesta) o creación de copias provisionales (mediante la opción Dual Commit).

Las reglas de ILM pueden filtrar y seleccionar objetos. Para los objetos ingeridos mediante S3, las reglas de ILM pueden filtrar objetos en función de los siguientes metadatos:

- Cuenta de inquilino
- Nombre del bloque
- Tiempo de ingesta
- Clave
- Hora del último acceso

> De forma predeterminada, las actualizaciones del último tiempo de acceso se deshabilitan para todos los bloques S3. Si el sistema StorageGRID incluye una regla de ILM que usa la opción Last Access Time, debe habilitar las actualizaciones a la hora del último acceso para los bloques S3 especificados en esa regla. Puede habilitar las actualizaciones de la última hora de acceso mediante LA solicitud DE LA última hora de acceso DE PUT Bucket, la casilla de verificación **S3** > **Cuchos** > **Configurar la última hora de acceso** en el Administrador de inquilinos o mediante la API de administración de inquilinos. Al habilitar las actualizaciones del último tiempo de acceso, tenga en cuenta que el rendimiento de StorageGRID puede reducirse, especialmente en sistemas con objetos pequeños.

- Restricción de ubicaciones
- Tamaño del objeto
- Metadatos del usuario
- Etiqueta de objeto

Para obtener más información sobre ILM, consulte las instrucciones para gestionar objetos con la gestión del ciclo de vida de la información.

Información relacionada

Usar cuenta de inquilino

Gestión de objetos con ILM

PUT Bucket última solicitud de tiempo de acceso

Control de versiones de objetos

Puede utilizar el control de versiones para conservar varias versiones de un objeto, lo que protege contra la eliminación accidental de objetos y le 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 habilitar explícitamente el control de versiones para cada segmento a fin de activar esta funcionalidad para el bloque. A cada objeto de su 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.

En el caso de objetos S3 en bloques habilitados para versionado, la compatibilidad con versionado le permite crear reglas de ILM que usen hora no corriente como tiempo de referencia. Cuando se actualiza un objeto, sus versiones anteriores se vuelven no actuales. El uso de un filtro de tiempo no actual 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.

Consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información para ver un ejemplo de política de ILM para objetos con versiones de S3.

Información relacionada

Gestión de objetos con ILM

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 el objeto exista realmente, debe utilizar el control de consistencia "'disponible'". Por ejemplo, debe utilizar el control de

coherencia "'disponible'" si su aplicación dirige una ubicación antes DE PONERLA en práctica.

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 el control de consistencia "'Available'" para cada bloque mediante LA solicitud DE consistencia PUT Bucket, o bien puede especificar el control de consistencia en el encabezado de solicitud para una operación de API individual.

Recomendaciones para las claves de objeto

En el caso de los bloques creados en StorageGRID 11.4 o posterior, ya no es necesario restringir los nombres de claves 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 claves de objeto.

Para los bloques que se crearon en las versiones anteriores a StorageGRID 11.4, siga estas recomendaciones para los nombres de claves de objetos:

- No debe utilizar valores aleatorios como los primeros cuatro caracteres de claves de objeto. Esto contrasta con la anterior recomendación de AWS para prefijos clave. 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 clave, debe anteponer 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
  ```

Recomendaciones para «lecturas de rango»

Si se selecciona la opción **Compress Stored Objects** (**CONFIGURATION** > **System** > **Grid options**), las aplicaciones cliente S3 deberían evitar realizar operaciones GET Object que especifiquen un intervalo de bytes. Estas operaciones de «lectura de rango» son ineficientes, ya que StorageGRID debe descomprimir de forma efectiva los objetos 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.

Información relacionada

- Controles de consistencia
- PONER solicitud de consistencia de bloque
- Administre StorageGRID

Operaciones y limitaciones compatibles con la API REST de S3

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 admite encabezados de solicitud comunes definidos por la "Documentación de Amazon Web Services (AWS): Referencia de API de Amazon simple Storage Service", 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 le 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
OBTENER servicio	Se implementa con todo el comportamiento de la API DE REST de Amazon S3.
Obtenga el 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. 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.

Información relacionada

OBTENGA la solicitud de uso del almacenamiento

Operaciones en bloques

El sistema StorageGRID admite un máximo de 1,000 bloques para cada cuenta de inquilino de S3.

Las restricciones de nombres de bloque siguen las restricciones de región del estándar estadounidense de AWS, pero debe restringirlas a convenciones de nomenclatura de DNS para admitir solicitudes de estilo hospedado virtual de S3.

"Documentación de Amazon Web Services (AWS): Restricciones y limitaciones de buckets"

Configure los nombres de dominio de extremo API de S3

Las operaciones GET Bucket (List Objects) Y GET Bucket admiten los controles de coherencia de StorageGRID.

Puede comprobar si las actualizaciones a la hora del último acceso están habilitadas o deshabilitadas para grupos individuales.

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
ELIMINAR bloque	Se implementa con todo el comportamiento de la API DE REST de Amazon S3.
ELIMINAR los cors de cucharón	Esta operación elimina la configuración de CORS para el cucharón.
DELETE Bucket Encryption	Esta operación elimina el cifrado predeterminado del bloque. Los objetos cifrados existentes permanecen cifrados, pero los nuevos objetos agregados al bloque no están cifrados.
ELIMINAR ciclo de vida de bloque	Esta operación elimina la configuración del ciclo de vida del bloque.
ELIMINE la política de bloques	Esta operación elimina la política asociada al bloque.
DELETE Bucket replicación	Esta operación elimina la configuración de replicación conectada al bloque.
DELETE Bucket tagging	Esta operación utiliza `tagging` subrecurso para quitar todas las etiquetas de un bloque.

Funcionamiento	Implementación
GET Bucket (List Objects), versión 1 y versión 2	Esta operación devuelve algunos o todos (hasta 1,000) de los objetos de un bloque. 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.
GET Bucket acl	Esta operación devuelve una respuesta positiva y el ID, DisplayName y permiso del propietario del bloque, lo que indica que el propietario tiene acceso completo al bloque.
OBTENGA los cors del cucharón	Esta operación devuelve el `cors` configuración del bloque.
OBTENGA el cifrado de bloque	Esta operación devuelve la configuración de cifrado predeterminada del bloque.
OBTENGA el ciclo de vida de la cuchara	Esta operación devuelve la configuración del ciclo de vida del bloque.
OBTENER ubicación de bloque	Esta operación devuelve la región que se estableció mediante el `LocationConstraint` Elemento de la solicitud PUT Bucket. Si la región del cucharón es `us-east-1`, se devuelve una cadena vacía para la región.
OBTENGA la notificación DE BUCKET	Esta operación devuelve la configuración de notificación asociada al bloque.
OBTENGA las versiones DE objeto Bucket	Con el acceso DE LECTURA en un bloque, esta operación con el `versions` subrecurso enumera los metadatos de todas las versiones de objetos del bloque.
OBTENGA la política de bloques	Esta operación devuelve la política asociada al bloque.
OBTENGA la replicación de Bucket	Esta operación devuelve la configuración de replicación asociada al bloque.
GET Bucket tagging	Esta operación utiliza `tagging` subrecurso para devolver todas las etiquetas de un bloque.

Funcionamiento	Implementación
OBTENGA el control de versiones de Bucket	Esta implementación usa la `versioning` subrecurso para devolver el estado de control de versiones de un bloque. • *Blank*: Nunca se ha activado el control de versiones (el cucharón es "'unversioned'") • Activado: El control de versiones está activado • Suspendido: El control de versiones se ha habilitado anteriormente y se ha suspendido
OBTENER configuración de bloqueo de objeto	Esta operación devuelve el modo de retención predeterminado de bloque y el período de retención predeterminado, si está configurado. Consulte OBTENER configuración de bloqueo de objeto para obtener información detallada.
Cubo DE CABEZA	Esta operación 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.

Funcionamiento	Implementación
COLOQUE el cucharón	Esta operación crea un nuevo bloque. 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 la solicitud PUT Bucket 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 Utilice el bloqueo de objetos de S3. Debe habilitar S3 Object Lock cuando crea el bloque. No se puede añadir o deshabilitar el bloqueo de objetos de S3 después de crear un bloque. S3 Object Lock requiere el control de versiones de bloques, que se habilita automáticamente al crear el bloque.
COLOQUE los cors del cucharón	Esta operación establece la configuración de CORS para un cucharón 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`.

Funcionamiento	Implementación
PUT Bucket Encryption	Esta operación establece el estado de cifrado predeterminado de un bloque 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 `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).
CICLO de vida DE la cuchara	Esta operación crea una nueva configuración del ciclo de vida para el bloque o reemplaza 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) • NoncurrentVersionExpiración (NoncurrentDays) • Filtro (prefijo, etiqueta) • Estado • ID StorageGRID no admite estas acciones: • AbortEncompleteMultipartUpload • ExpiredObjectDeleteMarker • Transición Para comprender cómo la acción de caducidad en el ciclo de vida de un bloque interactúa con las instrucciones de colocación de ILM, consulte ""Cómo funciona ILM durante la vida de un objeto" en las instrucciones para gestionar objetos con gestión del ciclo de vida de la información. **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

NOTIFICACIÓN DE PUT Bucket	Esta operación configura notificaciones para el bloque 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 temas como destinos el Servicio de notificación simple (SNS). No se admiten extremos 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 es posible configurar una notificación para los siguientes tipos de eventos. 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 el siguiente listado:
	• **EventSource**
	
	`sgws:s3`
	
	• * AwsRegion*
	
	no incluido
	
	• **x-amz-id-2**
	
	no incluido
	
	• **arn**
	
	`urn:sgws:s3:::bucket_name`

POLÍTICA DE PUT Bucket	Esta operación establece la política asociada al bloque.

Funcionamiento	Implementación

PUT Bucket replication	Esta operación configura la replicación de CloudMirror de StorageGRID para el bloque con el XML de configuración de replicación que se proporciona 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 detalles, consulte "Documentación de Amazon S3 en la configuración de la 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.
	
	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
PUT Bucket etiquetaje	Esta operación utiliza `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.
PONER creación de versiones de bloques	Esta implementación usa 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`.
PONER configuración de bloqueo de objeto	Esta operación configura o elimina el modo de retención predeterminado de bloque 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 PONER configuración de bloqueo de objeto para obtener información detallada.

Información relacionada

Controles de consistencia

GET Bucket última solicitud de tiempo de acceso

Políticas de acceso a bloques y grupos

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

Gestión de objetos con ILM

Usar cuenta de inquilino

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 para desarrolladores 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

Si aplica una configuración del ciclo de vida a un bloque, la configuración del ciclo de vida del bloque siempre anula la configuración de ILM de StorageGRID. StorageGRID utiliza la configuración de caducidad del bloque, no de ILM, para determinar si se deben eliminar o conservar objetos específicos.

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:

- ELIMINAR ciclo de vida de bloque
- OBTENGA el ciclo de vida de la cuchara
- CICLO de vida DE la cuchara

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 sólo se aplica 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 sólo se aplica 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 del ciclo de vida, se aplica a un bloque emitiendo una solicitud PUT Bucket Lifecycle.

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 se ha aplicado correctamente una configuración del ciclo de vida al bloque, emita una solicitud GET Bucket Lifecycle. 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 PUT Object, HEAD Object o GET Object. 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 PUT Object fue emitida 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 DE OBJETO HEAD se utilizó para obtener metadatos para el mismo objeto en el bloque 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": {}
}
```

Use la retención de bloque predeterminada de Object Lock de S3

Si un bloque tiene habilitado el bloqueo de objetos S3, puede especificar un modo de retención predeterminado y el período de retención predeterminado que se aplicará a cada objeto que se agregue al bloque.

- El bloqueo de objetos de S3 se puede habilitar o deshabilitar para un bloque durante la creación de bloques.
- Si se habilita el bloqueo de objetos S3 para un bloque, puede configurar la retención predeterminada para el bloque.
- La configuración de retención predeterminada especifica:
  - Modo de retención predeterminado: StorageGRID sólo admite el modo de “CUMPLIMIENTO”.
  - Período de retención predeterminado en días o años.

OBTENER configuración de bloqueo de objeto

La solicitud GET Object Lock Configuration (OBTENER configuración de bloqueo de objeto) permite determinar si el bloqueo de objeto está habilitado para un bloque y, si está habilitado, ver si hay un modo de

retención predeterminado y un período de retención configurado para el segmento.

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.

Para completar esta operación, debe tener el permiso s3:GetBucketObjectLockConfiguration o ser la raíz de la cuenta.

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>
```

PONER configuración de bloqueo de objeto

La solicitud DE CONFIGURACIÓN DE PUT Object Lock permite modificar el modo de retención

predeterminado y el período de retención predeterminado para un bloque que tiene el bloqueo de objetos 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` 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.

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 el permiso s3:PutBucketObjectLockConfiguration o ser la raíz de la cuenta para completar esta operación.

La `Content-MD5` La cabecera de la solicitud se debe especificar en la solicitud PUT.

Ejemplo de solicitud

```
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>
```

Operaciones personalizadas en bloques

El sistema StorageGRID admite operaciones de bloques personalizadas que se añaden a la API DE REST de S3 y son específicas del sistema.

En la siguiente tabla, se enumeran las operaciones de bloque personalizadas que admite StorageGRID.

Funcionamiento	Descripción	Si quiere más información
OBTENGA coherencia de bloques	Devuelve el nivel de coherencia que se aplica a un bloque determinado.	OBTENGA la solicitud de consistencia de bloque
PONGA la consistencia del cucharón	Establece el nivel de consistencia aplicado a un bloque determinado.	PONER solicitud de consistencia de bloque
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.	GET Bucket última solicitud de tiempo de acceso
PUT Bucket última hora de acceso	Permite habilitar o deshabilitar las actualizaciones del último tiempo de acceso para un bloque en particular.	PUT Bucket última solicitud de tiempo de acceso
DELETE bucket metadata notification Configuration	Elimina el XML de configuración de notificación de metadatos asociado a un bloque en particular.	DELETE bucket metadata notification Configuration
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.	OBTENGA la solicitud de configuración de notificación de metadatos del bloque
PUT bucket metadata notification Configuration	Configura el servicio de notificación de metadatos para un bloque.	PUT bucket metadata notification Configuration
COLOQUE el cucharón con la configuración de cumplimiento	Obsoleto y no compatible: Ya no puede crear nuevos bloques con el cumplimiento de normativas habilitado.	Obsoleto: COLOQUE el cucharón con la configuración de cumplimiento
Obtenga el cumplimiento de normativas de Bucket	Obsoleto pero compatible: Devuelve la configuración de cumplimiento vigente para un bloque compatible existente.	Obsoleto: GET Bucket Compliance Request
CUMPLIR con la normativa de los bloques	Obsoleto pero compatible: Permite modificar la configuración de cumplimiento de un bloque compatible heredado.	Obsoleto: PUT Bucket Compliance Request

Información relacionada

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

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 controles de consistencia son compatibles con todas las operaciones de los objetos, con la excepción de lo siguiente:
  - OBTENER ACL de objeto
  - `OPTIONS /`
  - PONER objeto legal
  - PUT Object retention
  - SELECCIONE Contenido de objeto
- 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 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 StorageGRID a través de Swift a través de S3.

En la siguiente tabla se describe cómo StorageGRID implementa operaciones de objetos API DE REST de S3.

Funcionamiento	Implementación
ELIMINAR objeto	Autenticación multifactor (MFA) y el encabezado de respuesta `x-amz-mfa` no son compatibles. 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 un plazo de 30 segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y luego indica que el cliente se ha realizado correctamente. **Versioning** 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.
ELIMINAR varios 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.

Funcionamiento	Implementación
ELIMINAR etiquetado de objetos	Utiliza la `tagging` subrecurso para quitar todas las etiquetas de un objeto. Se implementa con todo el comportamiento de la API DE REST de Amazon S3. **Versioning** 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 borrado, se devuelve el estado "MetodNotAllowed" con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.
OBTENER objeto	OBTENER objeto
OBTENER ACL de objeto	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.
OBTENER retención legal de objetos	Utilice el bloqueo de objetos de S3
OBTENGA retención de objetos	Utilice el bloqueo de objetos de S3
GET Object tagging	Utiliza la `tagging` subrecurso para devolver todas las etiquetas de un objeto. Se implementa con todo el comportamiento de la API DE REST de Amazon S3 **Versioning** 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 borrado, se devuelve el estado "MetodNotAllowed" con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.
OBJETO HEAD	OBJETO HEAD
Restauración DE objetos posterior	Restauración DE objetos posterior
OBJETO PUT	OBJETO PUT
PONER objeto: Copiar	PONER objeto: Copiar
PONER objeto legal	Utilice el bloqueo de objetos de S3

Funcionamiento	Implementación
PUT Object retention	Utilice el bloqueo de objetos de S3
PUT Object tagging	Utiliza la `tagging` subrecurso para agregar un conjunto de etiquetas a un objeto existente. Se implementa con todo el comportamiento de la API DE REST de Amazon S3 **Límites de etiquetas 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. **Actualizaciones de etiquetas y comportamiento de procesamiento** Cuando se utiliza PUT Object tagging para actualizar las etiquetas de un objeto, StorageGRID no vuelve a procesar 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 procesamiento, no se lleva a cabo ninguna acción si no se pueden realizar las ubicaciones de objetos necesarias (por ejemplo, porque una ubicación recientemente 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 S3 comienzan una operación. **Versioning** 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 borrado, se devuelve el estado "MetodNotAllowed" con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.

Información relacionada

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

Si la opción de configuración global de bloqueo de objetos S3 se encuentra habilitada para el sistema StorageGRID, puede crear bloques con la función S3 Object Lock habilitada y, a continuación, especificar los periodos de retención predeterminados para cada bloque o la configuración específica de retención hasta la fecha y la conservación legal para cada versión de objeto que añada a ese bloque.

El bloqueo de objetos S3 permite especificar configuraciones a nivel de objeto para evitar que los objetos se eliminen o se sobrescriban por un tiempo fijo o por tiempo indefinido.

La función de bloqueo de objetos StorageGRID S3 ofrece un único modo de retención equivalente al modo de cumplimiento de normativas Amazon S3. De forma predeterminada, cualquier usuario no puede sobrescribir ni eliminar una versión de objeto protegido. La función de bloqueo de objetos StorageGRID S3 no es compatible con un modo de gobierno y no permite a los usuarios con permisos especiales omitir la configuración de retención o eliminar objetos protegidos.

Habilite S3 Object Lock para bloque

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. Es posible usar cualquiera de estos métodos:

- Cree el bloque con el Administrador de arrendatarios.

  Usar cuenta de inquilino

- Cree el segmento mediante una solicitud PUT Bucket con el `x-amz-bucket-object-lock-enabled` solicite el encabezado.

  Operaciones en bloques

No se puede añadir o deshabilitar el bloqueo de objetos de S3 después de crear el bloque. S3 Object Lock requiere el control de versiones de bloques, que se habilita automáticamente al crear el bloque.

Un bloque con S3 Object Lock habilitado puede contener una combinación de objetos con y sin la configuración de S3 Object Lock. StorageGRID admite períodos de retención predeterminados para los objetos en bloques de bloqueo de objetos de S3 y admite la operación DE bloque de configuración PUT Object Lock. La `s3:object-lock-remaining-retention-days` la clave de condición de política establece los períodos de retención mínimos y máximos permitidos para los objetos.

Determinar si se habilitó el bloqueo de objetos S3 para el bloque

Para determinar si la opción S3 Object Lock está habilitada, use OBTENER configuración de bloqueo de objeto solicitud.

Crear objeto con la configuración de Object Lock de S3

Para especificar la configuración de S3 Object Lock (bloqueo de objetos S3) al agregar una versión de objeto a un bloque que tenga habilitado el bloqueo de objetos S3, emita un objeto PUT, PUT Object - Copy o inicie una solicitud de carga de varias partes. Utilice los siguientes encabezados de solicitud.

> Debe habilitar S3 Object Lock cuando se crea un bloque. No se puede añadir o deshabilitar el bloqueo de objetos de S3 después de crear un bloque.

- `x-amz-object-lock-mode`, Que debe ser DE CUMPLIMIENTO (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 admiten 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-*` El encabezado de la solicitud está presente en LA solicitud PUT Object. `Content-MD5` No es necesario PARA PONER objeto: Copiar o iniciar carga de varias partes.
- 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 PUT Object 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 HEAD Object 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.
- Una solicitud de ELIMINACIÓN de versión de objeto o ELIMINACIÓN de objetos no se realizará correctamente si se encuentra antes de la fecha de retención o si la retención legal está activada.

Actualice la configuración de bloqueo de objetos S3

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:

- `PUT Object legal-hold`

  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.

- `PUT Object retention`
  - El valor del modo debe ser DE CUMPLIMIENTO (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 admiten 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.

Información relacionada

Gestión de objetos con ILM

Usar cuenta de inquilino

OBJETO PUT

PONER objeto: Copiar

Inicie la carga de varias partes

Control de versiones de objetos

"Guía del usuario de Amazon simple Storage Service: Uso del bloqueo de objetos de S3"

Utilice S3 Select

StorageGRID admite las siguientes cláusulas, los tipos de datos y los operadores de AWS S3 Select SelectObjectContent.

No se admiten los elementos que no aparezcan.

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 AWS 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 PUT
- PONER objeto: Copiar
- Inicie la carga de varias partes

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:

- OBTENER objeto
- OBJETO HEAD
- OBJETO PUT

- PONER objeto: Copiar
- Inicie la carga de varias partes
- Cargar artículo
- Cargar pieza: Copiar

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 de CloudMirror está configurada para el bloque, no podrá procesar objetos SSE-C. La operación de ingesta fallará.

Información relacionada

OBTENER objeto

OBJETO HEAD

OBJETO PUT

PONER objeto: Copiar

Inicie la carga de varias partes

Cargar artículo

Cargar pieza: Copiar

"Guía para desarrolladores de Amazon S3: Protección de datos mediante cifrado en el lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)"

OBTENER objeto

Puede usar la solicitud GET Object de S3 para recuperar un objeto de un bloque de S3.

OBJETOS GET y objetos de varias partes

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/multipartes y no segmentados/no multipartes; sin embargo, la `x-amz-mp-parts-count` el elemento de respuesta sólo se devuelve para objetos segmentados o multipartes.

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 incluyen en el apartado «"usar cifrado en el servidor".

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 de un objeto con caracteres UTF-8 escapados en 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 el estado "'no encontrado'" con la `x-amz-delete-marker` encabezado de respuesta establecido en `true`.

Comportamiento de OBTENER objeto para objetos de pool de almacenamiento en cloud

Si un objeto se ha almacenado en un Cloud Storage Pool (consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información), el comportamiento de una solicitud GET Object depende del estado del objeto. Consulte «'HEAD Object'» para obtener más información.

Si un objeto está almacenado en un Cloud Storage Pool y existen también una o varias copias del objeto en el grid, GET Object Requests intentará recuperar datos del grid, antes de recuperarlos del Cloud Storage Pool.

Estado del objeto	Comportamiento DE GET Object
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 una solicitud DE restauración POSTERIOR a objetos para restaurar el objeto en un estado recuperable.
Objeto en proceso de restauración a partir de un estado no recuperable	`403 Forbidden`, `InvalidObjectState` Espere a que se complete la solicitud DE restauración DE objeto POSTERIOR.
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, es posible que UNA solicitud GET Object devuelva 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:

- La solicitud GET Object puede devolver algunos datos pero detenerse a mitad de camino a través de la transferencia.
- Una petición GET Object posterior podría devolver `403 Forbidden`.

Información relacionada

Usar cifrado del servidor

Gestión de objetos con ILM

Restauración DE objetos posterior

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

OBJETO HEAD

Puede usar la solicitud del ENCABEZADO Object de S3 para recuperar metadatos de un objeto sin devolver el objeto propiamente dicho. Si el objeto se almacena en un pool de almacenamiento en el cloud, puede usar HEAD Object para determinar el estado de transición del objeto.

OBJETO DE CABECERA y objetos de varias partes

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/multipartes y no segmentados/no multipartes; sin embargo, la `x-amz-mp-parts-count` el elemento de respuesta sólo se devuelve para objetos segmentados o multipartes.

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 incluyen en el apartado «"usar cifrado en el servidor".

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 de un objeto con caracteres UTF-8 escapados en 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`

Encabezados de respuesta para objetos de Cloud Storage Pool

Si el objeto se almacena en un grupo de almacenamiento en la nube (consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información), se devuelven los siguientes encabezados 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 al OBJETO PRINCIPAL
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", expiry-date="Sat, 23 July 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.

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", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Valor para `expiry-date` se configura a una hora distante en el futuro.
	
	Nota: Si la copia de la cuadrícula no está disponible (por ejemplo, un nodo de almacenamiento está inactivo), debe emitir una solicitud DE restauración DE objetos POST para restaurar la copia desde el grupo de almacenamiento en la nube 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`

Estado del objeto	Respuesta al OBJETO PRINCIPAL

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", expiry-date="Sat, 23 July 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, es posible que una solicitud HEAD Object devuelva incorrectamente `x-amz-restore: ongoing-request="false"` 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.

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 el estado "'no encontrado'" con la `x-amz-delete-marker` encabezado de respuesta establecido en `true`.

Información relacionada

Usar cifrado del servidor

Gestión de objetos con ILM

Restauración DE objetos posterior

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

Restauración DE objetos posterior

Puede usar la solicitud DE restauración DE objetos POST de S3 PARA restaurar un objeto almacenado en un pool de almacenamiento en cloud.

Tipo de solicitud admitido

StorageGRID solo admite solicitudes POSTERIORES a la restauración de objetos 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 la restauración POSTERIOR de objetos en objetos de Pool de almacenamiento en cloud

Si un objeto se ha almacenado en un Cloud Storage Pool (consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información), una solicitud POSTERIOR de restauración de objetos tiene el siguiente comportamiento, en función del estado del objeto. Consulte «'HEAD Object'» para obtener más información.

> Si un objeto se almacena en un Cloud Storage Pool y existen también una o varias copias del objeto en la cuadrícula, no es necesario restaurar el objeto mediante la emisión de una solicitud DE restauración DE objetos POSTERIOR. En su lugar, la copia local se puede recuperar directamente, utilizando UNA solicitud GET Object.

Estado del objeto	Comportamiento DE la restauración POSTERIOR de objetos
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 puede cambiar su `expiry-date`.
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. **Atención**: Si se ha realizado la transición de un objeto a S3 Glacier Deep Archive o el Cloud Storage Pool utiliza Azure Blob Storage, no puede restaurarlo con el `Expedited` nivel. Se devuelve el siguiente error `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class`.

Estado del objeto	Comportamiento DE la restauración POSTERIOR de objetos
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 DE restauración DE objeto POSTERIOR con un nuevo valor para `Days`. La fecha de restauración se actualiza en relación con la hora de la solicitud.

Información relacionada

Gestión de objetos con ILM

OBJETO HEAD

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

OBJETO PUT

Puede usar la solicitud PUT Object de S3 para añadir un objeto a un bloque.

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 *recomendado* para una única operación PUT Object 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.

> En StorageGRID 11.6, el tamaño máximo *admitido* para una única operación PUT Object es de 5 TIB (5,497,558,138,880 bytes). Sin embargo, la alerta * S3 PUT Object size demasiado grande* se activará si intenta cargar un objeto que supere los 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 PUT, PUT Object-Copy, GET y HEAD 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 utilizar un **tiempo de creación definido por el usuario** para el tiempo de referencia y las opciones equilibradas o estrictas para el comportamiento de procesamiento. 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 estos encabezados, la configuración de retención predeterminada del bloque se utiliza para calcular la versión del objeto mantener hasta la fecha.

  Utilice 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 los siguientes encabezados 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 estricta para el comportamiento de la ingesta, la `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 ILM, StorageGRID determina si estas copias provisionales iniciales satisfacen las instrucciones de colocación en la regla. Si no lo hacen, es posible que sea necesario realizar nuevas copias de objetos en ubicaciones diferentes y que sea necesario eliminar las copias provisionales iniciales.
  - **Balanceado**: Si la regla ILM especifica la opción equilibrada y StorageGRID no puede realizar inmediatamente todas las copias especificadas en la regla, StorageGRID realiza dos copias provisionales en nodos de almacenamiento diferentes.

    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).
  - **Balanceado**: Si la regla ILM especifica la opción equilibrada, StorageGRID realiza una única copia provisional sólo 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.

Atención: Tener sólo una copia replicada durante cualquier período 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 al número de copias del objeto que se realizan cuando el objeto se evalúa mediante la política de ILM activa y no provoca que los datos se almacenen en niveles inferiores de redundancia en el sistema StorageGRID.

Nota: Si está ingiriendo un objeto en un cubo con el bloqueo de objetos S3 activado, 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.

Atención: las claves de cifrado que usted proporciona nunca se almacenan. 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 incluyen en el apartado «"usar cifrado en el servidor".

Nota: 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.

Información relacionada

Gestión de objetos con ILM

Operaciones en bloques

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

Usar cifrado del servidor

Cómo se pueden configurar las conexiones de clientes

PONER objeto: Copiar

Puede usar la solicitud PUT Object - Copy de S3 para crear una copia de un objeto que ya está almacenado en S3. UNA operación PONER objeto - copia es la misma que

realizar UNA GET y LUEGO UN PUT.

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 *recomendado* para una única operación PUT Object 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.

> En StorageGRID 11.6, el tamaño máximo *admitido* para una única operación PUT Object es de 5 TIB (5,497,558,138,880 bytes). Sin embargo, la alerta * S3 PUT Object size demasiado grande* se activará si intenta cargar un objeto que supere los 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 estos encabezados, la configuración de retención predeterminada del bloque se utiliza para calcular la versión del objeto mantener hasta la fecha.

  Utilice 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 los siguientes encabezados 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 la solicitud y afecta al número de copias de objetos que crea StorageGRID si la regla de ILM coincidente especifica un comportamiento de ingesta de COMMIT doble o de equilibrado.

- `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 PUT Object - Copy

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 se puede utilizar PONER objeto - Copiar para cifrar un objeto existente en su lugar ni 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 procesamiento, no se lleva a cabo ninguna acción si no se pueden realizar las ubicaciones de objetos necesarias (por ejemplo, porque una ubicación recientemente 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 utiliza cifrado del servidor, los encabezados de solicitud que proporcione dependerán de si el objeto de origen está cifrado y de si planea cifrar el objeto de destino.

- Si el objeto de origen se cifra utilizando una clave proporcionada por el cliente (SSE-C), debe incluir los tres encabezados siguientes en LA solicitud PUT Object - Copy, para que el objeto se pueda descifrar y copiar a continuación:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm` Especifique `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.

Atención: las claves de cifrado que usted proporciona nunca se almacenan. 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 incluyen en el apartado «"usar cifrado en el servidor".

- Si desea cifrar el objeto de destino (la copia) con una clave única administrada por StorageGRID (SSE), incluya este encabezado en LA solicitud DE PUT Object - Copy:
  - `x-amz-server-side-encryption`

Nota: la `server-side-encryption` el valor del objeto no se puede actualizar. 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 «'null'».

Información relacionada

Gestión de objetos con ILM

Usar cifrado del servidor

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

OBJETO PUT

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 "Documentación de AWS para SelectObjectContent".

Lo que necesitará

- 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 tiene el formato CSV o es un archivo comprimido GZIP o BZIP2 que contiene un archivo con formato CSV.

- 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

```
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 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 omiten.

```
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

```
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,4779736,4854803,1.5705260708959658022953568983726297854
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

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 exceder 1,000 cargas simultáneas de varias partes en un solo bloque, ya que los resultados de List Multipart cargan consultas para ese bloque pueden 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. Dado que cada parte se considera un objeto único, el uso de tamaños de pieza grandes 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 tal como se procesa y para el objeto como un todo cuando se completa la carga de varias partes, si la regla de ILM utiliza el comportamiento estricto o equilibrado del procesamiento. Debe saber cómo afecta esto a la ubicación de objetos y piezas:
  - Si ILM cambia mientras se carga varias partes de S3, es posible que cuando la carga de varias partes completa algunas partes del objeto no cumplan los requisitos actuales de ILM. Cualquier pieza que no

se haya colocado correctamente se coloca en la cola de reevaluación de ILM y se mueve posteriormente 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 cumplen 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 como un todo, todas las partes del objeto se mueven a DC1.

- Todas las operaciones de carga de varias partes admiten controles de coherencia de StorageGRID.
- Según sea necesario, puede utilizar el cifrado del servidor con cargas en varias partes. Para usar SSE (cifrado en el servidor con claves gestionadas por StorageGRID), incluye el `x-amz-server-side-encryption` Solicite el encabezado sólo en la solicitud Iniciar carga de varias partes. Para utilizar SSE-C (cifrado del servidor con claves proporcionadas por el cliente), debe especificar los mismos tres encabezados de solicitud de clave de cifrado en la solicitud de carga de varias partes iniciada y en cada solicitud de artículo de carga posterior.

Funcionamiento	Implementación
Enumerar cargas de varias partes	Consulte Enumerar cargas de varias partes
Inicie la carga de varias partes	Consulte Inicie la carga de varias partes
Cargar artículo	Consulte Cargar artículo
Cargar pieza: Copiar	Consulte Cargar pieza: Copiar
Completar carga de varias partes	Consulte Completar carga de varias partes
Cancelar carga de varias partes	Se implementa con todo el comportamiento de la API DE REST de Amazon S3
Enumerar piezas	Se implementa con todo el comportamiento de la API DE REST de Amazon S3

Información relacionada

- Controles de consistencia
- Usar cifrado del servidor

Enumerar cargas de varias partes

La operación List Multipart carga enumera las cargas de varias partes en curso para un bloque.

Se admiten los siguientes parámetros de solicitud:

- `encoding-type`
- `max-uploads`

- `key-marker`
- `prefix`
- `upload-id-marker`

La `delimiter` el parámetro request no es compatible.

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. Cuando se realiza la operación de carga de varias partes completa, ese es el punto en el que se crean objetos (y se crean versiones si procede).

Inicie la carga de varias partes

La operación 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 la opción estricta para el comportamiento de la ingesta, la `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 ILM, StorageGRID determina si estas copias provisionales iniciales satisfacen las instrucciones de colocación en la regla. Si no lo hacen, es posible que sea necesario realizar nuevas copias de objetos en ubicaciones diferentes y que sea necesario eliminar las copias provisionales iniciales.
  - **Balanceado**: Si la regla ILM especifica la opción equilibrada y StorageGRID no puede realizar inmediatamente todas las copias especificadas en la regla, StorageGRID realiza dos copias provisionales en nodos de almacenamiento diferentes.

    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).
  - **Balanceado**: Si la regla ILM especifica la opción equilibrada, StorageGRID realiza una única copia provisional sólo 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.

Atención: Tener sólo una copia replicada durante cualquier período 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 al número de copias del objeto que se realizan cuando el objeto se evalúa mediante la política de ILM activa y no provoca que los datos se almacenen en niveles inferiores de redundancia en el sistema StorageGRID.

Nota: Si está ingiriendo un objeto en un cubo con el bloqueo de objetos S3 activado, 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.

Uso del 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 información acerca de cómo StorageGRID maneja los caracteres UTF-8, consulte la documentación de PUT Object.

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 Iniciar carga de varias partes si desea cifrar el objeto con una clave única gestionada por StorageGRID. No especifique este encabezado en ninguna de las solicitudes de artículo de carga.
  - `x-amz-server-side-encryption`
- **SSE-C**: Utilice los tres encabezados de la solicitud de carga de varias partes iniciada (y en cada solicitud de artículo de carga posterior) si desea cifrar el objeto con una clave única que proporciona y gestiona.
  - `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.

Atención: las claves de cifrado que usted proporciona nunca se almacenan. 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 incluyen en el apartado «"usar cifrado en el 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 crean versiones si corresponde) cuando se realiza la operación de carga de varias partes completa.

Información relacionada

Gestión de objetos con ILM

Usar cifrado del servidor

OBJETO PUT

Cargar artículo

La operación cargar pieza 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 ha especificado el cifrado SSE-C para la solicitud de carga de varias partes iniciada, también debe incluir los siguientes encabezados de solicitud en cada solicitud de artículo de carga:

- `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 Iniciar carga de varias partes.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el mismo resumen MD5 que ha proporcionado en la solicitud Iniciar carga de varias partes.

> 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 incluyen en el apartado «"usar cifrado en el 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 crean versiones si corresponde) cuando se realiza la operación de carga de varias partes completa.

Información relacionada

Usar cifrado del servidor

Cargar pieza: Copiar

La operación cargar pieza - Copiar carga una parte de un objeto copiando datos de un objeto existente como origen de datos.

La operación cargar pieza - copia se implementa con todo el comportamiento de la API DE REST de Amazon S3.

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 ha especificado el cifrado SSE-C para la solicitud de carga de varias partes iniciada, también debe incluir los siguientes encabezados de solicitud en cada parte de carga - solicitud de copia:

- `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 Iniciar carga de varias partes.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el mismo resumen MD5 que ha proporcionado en la solicitud Iniciar carga de varias partes.

Si el objeto de origen se cifra utilizando una clave proporcionada por el cliente (SSE-C), debe incluir los tres encabezados siguientes en la solicitud cargar pieza - Copiar, para que el objeto se pueda descifrar y copiar a continuación:

- `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 incluyen en el apartado «"usar cifrado en el 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 crean versiones si corresponde) cuando se realiza la operación de carga de varias partes completa.

Completar carga de varias partes

La operación de carga de varias partes completa completa finaliza una carga de varias partes de un objeto mediante el montaje de las piezas previamente cargadas.

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 la solicitud y afecta al número de copias de objetos que crea StorageGRID si la regla de ILM coincidente especifica un comportamiento de ingesta de COMMIT doble o de equilibrado.

- `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 habilitado para un bloque, la versión del objeto se crea al finalizar 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 mensaje Last Event muestra "'error al publicar notificaciones para la clave de objeto de nombre de bloque'" del último objeto cuya notificación ha fallado. (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.

Información relacionada

Gestión de objetos con ILM

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

Nombre	Estado de HTTP
InvalidArgument	400 solicitud incorrecta
InvalidBucketName	400 solicitud incorrecta
InvalidBucketState	409 conflicto
InvalidDigest	400 solicitud incorrecta
InvalidEncryptionAlgorithmError	400 solicitud incorrecta
InvalidPart	400 solicitud incorrecta
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

Nombre	Estado de HTTP
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
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

Nombre	Descripción	Estado de HTTP
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 de la API de REST de StorageGRID S3

Existen operaciones añadidas en la API DE REST de S3 específicas del sistema StorageGRID.

- OBTENGA la solicitud de consistencia de bloque

  La solicitud DE consistencia DE GET Bucket permite determinar el nivel de consistencia que se aplica a un bloque determinado.

- PONER solicitud de consistencia de bloque

  La solicitud PUT Bucket Consistency permite especificar el nivel de coherencia que se va a aplicar a las operaciones realizadas en un bloque.

- GET Bucket última solicitud de tiempo de acceso

  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.

- PUT Bucket última solicitud de tiempo 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.

- 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.

- OBTENGA la solicitud de configuración de notificación de metadatos del bloque

  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.

- PUT bucket metadata notification Configuration

  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.

- 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.

- Solicitudes de bloques 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.

OBTENGA la solicitud de consistencia de bloque

La solicitud DE consistencia DE GET Bucket permite determinar el nivel de consistencia que se aplica a un bloque determinado.

Los controles de consistencia predeterminados se establecen para garantizar la lectura tras escritura de los objetos recién creados.

Tiene el permiso s3:GetBucketConsistency, o bien sea raíz de la cuenta, para completar esta operación.

Ejemplo de solicitud

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Respuesta

En la respuesta XML, `<Consistency>` devolverá uno de los siguientes valores:

Control de consistencia	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.

Control de consistencia	Descripción
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. La mayoría concuerda estrechamente con las garantías de coherencia de Amazon S3. **Nota:** Si su aplicación utiliza PETICIONES HEAD en objetos que no existen, puede recibir un número elevado de 500 errores de Internal Server si uno o más nodos de almacenamiento no están disponibles. Para evitar estos errores, establezca el control de coherencia en "'Available'" a menos que necesite garantías de coherencia similares a las de Amazon S3.
Disponible (coherencia eventual para operaciones DE CABEZAL)	Se comporta del mismo modo que el nivel de consistencia "read-after-new-write", pero sólo proporciona consistencia eventual para las operaciones DE CABEZA. Ofrece una mayor disponibilidad para las OPERACIONES DE CABEZAL que una «escritura tras otra» si los nodos de almacenamiento no están disponibles. Se diferencia de las garantías de coherencia de Amazon S3 solo para operaciones HEAD.

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

Controles de consistencia

PONER solicitud de consistencia de bloque

La solicitud PUT Bucket Consistency permite especificar el nivel de coherencia que se va a aplicar a las operaciones realizadas en un bloque.

Los controles de consistencia predeterminados se establecen para garantizar la lectura tras escritura de los objetos recién creados.

Tiene el permiso s3:PutBucketConsistency, o bien sea raíz de la cuenta, para completar esta operación.

Solicitud

La `x-ntap-sg-consistency` el parámetro debe contener uno de los siguientes valores:

Control de consistencia	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. La mayoría concuerda estrechamente con las garantías de coherencia de Amazon S3. **Nota:** Si su aplicación utiliza PETICIONES HEAD en objetos que no existen, puede recibir un número elevado de 500 errores de Internal Server si uno o más nodos de almacenamiento no están disponibles. Para evitar estos errores, establezca el control de coherencia en "'Available'" a menos que necesite garantías de coherencia similares a las de Amazon S3.
Disponible (coherencia eventual para operaciones DE CABEZAL)	Se comporta del mismo modo que el nivel de consistencia "read-after-new-write", pero sólo proporciona consistencia eventual para las operaciones DE CABEZA. Ofrece una mayor disponibilidad para las OPERACIONES DE CABEZAL que una «escritura tras otra» si los nodos de almacenamiento no están disponibles. Se diferencia de las garantías de coherencia de Amazon S3 solo para operaciones HEAD.

Nota: en general, se debe utilizar el valor de control de la coherencia "read-after-new-write". Si las solicitudes no funcionan correctamente, cambie el comportamiento del cliente de la aplicación, si es posible. O bien, configure el cliente para especificar el control de consistencia de cada solicitud API. Establecer el control de consistencia a nivel de cucharón únicamente como último recurso.

Ejemplo de solicitud

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Información relacionada

Controles de consistencia

GET Bucket última solicitud de tiempo de acceso

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.

Tiene el permiso s3:GetBucketLastAccessTime, o sea la raíz de la cuenta, para completar esta operación.

Ejemplo de solicitud

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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 solicitud de tiempo 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.

Tiene el permiso s3:PutBucketLastAccessTime para que un bloque, o sea la raíz de la cuenta, complete esta operación.

> 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 habilitar o deshabilitar las actualizaciones para la última hora de acceso mediante LA solicitud DE LA última hora de ACCESO DE PUT Bucket, la casilla de verificación **S3** > **Cuchos** > **Cambiar la última configuración de acceso** en el Administrador de inquilinos o la API de administración de inquilinos.

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 GET Object, GET Object ACL, GET Object Etiquetado y HEAD Object no actualizan la última hora de acceso. El objeto no se agrega a las colas para la evaluación de la gestión del ciclo de vida de la información (ILM).
- PUT Object (PONER objeto): Copie y COLOQUE las solicitudes de etiquetado de objetos que sólo actualizan los metadatos. También actualice la hora del último acceso. El objeto se agrega a las colas para la evaluación de ILM.
- Si las actualizaciones a la hora del último acceso están deshabilitadas para el bloque de origen, PUT Object - Copy Requests 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, PONER objeto - Copiar solicitudes siempre actualizar la última hora de acceso. La copia del objeto se agrega a las colas para la evaluación de ILM.
- Completar solicitudes de carga de varias partes actualizar la última hora de 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

En este ejemplo se deshabilita la hora de último acceso para un bloque.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Información relacionada

Usar cuenta de inquilino

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.

Tiene el permiso s3:DeleteBucketMetadataNotification para un bucket, o sea root de la cuenta, para completar esta operación.

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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

OBTENGA la solicitud de configuración de notificación de metadatos del bloque

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.

Tiene el permiso s3:GetBucketMetadataNotification o ser raíz de la cuenta, para completar esta operación.

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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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
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

Nombre	Descripción	Obligatorio
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 cuenta de inquilino

PUT bucket metadata notification Configuration

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.

Tiene el permiso s3:PutBucketMetadataNotification para un bloque o ser raíz de la cuenta, para completar esta operación.

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

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

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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<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

Nota: para etiquetas y metadatos de usuario, StorageGRID pasa fechas y 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. Una vez indizado un documento, no se pueden editar los tipos de campo del documento en el índice.

Información relacionada

Usar 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 puede obtenerse mediante una solicitud DE SERVICIO GET 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 sólida, StorageGRID intenta recuperar la información de uso con una coherencia de sitio sólida.

Tiene 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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 borrado no se agregan a la `ObjectCount` total.

Información relacionada

Controles de consistencia

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.

- Utilice 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: GET Bucket Compliance Request

  La solicitud DE cumplimiento GET Bucket queda obsoleta. Sin embargo, puede seguir utilizando esta solicitud para determinar la configuración de cumplimiento actual para un bloque compatible heredado existente.

- 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.

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.

> 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.

Utilice 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"

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 la solicitud PUT Bucket para cumplir con las normativas a fin de crear un nuevo bloque compatible:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Información relacionada

Gestión de objetos con ILM

Usar cuenta de inquilino

Obsoleto: GET Bucket Compliance Request

La solicitud DE cumplimiento GET Bucket queda 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.

Utilice 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"

Tiene el permiso s3:GetBucketCompliance o ser la raíz de la cuenta para completar esta operación.

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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
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 segmento no se pueden eliminar hasta que se levante la retención 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`.

Información relacionada

Gestión de objetos con ILM

Usar cuenta de inquilino

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.

Utilice 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"

Tiene 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: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
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. **Atención:** al especificar un nuevo valor para RetentionPeriodonMinutes, debe especificar un valor igual o mayor que el período de retención actual del cucharón. Una vez establecido el período de retención del segmento, no podrá disminuir dicho valor; sólo podrá aumentarlo.
LegalHold	• Cierto: Este segmento está actualmente bajo un control legal. Los objetos de este segmento no se pueden eliminar hasta que se levante la retención 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.

Nivel de coherencia para la configuración de cumplimiento de normativas

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 el nivel de consistencia **strong-global** para garantizar que todos los sitios de centros de datos y todos los nodos de almacenamiento que contienen metadatos de bloques tengan coherencia de lectura tras escritura para la configuración de cumplimiento modificada.

Si StorageGRID no puede alcanzar el nivel de consistencia **strong-global** debido a que un sitio de centro de datos o varios nodos de almacenamiento de un sitio no están disponibles, el código de estado HTTP de 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 hacer que haya suficientes nodos de almacenamiento en cada sitio disponibles, el soporte técnico puede pedirle que vuelva a intentar la solicitud fallida forzando el nivel de consistencia de **sitio seguro**.

> Nunca fuerce el nivel de consistencia de **sitio fuerte** para EL cumplimiento DE LA cuchara DE PUT a menos que usted haya sido dirigido a hacerlo por el soporte técnico y a menos que usted entienda las consecuencias potenciales de usar este nivel.

Cuando el nivel de consistencia se reduce a **sitio seguro**, StorageGRID garantiza que la configuración de cumplimiento actualizada tendrá coherencia de lectura tras escritura sólo para las solicitudes de cliente 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 coloca un bloque bajo una retención legal y fuerza un nivel de coherencia más bajo, la configuración de cumplimiento anterior del bloque (es decir, la retención legal) puede seguir vigente en algunos centros 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 del nivel de consistencia de **sitio fuerte**, 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

Usar cuenta de inquilino

Gestión de objetos con ILM

Políticas de acceso a 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 bloque**, que se configuran mediante las operaciones API Get Bucket, PUT Bucket y DELETE Bucket Policy 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.

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.

Elemento	Descripción
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, los caracteres comodín no se admiten excepto para establecer el acceso anónimo, que concede permiso a todos. Por ejemplo, el comodín (*) se establece como el valor Principal.

```
"Principal":"*"
```

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.

Información relacionada

Usar cuenta de inquilino

Configuración de control de coherencia para políticas

De forma predeterminada, cualquier actualización que realice a las directivas de grupo será consistente. Una vez que la política de grupo sea coherente, los cambios pueden tardar 15 minutos más en aplicarse, debido al almacenamiento en caché de políticas. De forma predeterminada, las actualizaciones que realice en las políticas de bloques también serán coherentes.

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 se convierta en una Lo antes posible. efectiva por motivos de seguridad.

En este caso, puede ajustar la `Consistency-Control` En la solicitud DE política PUT Bucket, o puede utilizar la solicitud DE consistencia PUT Bucket. Al cambiar el control de coherencia para esta solicitud, debe utilizar el valor **all**, que ofrece la mayor garantía de coherencia de lectura tras escritura. Si especifica cualquier otro valor de control de consistencia en un encabezado para LA solicitud DE consistencia PUT Bucket, la solicitud será rechazada. Si especifica cualquier otro valor para una solicitud DE política PUT Bucket, el valor se ignorará. Una vez que una política de bloques se vuelve coherente, los cambios pueden tardar 8 segundos más en aplicarse, debido al almacenamiento en caché de la política.

> Si establece el nivel de consistencia en **all** para forzar la aplicación de una nueva política de cucharón antes, asegúrese de volver a establecer el control de nivel de cucharón en su valor original cuando haya terminado. De lo contrario, todas las solicitudes de segmentos futuras utilizarán la configuración **all**.

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 solicitud HTTP para la operación DE política PUT Bucket debe codificarse 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.

Información relacionada

Especifique las variables en una política

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 declaraciones de política en una política de grupo no necesitan el elemento Principal porque se entiende que el grupo es el principal.
- En una política, los directores son denotados por el elemento «'Principal,'» o «'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 utiliza ahora el permiso s3:PutReplicationConfiguration para LAS acciones de replicación PUT y DELETE Bucket. StorageGRID utiliza permisos independientes para cada acción, que coinciden con la especificación original de Amazon S3.

> SE realiza UNA ELIMINACIÓN cuando se utiliza UNA PUESTA 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	COLOQUE el cucharón	
s3:DeleteBucket	ELIMINAR bloque	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:DeleteBucketMetadataNotification	DELETE bucket metadata notification Configuration	Sí
s3:DeleteBucketPolicy	ELIMINE la política de bloques	
s3:DeleteReplicationConfiguration	DELETE Bucket replicación	Sí, separe los permisos PARA PUT y DELETE*
s3:GetBucketAcl	GET Bucket ACL	
s3:GetBucketCompliance	CUMPLIMIENTO de LA normativa GET Bucket (obsoleto)	Sí
s3:GetBucketConsistency	OBTENGA coherencia de bloques	Sí
s3: GetBucketCORS	OBTENGA los cors del cucharón	
s3:GetEncryptionConfiguration	OBTENGA el cifrado de bloque	
s3:GetBucketLastAccessTime	HORA de último acceso al bloque DE GET	Sí
s3:GetBucketLocation	OBTENER ubicación de bloque	
s3:GetBucketMetadataNotification	OBTENGA la configuración de notificación de metadatos del bloque de datos	Sí
s3:GetBucketNotification	OBTENGA la notificación DE BUCKET	
s3:GetBucketObjectLockConfiguration	OBTENER configuración de bloqueo de objeto	
s3:GetBucketPolicy	OBTENGA la política de bloques	
s3:GetBucketTagging	GET Bucket tagging	
s3:GetBucketVersioning	OBTENGA el control de versiones de Bucket	
s3:GetLifecycleConfiguration	OBTENGA el ciclo de vida de la cuchara	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:GetReplicationConfiguration	OBTENGA la replicación de Bucket	
s3:ListAllMyBuckets	• OBTENER servicio • Obtenga el uso del almacenamiento	Sí, PARA OBTENER el uso del almacenamiento
s3:ListBucket	• GET Bucket (objetos de lista) • Cubo DE CABEZA • Restauración DE objetos posterior	
s3:ListBucketMultipartUploads	• Enumerar cargas de varias partes • Restauración DE objetos posterior	
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	• ELIMINAR los segmentos de cucharón† • COLOQUE los cors del cucharón	
s3:PutEncryptionConfiguration	• DELETE Bucket Encryption • PUT Bucket Encryption	
s3:PutBucketLastAccessTime	PUT Bucket última hora de acceso	Sí
s3:PutBucketMetadataNotification	PUT bucket metadata notification Configuration	Sí
s3:PutBucketNotification	NOTIFICACIÓN DE PUT Bucket	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:PutBucketObjectLockConfiguration	• COLOQUE el cucharón con el `x-amz-bucket-object-lock-enabled: true` Encabezado de solicitud (también requiere el permiso s3:CreateBucket) • PONER configuración de bloqueo de objeto	
s3:PutBucketPolicy	POLÍTICA DE PUT Bucket	
s3:PutBucketEtiquetado	• ELIMINAR etiquetado de bloque† • PUT Bucket etiquetaje	
s3:PutBucketVersioning	PONER creación de versiones de bloques	
s3:PutLipeycleConfiguration	• ELIMINAR ciclo de vida del cucharón† • CICLO de vida DE la cuchara	
s3:PutReplicationConfiguration	PUT Bucket replication	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	• Cancelar carga de varias partes • Restauración DE objetos posterior	
s3:DeleteObject	• ELIMINAR objeto • ELIMINAR varios objetos • Restauración DE objetos posterior	
s3:DeleteObjectTagging	ELIMINAR etiquetado de objetos	
s3:DeleteObjectVersionTagging	ELIMINAR etiquetado de objetos (una versión específica del objeto)	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:DeleteObjectVersion	ELIMINAR objeto (una versión específica del objeto)	
s3:GetObject	• OBTENER objeto • OBJETO HEAD • Restauración DE objetos posterior • SELECCIONE Contenido de objeto	
s3:GetObjectAcl	OBTENER ACL de objeto	
s3:GetObjectLegalHold	OBTENER retención legal de objetos	
s3:GetObjectRetention	OBTENGA retención de objetos	
s3:GetObjectTagging	OBTENER etiquetado de objetos	
s3:GetObjectVersionTagging	OBTENER etiquetado de objetos (una versión específica del objeto)	
s3:GetObjectVersion	GET Object (una versión específica del objeto)	
s3:ListMultipartUploadParts	Elementos de lista, restauración POSTERIOR al objeto	
s3:PutObject	• OBJETO PUT • PONER objeto: Copiar • Restauración DE objetos posterior • Inicie la carga de varias partes • Completar carga de varias partes • Cargar artículo • Cargar pieza: Copiar	
s3:PutObjectLegalHold	PONER objeto legal	
s3:PutObjectRetention	PUT Object retention	
s3:PutObjectEtiquetado	PONER etiquetado de objetos	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:PutObjectVersionEtiquetado	PONER etiquetado de objetos (una versión específica del objeto)	
s3:PutOverwriteObject	• OBJETO PUT • PONER objeto: Copiar • PUT Object tagging • ELIMINAR etiquetado de objetos • Completar carga de varias partes	Sí
s3:RestoreObject	Restauración DE objetos posterior	

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:
    - No se pueden sobrescribir los datos, los metadatos definidos por el usuario ni el etiquetado de objetos de S3 del objeto.
    - Se cancela cualquier operación de ingesta en curso y se devuelve un error.
    - Si se habilita el control de versiones de S3, la configuración Denegar evita QUE LAS operaciones PUT Object tagging o DELETE Object tagging modifiquen el conjunto de etiquetas 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 política actual de S3 permite sobrescribir y el permiso PutOverwriteObject se establece en Deny, el cliente no puede sobrescribir los datos de un objeto, metadatos definidos por el usuario ni el etiquetado de objetos. Además, si la casilla de verificación **evitar modificación de cliente** está activada (**CONFIGURACIÓN** > **sistema** > **Opciones de cuadrícula**), esa configuración anula la configuración del permiso PutOverwriteObject.

Información relacionada

Ejemplos de políticas de grupo S3

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).

Operadores de condición	Descripción
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.
NumericGreatertan	Compara una clave con un valor numérico basado en la coincidencia "'mayor que'".
NumericGreaterThanEquals	Compara una clave con un valor numérico basado en la coincidencia "'mayor que o igual'".
NumericLessThan	Compara una clave con un valor numérico basado en la coincidencia "'less than'".
NumericLesThanEquals	Compara una clave con un valor numérico basado en la coincidencia "'menor que o igual'".
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

Categoría	Teclas de condición aplicables	Descripción
Operadores IP	aws:SourceIp	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` se ignorará el encabezado ya que no se puede comprobar su validez.
Recurso/identidad	aws:nombre de usuario	Comparará con el nombre de usuario del remitente desde el que se envió la solicitud. Se puede utilizar para operaciones de bloques u objetos.
s3:ListBucket y. s3:ListBucketVersions permisos	s3:delimitador	Comparará con el parámetro delimitador especificado en una solicitud GET Bucket o GET Bucket Object Versions.
s3:ListBucket y. s3:ListBucketVersions permisos	s3:max-keys	Comparará con el parámetro max-keys especificado en una solicitud GET Bucket o GET Bucket Object Versions.
s3:ListBucket y. s3:ListBucketVersions permisos	s3:prefijo	Se comparará con el parámetro prefix especificado en una solicitud GET Bucket o GET Bucket Object Versions.

Categoría	Teclas de condición aplicables	Descripción
s3:PutObject	s3:retención-días restante del bloqueo de objetos	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 PUT • PONER objeto: Copiar • Inicie la carga de varias partes
s3:PutObjectRetention	s3:retención-días restante del bloqueo de objetos	Compara con la fecha de retención especificada en la solicitud DE RETENCIÓN DE objeto PUT para garantizar que se encuentra dentro del intervalo permitido.

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.

Variable	Descripción
`${aws:username}`	Utiliza la clave de nombre de usuario como la variable proporcionada.
`${s3:prefix}`	Utiliza la clave de prefijo específica del servicio como variable proporcionada.
`${s3:max-keys}`	Utiliza la clave de max-keys específica del servicio como la variable proporcionada.
`${*}`	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

Descripción de la política	Tipo de política	Comportamiento de Amazon	Comportamiento de StorageGRID
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
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
La directiva otorga a una cuenta que no es 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** > **sistema** > **Opciones de cuadrícula** y seleccione la casilla de verificación **evitar modificación de 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.
  - Añada una operación PUT Object ALLOW a la política de S3.

> Al establecer DeleteObject en DENEGAR en una directiva S3, no se impide que ILM elimine objetos cuando existe una regla como "'copias cero después de 30 días'".

> Incluso cuando se aplican todas estas reglas y políticas, no se protegen contra las escrituras simultáneas (véase 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

Gestión de objetos con ILM

Crear directivas que requieran un manejo especial

Cómo gestionan las reglas de ILM de StorageGRID los objetos

Ejemplos de políticas de grupo S3

Ejemplos de políticas de S3

Utilice los ejemplos de esta sección para crear políticas de acceso de StorageGRID para bloques y grupos.

Ejemplos de políticas de bloques de S3

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.

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, todos, incluido el anónimo, pueden enumerar objetos en el bloque y realizar operaciones Get Object en todos los objetos del bloque. Se denegarán todas las demás operaciones. Tenga en cuenta que esta directiva podría no ser particularmente útil ya que nadie, excepto la raíz de la cuenta, tiene permisos para escribir en el bloque.

```
{
  "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 los usuarios, incluido el anónimo, pueden enumerar el bloque y realizar operaciones GET Object en todos los objetos del bloque, mientras que sólo 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::9539088723000255820 2:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::9539088723000255820 2: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/*"
    }
  ]
}
```

Información relacionada

Operaciones en bloques

Ejemplos de políticas de grupo S3

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, ya que 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

Cuando utilice el Administrador de inquilinos para agregar o editar un grupo, puede seleccionar cómo desea crear la política de grupo que define qué miembros de permisos de acceso S3 de este grupo tendrán, de la siguiente manera:

- **Sin acceso S3**: Opción predeterminada. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que se conceda el acceso mediante una política de bloques. 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.
- **Personalizado**: A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto.

  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.

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 el pleno acceso sólo a su «carpeta» en un cubo

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}/*"
    }
  ]
}
```

Información relacionada

Usar cuenta de inquilino

Configure la seguridad de la API de REST

Debe revisar las medidas de seguridad implementadas para la API REST y entender cómo proteger el sistema.

Cómo proporciona StorageGRID seguridad para la API de REST

Debe entender cómo el sistema StorageGRID implementa la seguridad, la autenticación y la autorización para la API DE REST.

StorageGRID usa las siguientes medidas de seguridad.

- Las comunicaciones de cliente con el servicio Load Balancer utilizan HTTPS si HTTPS está configurado para el extremo de equilibrio de carga.

  Al configurar un extremo de equilibrio de carga, HTTP se puede habilitar opcionalmente. Por ejemplo, puede usar HTTP para pruebas u otros fines que no sean de producción. Consulte las instrucciones para administrar StorageGRID si desea obtener más información.

- De forma predeterminada, StorageGRID utiliza HTTPS para las comunicaciones del cliente con los nodos de almacenamiento y el servicio CLB en los nodos de puerta de enlace.

  Opcionalmente, HTTP se puede habilitar para estas conexiones. Por ejemplo, puede usar HTTP para

pruebas u otros fines que no sean de producción. Consulte las instrucciones para administrar StorageGRID si desea obtener más información.

> El servicio CLB está obsoleto.

- 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.

Certificados de seguridad y aplicaciones cliente

Los clientes pueden conectarse al servicio Load Balancer en los nodos de Gateway o de administrador, directamente a los nodos de almacenamiento o al servicio CLB en los nodos de Gateway.

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, lo hacen utilizando el certificado que se configuró para el extremo de equilibrio de carga específico utilizado para realizar la conexión. Cada extremo tiene su propio certificado, que es 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 extremo.
- Cuando las aplicaciones cliente se conectan directamente a un nodo de almacenamiento o al servicio CLB en los nodos de puerta de enlace, utilizan los certificados de servidor generados por el sistema que se generaron para los nodos de almacenamiento cuando se instaló el sistema StorageGRID (firmados por la autoridad de certificación del sistema), o un único certificado de servidor personalizado que un administrador de grid suministra para la cuadrícula.

Los clientes deben configurarse para que confíen en la entidad emisora de certificados que firmó el certificado que utilicen para establecer conexiones TLS.

Consulte las instrucciones para administrar StorageGRID para obtener información sobre la configuración de extremos de equilibrador de carga y para obtener instrucciones sobre cómo agregar un único certificado de servidor personalizado para conexiones TLS directamente a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace.

Resumen

En la siguiente tabla, se muestra cómo se implementan los problemas de seguridad en 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

Problema de seguridad	Implementación de la API DE REST
Autentificación de clientes	• S3: Cuenta de S3 (ID de clave de acceso y clave de acceso secreta) • Swift: Cuenta de Swift (nombre de usuario y contraseña)
Autorización de cliente	• S3: Propiedad de bloque y todas las políticas de control de acceso aplicables • Swift: Acceso a roles de administrador

Información relacionada

Administre StorageGRID

Algoritmos de cifrado y hash compatibles para bibliotecas TLS

El sistema StorageGRID admite un conjunto limitado de conjuntos de cifrado que las aplicaciones cliente pueden utilizar al establecer una sesión de seguridad de la capa de transporte (TLS).

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.

Paquetes de cifrado compatibles

Versión TLS	Nombre IANA de conjunto cifrado
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
1.2	TLS_ECDHE_RSA_WITH_CHA20_POLY1305_SHA 256
1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
1.3	TLS_CHA20_POLY1305_SHA256
1.3	TLS_AES_128_GCM_SHA256

Suites de cifrado obsoletas

Los siguientes conjuntos de cifrado están desaprobados. La compatibilidad con estos cifrados se eliminará en una versión futura.

Nombre de IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Información relacionada

Cómo se pueden configurar las conexiones de clientes

Supervisar y auditar operaciones

Puede supervisar las cargas de trabajo y las eficiencias de las operaciones del cliente al ver las tendencias de las transacciones de todo el grid o de nodos específicos. Puede utilizar mensajes de auditoría para supervisar las operaciones y transacciones del cliente.

Supervise las tasas de procesamiento y recuperación de objetos

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.

Pasos

1. Inicie sesión en Grid Manager mediante una navegador web compatible.
2. En la consola, busque la sección Operaciones de protocolo.

   En esta sección se resume el número de operaciones de cliente que realiza su sistema StorageGRID. La media de las tasas de protocolo se hace durante los últimos dos minutos.

3. Seleccione **NODES**.
4. En la página de inicio de nodos (nivel de implementación), haga clic en la ficha **Load Balancer**.

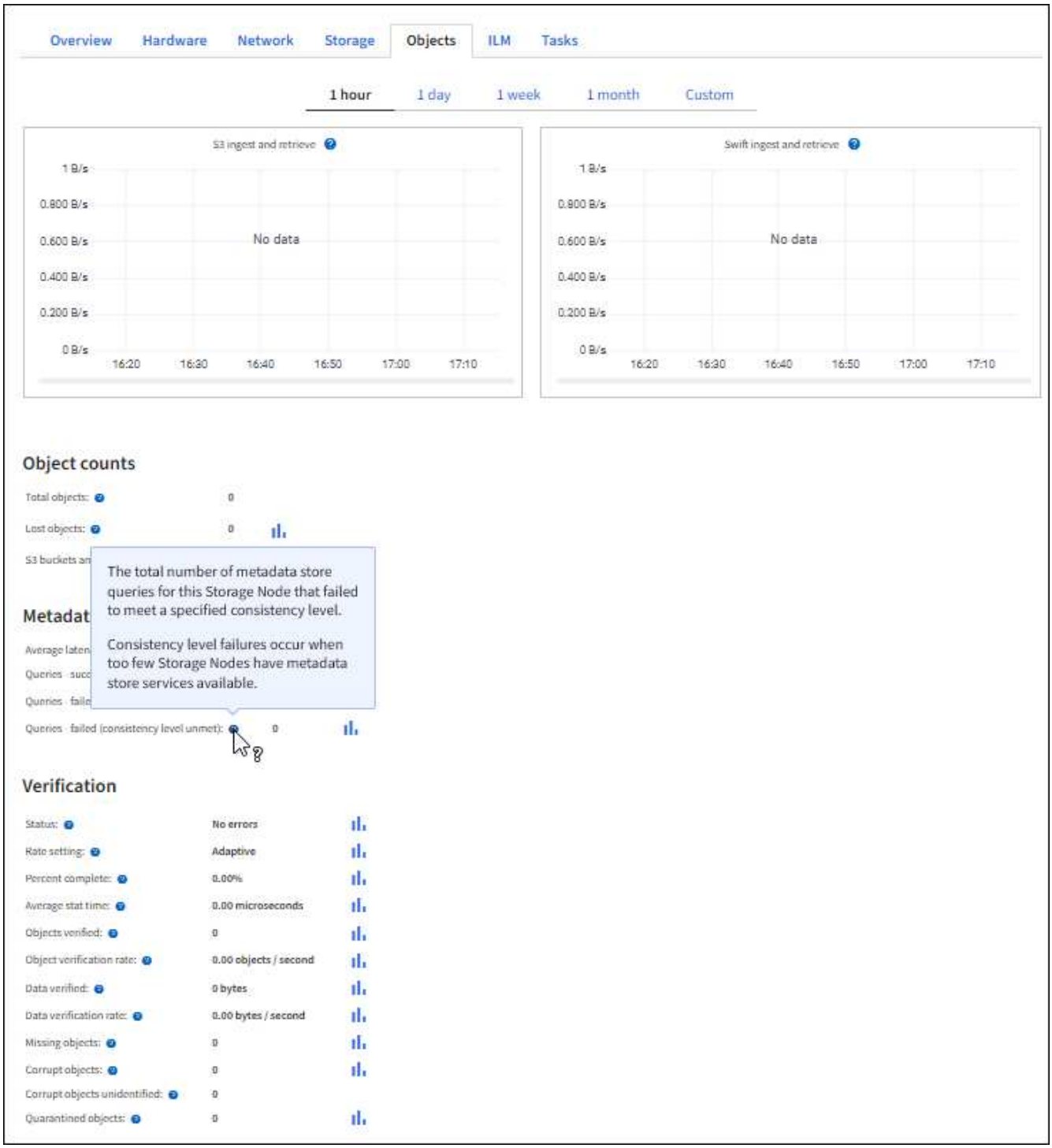
   Los gráficos muestran tendencias para todo el tráfico de cliente dirigido a los extremos de equilibrador de carga dentro de la cuadrícula. Es posible seleccionar un intervalo de tiempo en horas, días, semanas, meses o años. también puede aplicar un intervalo personalizado.

5. En la página de inicio de nodos (nivel de implementación), haga clic en la ficha **objetos**.

   El gráfico muestra las tasas de procesamiento y recuperación de todo el sistema StorageGRID en bytes por segundo y bytes totales. Es posible seleccionar un intervalo de tiempo en horas, días, semanas, meses o años. también puede aplicar un intervalo personalizado.

6. Para ver información sobre un nodo de almacenamiento en particular, seleccione el nodo en la lista de la izquierda y haga clic en la ficha **objetos**.

   El gráfico muestra las tasas de procesamiento y recuperación de objetos de este nodo de almacenamiento. La pestaña también incluye métricas para el recuento de objetos, consultas y verificación. Puede hacer clic en las etiquetas para ver las definiciones de estas métricas.



7. Si desea aún más detalles:
   a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
   b. Seleccione ***site*** > **Descripción general** > **Principal**.

      La sección API Operations muestra información resumida de la cuadrícula completa.

   c. Seleccione ***Storage Node*** > **LDR** > ***Client Application*** > **Overview** > **Main**

      La sección Operaciones muestra información de resumen del nodo de almacenamiento seleccionado.

Acceder y revisar registros de auditoría

Los servicios de StorageGRID generan los mensajes de auditoría y se almacenan en archivos de registro de texto. Los mensajes de auditoría específicos de API de los registros de auditoría ofrecen datos críticos de seguridad, operación y supervisión del rendimiento que pueden ayudar a evaluar el estado del sistema.

Lo que necesitará

- Tiene permisos de acceso específicos.
- Usted tiene la `Passwords.txt` archivo.
- Conoce la dirección IP de un nodo de administrador.

Acerca de esta tarea

Se denomina el archivo de registro de auditoría activo `audit.log`, Y se almacena en los nodos Admin.

Una vez al día, se guarda el archivo audit.log activo, y otro 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.

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
```

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.
2. Vaya al directorio que contiene los archivos del registro de auditoría:

   ```
   cd /var/local/audit/export
   ```

3. Ver el archivo de registro de auditoría actual o guardado, según sea necesario.

Se realizó un seguimiento de las operaciones de S3 en los registros de auditoría

Se realiza un seguimiento de varias operaciones de bloques y de objetos en los registros de auditoría de StorageGRID.

Se realizó un seguimiento de las operaciones de bloque en los registros de auditoría

- ELIMINAR bloque
- DELETE Bucket tagging
- ELIMINAR varios objetos
- GET Bucket (objetos de lista)
- OBTENGA las versiones DE objeto Bucket
- GET Bucket tagging
- Cubo DE CABEZA
- COLOQUE el cucharón
- CUMPLIR con la normativa de los bloques
- PUT Bucket etiquetaje
- PONER creación de versiones de bloques

Se realizó un seguimiento de las operaciones de objetos en los registros de auditoría

- Completar carga de varias partes
- Cargar pieza (cuando la regla ILM usa los comportamientos de consumo estrictos o equilibrados)
- Cargar pieza: Copia (cuando la regla ILM usa los comportamientos de ingesta estrictos o equilibrados)
- ELIMINAR objeto
- OBTENER objeto
- OBJETO HEAD
- Restauración DE objetos posterior
- OBJETO PUT
- PONER objeto: Copiar

Información relacionada

Operaciones en bloques

Operaciones en objetos

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 directamente a nodos de almacenamiento o al servicio CLB (obsoleto) en nodos de puerta de enlace, 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 conexiones de clientes a nodos de almacenamiento o al servicio CLB, limitar las conexiones HTTP activas proporciona las siguientes ventajas:

- Permite un balanceo de carga óptimo en el sistema StorageGRID.

  Cuando utilice el servicio CLB, debe evitar conexiones TCP/IP de larga duración-para optimizar el equilibrio de carga en todo el sistema StorageGRID. Debe configurar las aplicaciones cliente para realizar un seguimiento de la duración de cada conexión HTTP y cerrar la conexión HTTP después de una hora establecida para que la conexión HTTP se pueda restablecer y reequilibrar.

  El servicio CLB equilibra la carga a través del sistema StorageGRID en el momento en que una aplicación cliente establece una conexión HTTP. 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.

El servicio CLB está obsoleto.

- 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 cliente no es limitada, las conexiones activas pueden tardar varios minutos en terminarse 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.

Use Swift

Use Swift: Descripción general

Las aplicaciones cliente pueden usar la API Swift de OpenStack para interactuar con el sistema StorageGRID.

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, consulte 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
11.6	Cambios editoriales menores.

Liberar	Comentarios
11.5	Se ha eliminado el control de consistencia débil. En su lugar, se utilizará el nivel de consistencia disponible.
11.4	Se ha agregado compatibilidad con TLS 1.3 y se ha actualizado la lista de conjuntos de cifrado TLS compatibles. CLB está en desuso. Se añadió la descripción de la relación entre ILM y la configuración de 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. Lista actualizada de conjuntos de cifrado TLS admitidos. 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 controles de coherencia.
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 se han ingerido objetos Swift en el sistema StorageGRID, se gestionan con las reglas de gestión de ciclo de vida de la información (ILM) de la política de ILM activa del sistema. Las reglas y políticas de ILM determinan la manera en que StorageGRID crea y distribuye copias de datos de objetos y la manera en que las administra. 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 administrador de StorageGRID si necesita comprender cómo las políticas y las reglas de ILM de la cuadrícula afectarán a los objetos de la cuenta de inquilino de 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. 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.

StorageGRID también le permite controlar la coherencia de cada contenedor. Puede cambiar el control de coherencia para proporcionar un equilibrio entre la disponibilidad de los objetos y la coherencia de esos objetos en diferentes nodos de almacenamiento y sitios, según lo requiera la aplicación.

Información relacionada

Gestión de objetos con ILM

OBTENGA la solicitud de consistencia del contenedor

PONGA la solicitud de consistencia del contenedor

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 de forma rutinaria si existe un objeto en una ruta en la que no espera que el objeto exista realmente, debe utilizar el control de consistencia "'disponible'". Por ejemplo, debe utilizar el control de coherencia "'disponible'" si la aplicación realiza una OPERACIÓN HEAD a una ubicación antes de realizar una operación PUT 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 el control de coherencia "'disponible'" para cada contenedor utilizando la solicitud DE

consistencia DEL contenedor PUT.

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 se selecciona la opción **Compress Stored Objects** (**CONFIGURATION** > **System** > **Grid options**), las aplicaciones cliente Swift deberían evitar realizar operaciones GET object que especifiquen un intervalo de bytes. Estas operaciones de «lectura de rango» son ineficientes, ya que StorageGRID debe descomprimir de forma efectiva los objetos 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.

Información relacionada

OBTENGA la solicitud de consistencia del contenedor

PONGA la solicitud de consistencia del contenedor

Administre StorageGRID

Configure las conexiones y las cuentas de inquilino

Para configurar StorageGRID para aceptar conexiones desde aplicaciones cliente, es necesario crear una o más cuentas de inquilino y configurar las conexiones.

Cree y configure cuentas de inquilino de Swift

Se requiere una cuenta de inquilino de Swift para que los clientes de la API de Swift puedan almacenar y recuperar objetos en StorageGRID. Cada cuenta de inquilino tiene su propio ID de cuenta, grupos y usuarios, y contenedores y objetos.

Las cuentas de inquilino de Swift las crea un administrador de grid de StorageGRID mediante Grid Manager o la API de gestión de grid.

Al crear una cuenta de inquilino de Swift, el administrador de grid especifica la siguiente información:

- Nombre para mostrar del inquilino (el ID de cuenta del inquilino se asigna automáticamente y no se puede cambiar)
- Opcionalmente, una cuota de almacenamiento para la cuenta de inquilino: El número máximo de gigabytes, terabytes o petabytes disponibles para los objetos del inquilino. La cuota de almacenamiento de un inquilino representa una cantidad lógica (tamaño de objeto), no una cantidad física (tamaño en disco).
- Si el sistema StorageGRID no utiliza el inicio de sesión único (SSO), tanto si la cuenta de inquilino usará su propio origen de identidad como si comparte el origen de identidad de la cuadrícula, así como la contraseña inicial del usuario raíz local del inquilino.
- Si SSO está habilitado, qué grupo federado tiene permiso de acceso raíz para configurar la cuenta de inquilino.

Después de crear una cuenta de inquilino de Swift, los usuarios con permiso de acceso raíz pueden acceder al Administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidades (a menos que el origen de identidades se comparta con la cuadrícula) y crear grupos y usuarios locales
- Supervisión del uso de almacenamiento

> Los usuarios de Swift deben tener el permiso acceso raíz para acceder al Administrador de inquilinos. Sin embargo, el permiso Root Access 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.

Información relacionada

Administre StorageGRID

Usar cuenta de inquilino

Extremos de API de Swift compatibles

Cómo se pueden configurar las conexiones de clientes

Un administrador de grid toma opciones de configuración que afectan a la forma en que los clientes de Swift se conectan a StorageGRID para almacenar y recuperar los datos. La información específica que necesita para realizar una conexión depende de la configuración elegida.

Las aplicaciones cliente pueden almacenar o recuperar objetos conectándose a cualquiera de los siguientes elementos:

- El servicio Load Balancer en los nodos de administrador o de puerta de enlace, o bien, de forma opcional, la dirección IP virtual de un grupo de alta disponibilidad (ha) de nodos de administración o nodos de puerta de enlace

- El servicio CLB en los nodos de puerta de enlace o, opcionalmente, la dirección IP virtual de un grupo de nodos de puerta de enlace de alta disponibilidad

> El servicio CLB está obsoleto. Los clientes configurados antes de la versión StorageGRID 11.3 pueden seguir utilizando el servicio CLB en los nodos de puerta de enlace. El resto de aplicaciones cliente que dependen de StorageGRID para proporcionar equilibrio de carga se deben conectar mediante el servicio Load Balancer.

- Nodos de almacenamiento, con o sin un equilibrador de carga externo

Al configurar StorageGRID, un administrador de grid puede utilizar Grid Manager o la API de gestión de grid para realizar los siguientes pasos, todos ellos opcionales:

1. Configure los extremos para el servicio Load Balancer.

   Debe configurar los extremos para usar el servicio Load Balancer. El servicio Load Balancer en los nodos de administrador o de puerta de enlace distribuye conexiones de red entrantes desde aplicaciones cliente hasta los nodos de almacenamiento. Al crear un extremo de equilibrio de carga, el administrador de StorageGRID especifica un número de puerto, tanto si el extremo acepta conexiones HTTP o HTTPS, como el tipo de cliente (S3 o Swift) que utilizará el extremo y el certificado que se utilizará para las conexiones HTTPS (si procede).

2. Configure redes de cliente no fiables.

   Si un administrador de StorageGRID configura la red cliente de un nodo para que no sea de confianza, el nodo sólo acepta conexiones entrantes en la red cliente en puertos que se configuran explícitamente como extremos equilibradores de carga.

3. Configuración de grupos de alta disponibilidad.

   Si un administrador crea un grupo de alta disponibilidad, las interfaces de red de varios nodos de administrador o nodos de puerta de enlace se colocan en una configuración de backup activo. Las conexiones de clientes se realizan mediante la dirección IP virtual del grupo de alta disponibilidad.

Para obtener más información acerca de cada opción, consulte las instrucciones para administrar StorageGRID.

Resumen: Direcciones IP y puertos para conexiones cliente

Las aplicaciones cliente se conectan a StorageGRID mediante la dirección IP de un nodo de grid y el número de puerto de un servicio en ese nodo. Si se configuran los grupos de alta disponibilidad, las aplicaciones cliente se pueden conectar mediante la dirección IP virtual del grupo de alta disponibilidad.

Información necesaria para realizar conexiones de cliente

La tabla resume las distintas maneras en que los clientes pueden conectarse a StorageGRID y las direcciones IP y los puertos que se utilizan para cada tipo de conexión. Póngase en contacto con el administrador de StorageGRID para obtener más información o consulte las instrucciones para administrar StorageGRID para obtener una descripción de cómo encontrar esta información en el administrador de grid.

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 de punto final del equilibrador de carga
Grupo de ALTA DISPONIBILIDAD	CLB **Nota:** el servicio CLB está en desuso.	La dirección IP virtual de un grupo de alta disponibilidad	Puertos Swift predeterminados: • HTTPS: 8083 • HTTP: 8085
Nodo de administración	Equilibrador de carga	La dirección IP del nodo de administrador	• Puerto de punto final del equilibrador de carga
Nodo de puerta de enlace	Equilibrador de carga	La dirección IP del nodo de puerta de enlace	• Puerto de punto final del equilibrador de carga
Nodo de puerta de enlace	CLB **Nota:** el servicio CLB está en desuso.	La dirección IP del nodo de puerta de enlace **Nota:** de forma predeterminada, los puertos HTTP para CLB y LDR no están habilitados.	Puertos Swift predeterminados: • HTTPS: 8083 • HTTP: 8085
Nodo de almacenamiento	LDR	La dirección IP del nodo de almacenamiento	Puertos Swift predeterminados: • HTTPS: 18083 • HTTP: 18085

Ejemplo

Para conectar un cliente Swift al extremo Load Balancer de un grupo de 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 de alta disponibilidad es 192.0.2.6 y el número de puerto de un extremo de equilibrio de carga de Swift es 10444, un cliente de Swift puede usar la siguiente URL para conectarse a StorageGRID:

- `https://192.0.2.6:10444`

Es posible configurar un nombre DNS para la dirección IP que utilizan los clientes para conectarse a StorageGRID. Póngase en contacto con el administrador de red local.

Decidir usar conexiones HTTPS o HTTP

Cuando se realizan conexiones de cliente mediante un extremo de equilibrio de carga, es necesario realizar conexiones mediante el protocolo (HTTP o HTTPS) especificado para ese extremo. Para utilizar HTTP para las conexiones de clientes a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace, debe habilitar su uso.

De forma predeterminada, cuando las aplicaciones cliente se conectan a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace, deben utilizar HTTPS cifrado para todas las conexiones. Opcionalmente, puede habilitar conexiones HTTP menos seguras seleccionando la opción de cuadrícula **Activar conexión HTTP** en el Administrador de grid. Por ejemplo, una aplicación cliente puede utilizar HTTP al probar la conexión a un nodo de almacenamiento en un entorno no de producción.

> Tenga cuidado al habilitar HTTP para una cuadrícula de producción, ya que las solicitudes se enviarán sin cifrar.

> El servicio CLB está obsoleto.

Si se selecciona la opción **Activar conexión HTTP**, los clientes deben utilizar puertos diferentes para HTTP que los que utilizan para HTTPS. Consulte las instrucciones para administrar StorageGRID.

Información relacionada

Administre StorageGRID

Pruebe la conexión en la configuración de la API de Swift

Puede usar la interfaz de línea de comandos de Swift para probar la conexión con el sistema StorageGRID y verificar que puede leer y escribir objetos en el sistema.

Lo que necesitará

- Debe haber descargado e instalado python-swiftclient, el cliente de línea de comandos de Swift.

  "SwiftStack: python-swiftclient"

- Debe tener una cuenta de inquilino de Swift en el sistema StorageGRID.

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
```

Información relacionada

Cree y configure cuentas de inquilino de Swift

Configure la seguridad de la API de REST

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. No se puede configurar el usuario raíz del inquilino para usar la API DE 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 satisfactoria devuelve los siguientes encabezados con una respuesta «'HTTP/1.1 204 sin contenido» si se encuentra la cuenta y no tiene contenedores o la lista de contenedores está vacía; o una respuesta «'HTTP/1.1 200 OK'» 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 satisfactoria devuelve los encabezados siguientes 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

Supervisar y auditar operaciones

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.

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 un plazo de 30

segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y luego indica que el cliente se ha realizado correctamente.

Para obtener más información sobre cómo eliminar objetos, consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

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 chunked `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 comprimido ni descomprimido `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 las reglas de la ubicación síncrona y ILM, consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

- `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 denominado `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).
- **Balanceado**: Si la regla ILM especifica la opción equilibrada, StorageGRID realiza una única copia provisional sólo 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 al número de copias del objeto que se realizan cuando el objeto se evalúa mediante la política de ILM activa y no provoca que los datos se almacenen en niveles más bajos de redundancia en el 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`

Información relacionada

Gestión de objetos con ILM

Supervisar y auditar operaciones

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 OPTIONS no se puede utilizar con la dirección URL de autenticación.

Se requiere el siguiente parámetro request:

- `Account`

Los siguientes parámetros de solicitud son opcionales:

- `Container`
- `Object`

Una ejecución satisfactoria devuelve los encabezados siguientes con una respuesta «'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

Nombre de error de Swift	Estado de HTTP
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

El nivel de consistencia proporciona un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en distintos nodos de almacenamiento y sitios. La solicitud DE consistencia DEL contenedor le permite determinar el nivel de consistencia que se aplica a un contenedor en particular.

Solicitud

Solicitar encabezado HTTP	Descripción
`X-Auth-Token`	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
`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.

Encabezado HTTP de respuesta	Descripción
`x-ntap-sg-consistency`	El nivel de control de consistencia que se aplica al contenedor. Se admiten los siguientes valores: • **Todos**: Todos los nodos reciben los datos inmediatamente o la solicitud falla. • **Strong-global**: Garantiza la coherencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios. • **Strong-site**: Garantiza la coherencia de lectura después de escritura para todas las solicitudes de cliente dentro de un sitio. • **Read-after-new-write**: Proporciona consistencia de lectura-after-write para nuevos objetos y eventual consistencia para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. **Nota**: Si su aplicación utiliza PETICIONES HEAD en objetos que no existen, puede recibir un número elevado de 500 errores internos del servidor si uno o más nodos de almacenamiento no están disponibles. Para evitar estos errores, utilice el nivel "'disponible'". • **Disponible** (eventual consistencia para las operaciones DE LA CABEZA): Se comporta igual que el nivel de consistencia "entre-después-nueva-escritura", pero sólo proporciona consistencia eventual para las operaciones DE LA CABEZA. Ofrece una mayor disponibilidad para las OPERACIONES DE CABEZAL que una «escritura tras otra» si los nodos de almacenamiento no están disponibles.

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
```

Información relacionada

Usar cuenta de inquilino

PONGA la solicitud de consistencia del contenedor

La solicitud DE PUT Container permite especificar el nivel de coherencia que se aplicará a las operaciones realizadas en un contenedor. De forma predeterminada, se crean nuevos contenedores utilizando el nivel de coherencia «entre una y otra escritura».

Solicitud

Solicitar encabezado HTTP	Descripción
`X-Auth-Token`	El token de autenticación Swift de la cuenta que se va a utilizar para la solicitud.
`x-ntap-sg-consistency`	El nivel de control de coherencia que se va a aplicar a las operaciones en el contenedor. Se admiten los siguientes valores: • **Todos**: Todos los nodos reciben los datos inmediatamente o la solicitud falla. • **Strong-global**: Garantiza la coherencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios. • **Strong-site**: Garantiza la coherencia de lectura después de escritura para todas las solicitudes de cliente dentro de un sitio. • **Read-after-new-write**: Proporciona consistencia de lectura-after-write para nuevos objetos y eventual consistencia para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. **Nota**: Si su aplicación utiliza PETICIONES HEAD en objetos que no existen, puede recibir un número elevado de 500 errores internos del servidor si uno o más nodos de almacenamiento no están disponibles. Para evitar estos errores, utilice el nivel "'disponible'". • **Disponible** (eventual consistencia para las operaciones DE LA CABEZA): Se comporta igual que el nivel de consistencia "entre-después-nueva-escritura", pero sólo proporciona consistencia eventual para las operaciones DE LA CABEZA. Ofrece una mayor disponibilidad para las OPERACIONES DE CABEZAL que una «escritura tras otra» si los nodos de almacenamiento no están disponibles.
`Host`	El nombre de host al que se dirige la solicitud.

Cómo interactúan los controles de consistencia y las reglas de ILM para afectar a la protección de datos

Tanto la elección del control de coherencia como la regla de ILM afectan a la forma en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, el control de consistencia usado cuando se almacena un objeto afecta a la colocación inicial de los metadatos de objetos, mientras que el comportamiento de procesamiento seleccionado para la regla de ILM afecta a la colocación inicial de las copias de objetos. Dado que StorageGRID requiere acceso tanto a los metadatos de un objeto como a sus datos para cumplir con las solicitudes de los clientes, seleccionar los niveles de protección correspondientes para el nivel de coherencia y el comportamiento de ingesta puede proporcionar una mejor protección de datos inicial y respuestas más predecibles del sistema.

Para las reglas de ILM hay disponibles los siguientes comportamientos de consumo:

- **Estricto**: Todas las copias especificadas en la regla ILM deben hacerse antes de que el éxito se devuelva al cliente.
- **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.
- **Commit doble**: StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

> Antes de seleccionar el comportamiento de procesamiento de una regla de ILM, lea la descripción completa de estos ajustes en las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

Ejemplo de cómo pueden interactuar el control de consistencia y la regla de ILM

Suponga que tiene una cuadrícula de dos sitios con la siguiente regla de ILM y la siguiente configuración de nivel de coherencia:

- **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.
- **Nivel de coherencia**: "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 su lugar usa la misma regla de ILM y el nivel de consistencia de «otrong-site», es posible que el cliente reciba un mensaje de éxito después de replicar los datos del objeto en el sitio remoto, pero antes de que los metadatos del objeto 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 los niveles de coherencia y las reglas del 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
```

Información relacionada

Usar cuenta de inquilino

Configure la seguridad de la API de REST

Debe revisar las medidas de seguridad implementadas para la API REST y entender cómo proteger el sistema.

Cómo proporciona StorageGRID seguridad para la API de REST

Debe entender cómo el sistema StorageGRID implementa la seguridad, la autenticación y la autorización para la API DE REST.

StorageGRID usa las siguientes medidas de seguridad.

- Las comunicaciones de cliente con el servicio Load Balancer utilizan HTTPS si HTTPS está configurado para el extremo de equilibrio de carga.

  Al configurar un extremo de equilibrio de carga, HTTP se puede habilitar opcionalmente. Por ejemplo,

puede usar HTTP para pruebas u otros fines que no sean de producción. Consulte las instrucciones para administrar StorageGRID si desea obtener más información.

- De forma predeterminada, StorageGRID utiliza HTTPS para las comunicaciones del cliente con los nodos de almacenamiento y el servicio CLB en los nodos de puerta de enlace.

  Opcionalmente, HTTP se puede habilitar para estas conexiones. Por ejemplo, puede usar HTTP para pruebas u otros fines que no sean de producción. Consulte las instrucciones para administrar StorageGRID si desea obtener más información.

  El servicio CLB está obsoleto.

- 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.

Certificados de seguridad y aplicaciones cliente

Los clientes pueden conectarse al servicio Load Balancer en los nodos de Gateway o de administrador, directamente a los nodos de almacenamiento o al servicio CLB obsoleto en los nodos de Gateway.

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, lo hacen utilizando el certificado que se configuró para el extremo de equilibrio de carga específico utilizado para realizar la conexión. Cada extremo tiene su propio certificado, que es 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 extremo.
- Cuando las aplicaciones cliente se conectan directamente a un nodo de almacenamiento o al servicio CLB en los nodos de puerta de enlace, utilizan los certificados de servidor generados por el sistema que se generaron para los nodos de almacenamiento cuando se instaló el sistema StorageGRID (firmados por la autoridad de certificación del sistema), o un único certificado de servidor personalizado que un administrador de grid suministra para la cuadrícula.

Los clientes deben configurarse para que confíen en la entidad emisora de certificados que firmó el certificado que utilicen para establecer conexiones TLS.

Consulte las instrucciones para administrar StorageGRID para obtener información sobre la configuración de extremos de equilibrador de carga y para obtener instrucciones sobre cómo agregar un único certificado de servidor personalizado para conexiones TLS directamente a nodos de almacenamiento o al servicio CLB en nodos de puerta de enlace.

Resumen

En la siguiente tabla, se muestra cómo se implementan los problemas de seguridad en 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 de S3 (ID de clave de acceso y clave de acceso secreta) • Swift: Cuenta de Swift (nombre de usuario y contraseña)
Autorización de cliente	• S3: Propiedad de bloque y todas las políticas de control de acceso aplicables • Swift: Acceso a roles de administrador

Información relacionada

Administre StorageGRID

Algoritmos de cifrado y hash compatibles para bibliotecas TLS

El sistema StorageGRID admite un conjunto limitado de conjuntos de cifrado que las aplicaciones cliente pueden utilizar al establecer una sesión de seguridad de la capa de transporte (TLS).

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.

Paquetes de cifrado compatibles

Versión TLS	Nombre IANA de conjunto cifrado
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHA20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
TLS_CHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

Suites de cifrado obsoletas

Los siguientes conjuntos de cifrado están desaprobados. La compatibilidad con estos cifrados se eliminará en una versión futura.

Nombre de IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Información relacionada

Configure las conexiones y las cuentas de inquilino

Supervisar y auditar operaciones

Puede supervisar las cargas de trabajo y las eficiencias de las operaciones del cliente al ver las tendencias de las transacciones de todo el grid o de nodos específicos. Puede utilizar mensajes de auditoría para supervisar las operaciones y transacciones del cliente.

Supervise las tasas de procesamiento y recuperación de objetos

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.

Pasos

1. Inicie sesión en Grid Manager mediante una navegador web compatible.
2. En la consola, busque la sección Operaciones de protocolo.

   En esta sección se resume el número de operaciones de cliente que realiza su sistema StorageGRID. La media de las tasas de protocolo se hace durante los últimos dos minutos.

3. Seleccione **NODES**.
4. En la página de inicio de nodos (nivel de implementación), haga clic en la ficha **Load Balancer**.

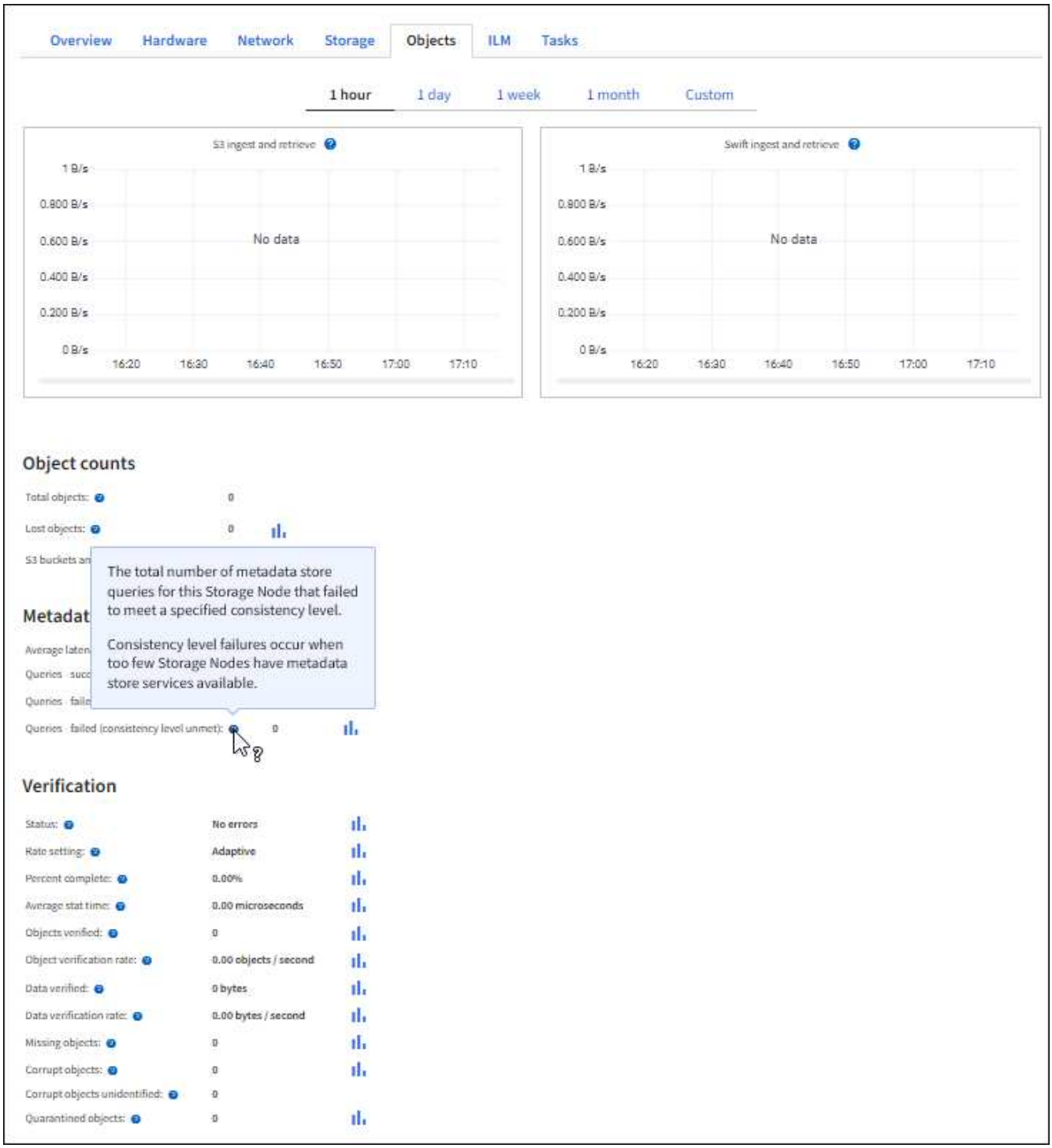
   Los gráficos muestran tendencias para todo el tráfico de cliente dirigido a los extremos de equilibrador de carga dentro de la cuadrícula. Es posible seleccionar un intervalo de tiempo en horas, días, semanas, meses o años. también puede aplicar un intervalo personalizado.

5. En la página de inicio de nodos (nivel de implementación), haga clic en la ficha **objetos**.

   El gráfico muestra las tasas de procesamiento y recuperación de todo el sistema StorageGRID en bytes por segundo y bytes totales. Es posible seleccionar un intervalo de tiempo en horas, días, semanas, meses o años. también puede aplicar un intervalo personalizado.

6. Para ver información sobre un nodo de almacenamiento en particular, seleccione el nodo en la lista de la izquierda y haga clic en la ficha **objetos**.

   El gráfico muestra las tasas de procesamiento y recuperación de objetos de este nodo de almacenamiento. La pestaña también incluye métricas para el recuento de objetos, consultas y verificación. Puede hacer clic en las etiquetas para ver las definiciones de estas métricas.



7. Si desea aún más detalles:
   a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
   b. Seleccione ***site*** > **Descripción general** > **Principal**.

      La sección API Operations muestra información resumida de la cuadrícula completa.

   c. Seleccione ***Storage Node*** > **LDR** > ***Client Application*** > **Overview** > **Main**

      La sección Operaciones muestra información de resumen del nodo de almacenamiento seleccionado.

Acceder y revisar registros de auditoría

Los servicios de StorageGRID generan los mensajes de auditoría y se almacenan en archivos de registro de texto. Los mensajes de auditoría específicos de API de los registros de auditoría ofrecen datos críticos de seguridad, operación y supervisión del rendimiento que pueden ayudar a evaluar el estado del sistema.

Lo que necesitará

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la dirección IP de un nodo de administrador.

Acerca de esta tarea

Se denomina el archivo de registro de auditoría activo `audit.log`, Y se almacena en los nodos Admin.

Una vez al día, se guarda el archivo audit.log activo y se inicia un nuevo archivo audit.log. 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.

En este ejemplo, se muestra el archivo audit.log activo, 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
```

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.
2. Vaya al directorio que contiene los archivos del registro de auditoría:`cd /var/local/audit/export`
3. Ver el archivo de registro de auditoría actual o guardado, según sea necesario.

Información relacionada

Revisar los registros de auditoría

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 no se registran ni se registran solicitudes de información, autenticación u OPCIONES.

Consulte *Descripción de los mensajes de auditoría* para obtener detalles sobre la información de la que se realiza el seguimiento para las siguientes operaciones de Swift.

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

Revisar los registros de auditoría

Operaciones de cuentas

Operaciones de contenedor

Operaciones de objeto

Supervisar y mantener StorageGRID

Supervisión y solución de problemas

Supervisión y solución de problemas: Descripción general

Use estas instrucciones para supervisar un sistema StorageGRID y para evaluar y resolver los problemas que puedan producirse.

Acerca de estas instrucciones

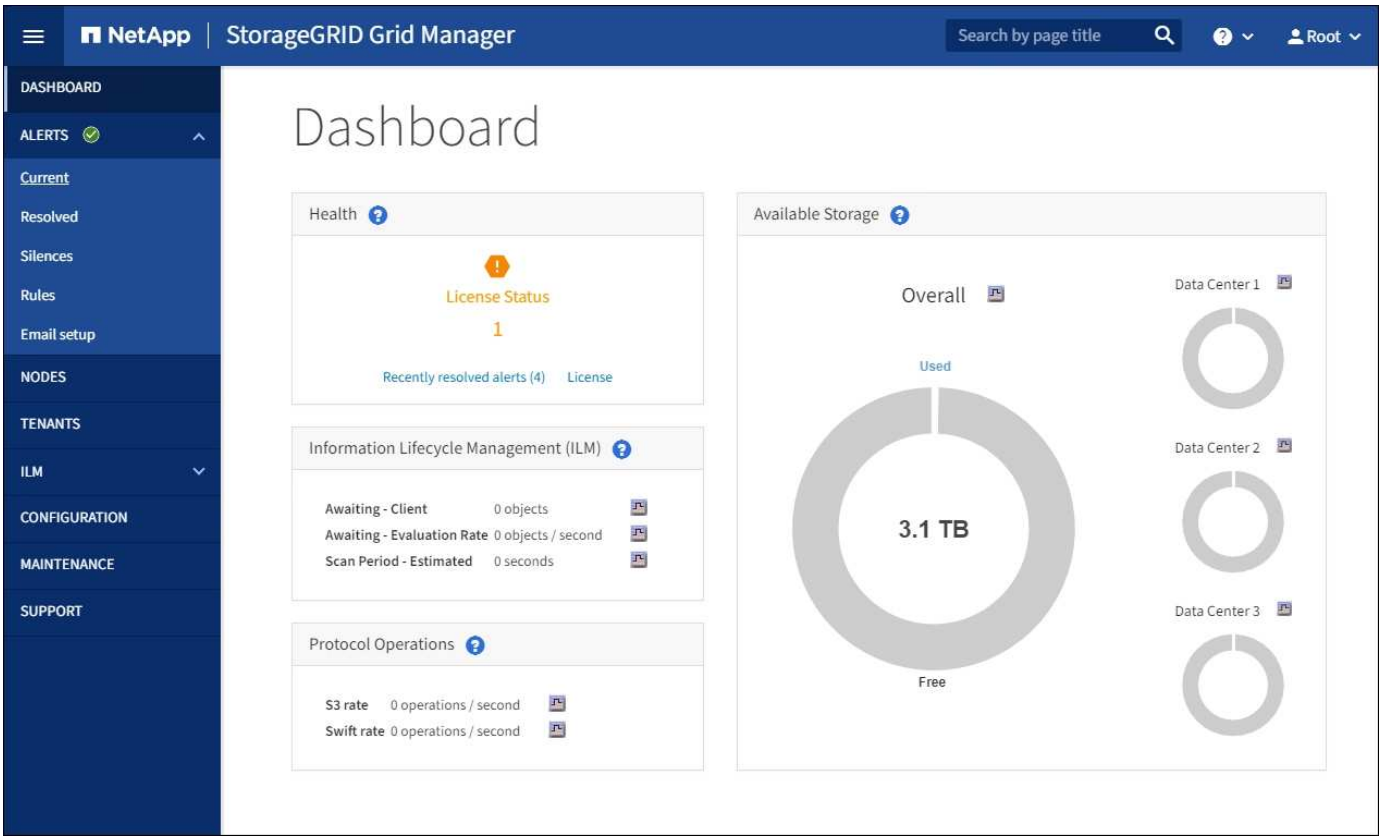
Estas instrucciones describen cómo utilizar Grid Manager para supervisar un sistema StorageGRID. Aprenderá qué información debe supervisar con regularidad, cómo gestionar alertas y alarmas heredadas, cómo utilizar SNMP para realizar la supervisión y cómo obtener datos de StorageGRID adicionales, incluidos métricas y diagnósticos.

Estas instrucciones también describen cómo solucionar problemas de un sistema StorageGRID y describen todas las alertas del sistema, las alarmas heredadas y los archivos de registro.

Siga estas instrucciones si va a supervisar y dar soporte a un sistema StorageGRID después de que se haya instalado.

Consulte la consola

Cuando inicie sesión por primera vez en Grid Manager, puede utilizar el panel para supervisar las actividades del sistema de un vistazo. La consola incluye información sobre el estado del sistema, las métricas de uso y los gráficos y tendencias operativas.



Campo de búsqueda

El campo **Buscar** de la barra de encabezado le permite navegar rápidamente a una página específica o entrada de barra lateral dentro de Grid Manager. Por ejemplo, puede introducir **key** para acceder a la página del servidor de gestión de claves.

Panel de estado

Descripción	Ver detalles adicionales	Leer más
Resume el estado del sistema. Una Marca de verificación verde significa que no hay alertas actuales y que todos los nodos de grid están conectados. Cualquier otro icono significa que hay al menos un nodo de alerta actual o desconectado.	Puede que vea uno o varios de los siguientes enlaces: • **Detalles de la cuadrícula**: Aparece si alguno de los nodos está desconectado (estado de conexión desconocido o administrativamente abajo). Haga clic en el enlace o haga clic en el icono azul o gris para determinar qué nodo o nodos están afectados. • **Alertas actuales**: Aparece si hay alguna alerta activa. Haga clic en el enlace o haga clic en **crítico**, **mayor** o **menor** para ver los detalles en la página **ALERTAS** > **actual**. • **Alertas resueltas recientemente**: Aparece si se han resuelto las alertas activadas en la última semana. Haga clic en el enlace para ver los detalles en la página **ALERTS** > **Resolved**. • **Alarmas heredadas**: Aparece si alguna alarma (sistema heredado) está activa actualmente. Haga clic en el enlace para ver los detalles en la página **SUPPORT** > **Alarms (Legacy)** > **Current Alarms**. • **Licencia**: Aparece si hay un problema con la licencia de software para este sistema StorageGRID. Haga clic en el enlace para ver los detalles en la página **MANTENIMIENTO** > **sistema** > **Licencia**.	• Supervise los estados de conexión de los nodos • Ver las alertas actuales • Ver alertas resueltas • Ver alarmas heredadas • Administre StorageGRID

Panel almacenamiento disponible

Descripción	Ver detalles adicionales	Leer más
Muestra la capacidad de almacenamiento disponible y utilizada en toda la cuadrícula, sin incluir los medios de archivado. El gráfico general presenta los totales de toda la cuadrícula. Si se trata de una cuadrícula de varios sitios, aparecerán gráficos adicionales para cada sitio del centro de datos. Esta información se puede usar para comparar el almacenamiento usado con el almacenamiento disponible. Si tiene una cuadrícula de varios sitios, puede determinar qué sitio consume más almacenamiento.	• Para ver la capacidad, coloque el cursor sobre las secciones de capacidad disponible y utilizada del gráfico. • Para ver las tendencias de capacidad sobre un rango de fechas, haga clic en el icono del gráfico para la grid general o para el sitio de un centro de datos. • Para ver los detalles, seleccione **NODES**. A continuación, vea la pestaña almacenamiento de toda la cuadrícula, un sitio entero o un único nodo de almacenamiento.	• Consulte la pestaña almacenamiento • Supervise la capacidad de almacenamiento

Panel Information Lifecycle Management (ILM)

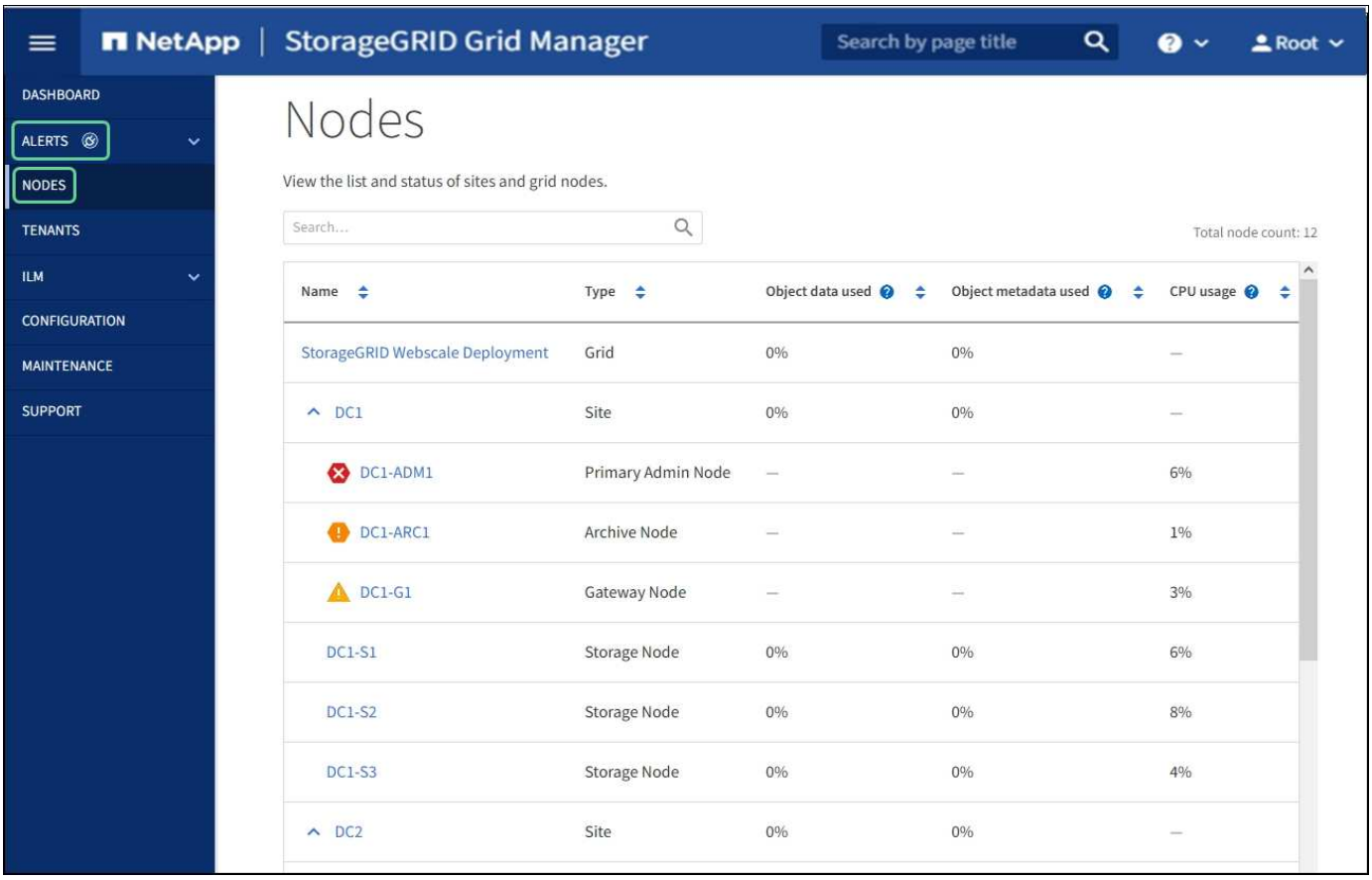
Descripción	Ver detalles adicionales	Leer más
Muestra las operaciones de ILM y las colas de ILM actuales del sistema. Puede utilizar esta información para supervisar la carga de trabajo del sistema. • **Esperando - Cliente**: El número total de objetos que esperan la evaluación de ILM de las operaciones cliente (por ejemplo, ingesta). • **Esperando - tasa de evaluación**: La velocidad actual a la que se evalúan los objetos en comparación con la política de ILM de la red. • **Período de exploración - estimado**: El tiempo estimado para completar una exploración completa de ILM de todos los objetos. **Nota:** una exploración completa no garantiza que ILM se haya aplicado a todos los objetos.	• Para ver los detalles, seleccione **NODES**. A continuación, vea la pestaña ILM de toda la cuadrícula, un sitio entero o un nodo de almacenamiento único. • Para ver las reglas de ILM existentes, seleccione **ILM** > **Reglas**. • Para ver las directivas de ILM existentes, seleccione **ILM** > **Directivas**.	• Vea la pestaña ILM • Administre StorageGRID.

Panel de operaciones de protocolo

Descripción	Ver detalles adicionales	Leer más
Muestra la cantidad de operaciones específicas de protocolos (S3 y Swift) que realiza el sistema. Puede utilizar esta información para supervisar las cargas de trabajo y las eficiencias del sistema. La media de las tasas de protocolo se hace durante los últimos dos minutos.	• Para ver los detalles, seleccione **NODES**. A continuación, visualice la ficha objetos de toda la cuadrícula, de todo un sitio o de un único nodo de almacenamiento. • Para ver las tendencias en un intervalo de fechas, haga clic en el icono del gráfico A la derecha de la tasa del protocolo S3 o Swift.	• Abra la pestaña objetos • Use S3 • Use Swift

Vea la página Nodes

Si necesita información más detallada sobre el sistema StorageGRID de la que proporciona la consola, puede usar la página nodos para ver métricas de toda la cuadrícula, cada sitio de la cuadrícula y cada nodo de un sitio.



En la tabla Nodes, se muestran todos los sitios y los nodos del sistema StorageGRID. La información de resumen se muestra para cada nodo. Si un nodo 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.

Iconos de estado de conexión

- **No conectado - Desconocido** : El nodo no está conectado a la cuadrícula por una razón desconocida. Por ejemplo, se ha perdido la conexión de red entre los nodos o se ha apagado el suministro eléctrico. 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.

- **No conectado - 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.

Si un nodo está desconectado de la cuadrícula, puede tener una alerta subyacente, pero sólo aparece el icono "'no conectado'". Para ver las alertas activas de un nodo, seleccione el nodo.

Iconos de alerta

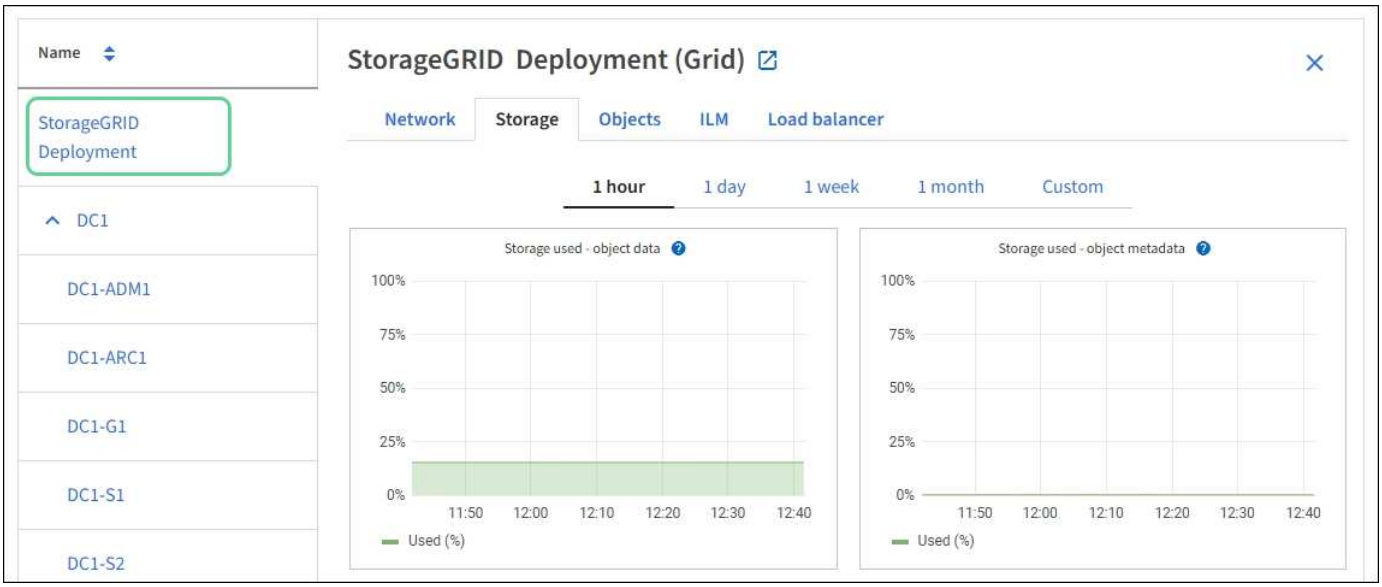
Si hay una alerta activa de un nodo, aparece uno de los siguientes iconos junto al nombre del nodo:

- **Crítico** : Existe una condición anormal que ha detenido las operaciones normales de un nodo 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. Deberá supervisar y resolver las alertas menores que no se despicen por sí mismas para asegurarse de que no provoquen un problema más grave.

Ver detalles de un sistema, sitio o nodo

Para ver la información disponible, seleccione el nombre de la cuadrícula, sitio o nodo de la siguiente manera:

- 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.



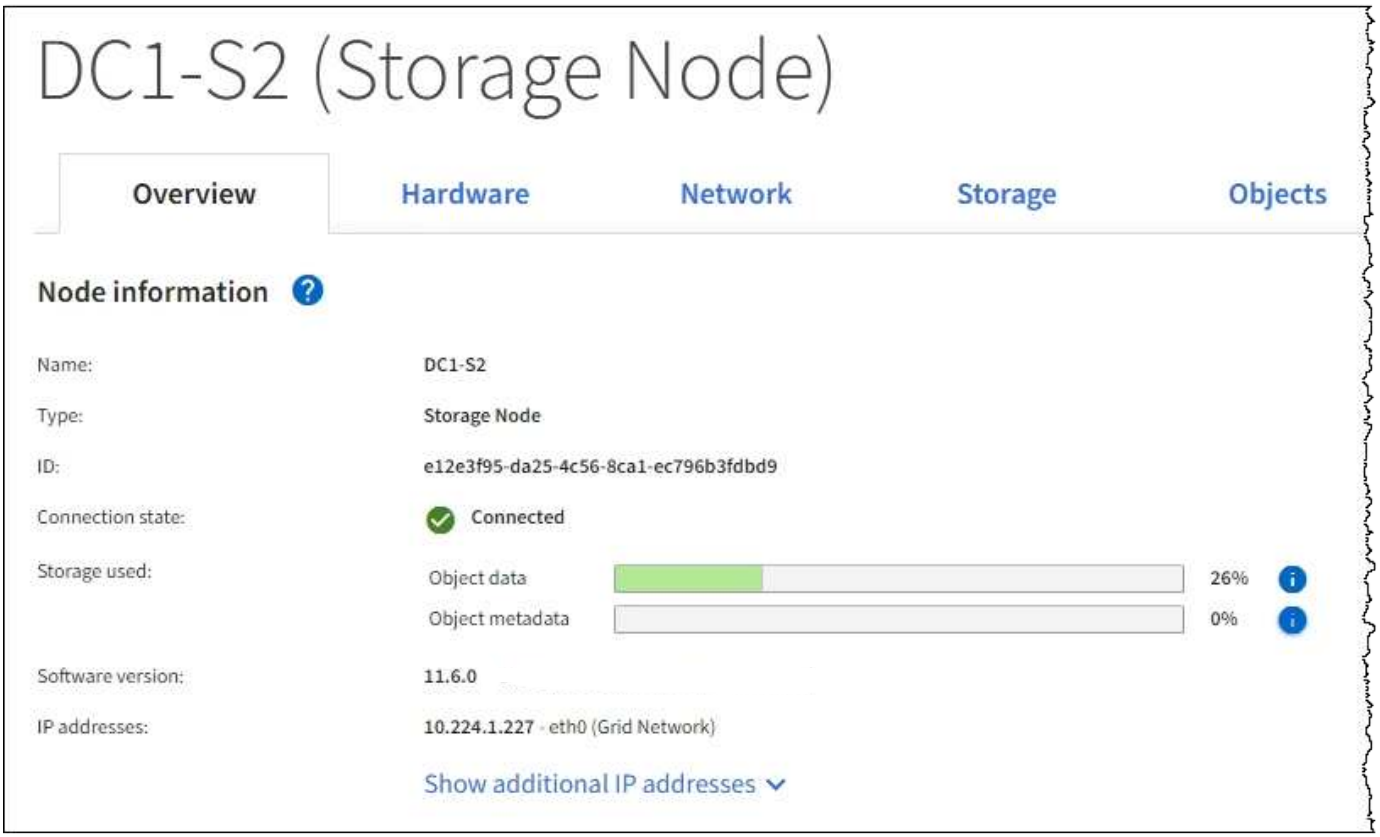
Vea la ficha Descripción general

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

En la sección Información del nodo de la ficha Descripción general se muestra información básica sobre el nodo de cuadrícula.



La información general de un nodo incluye lo siguiente:

- **Nombre**: Nombre de host asignado al nodo y mostrado en el Administrador de cuadrícula.
- **Tipo**: Tipo de nodo — nodo de administración, nodo de administración principal, nodo de almacenamiento, nodo de puerta de enlace o nodo de archivado.
- **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** : El nodo no está conectado a la cuadrícula por una razón desconocida. Por ejemplo, se ha perdido la conexión de red entre los nodos o se ha apagado el suministro eléctrico. 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 de la ficha Descripción general enumera todas las alertas que afectan actualmente a este nodo que no se han silenciado. Haga clic en el nombre de la alerta para ver más detalles y las acciones recomendadas.

Información relacionada

Supervise los estados de conexión de los nodos

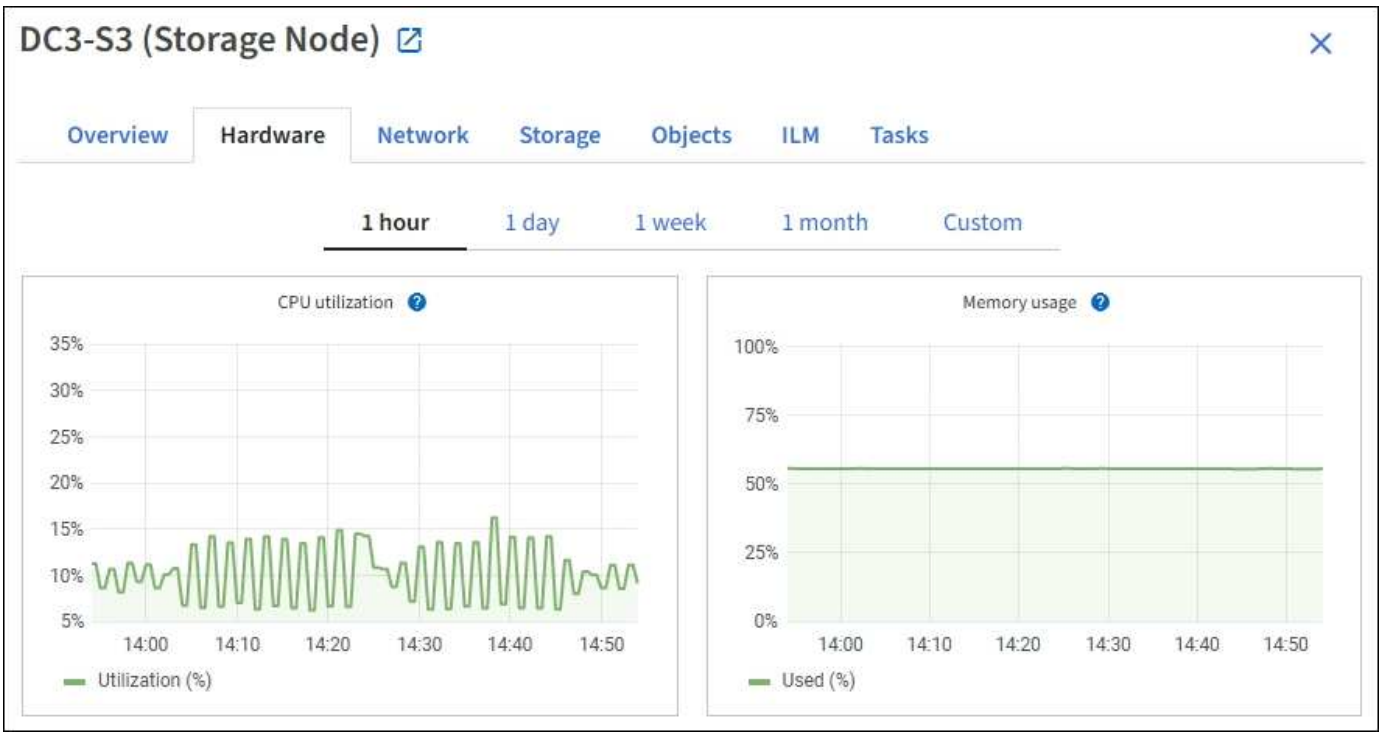
Ver las alertas actuales

Ver una alerta específica

Vea la pestaña hardware

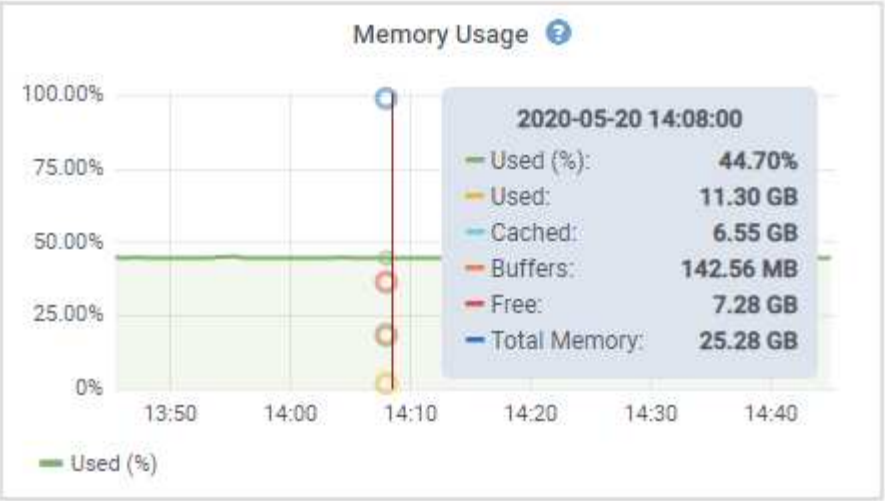
En la pestaña hardware, se muestra la utilización de CPU y la memoria de cada nodo, así como información de hardware adicional sobre los dispositivos.

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 la memoria, pase 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

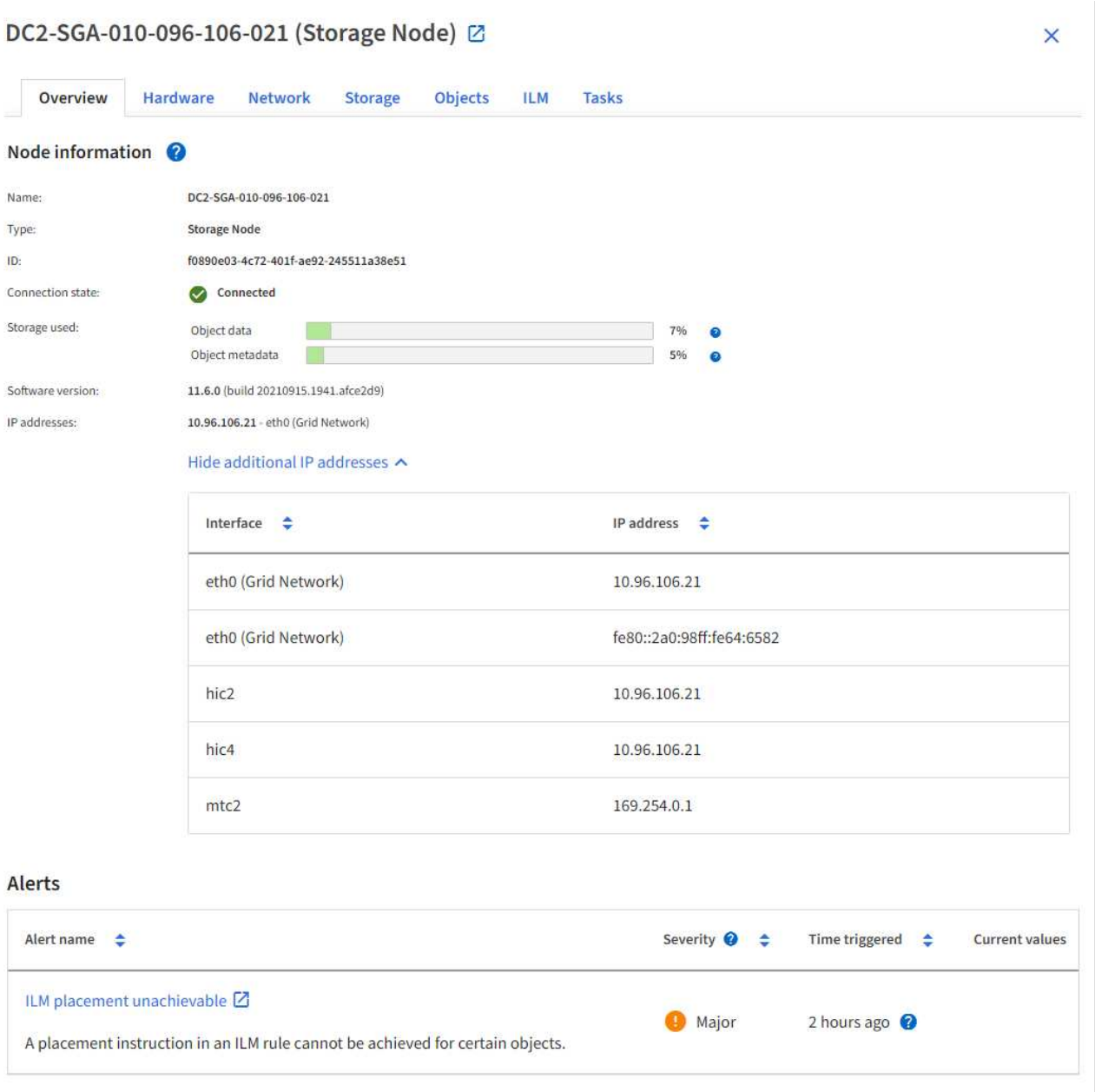
En la página Nodes, se incluye información sobre el estado del servicio y todos los recursos computacionales, de dispositivo de disco y de red para cada nodo de almacenamiento del dispositivo. También puede ver memoria, hardware de almacenamiento, versión del firmware de la controladora, recursos de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

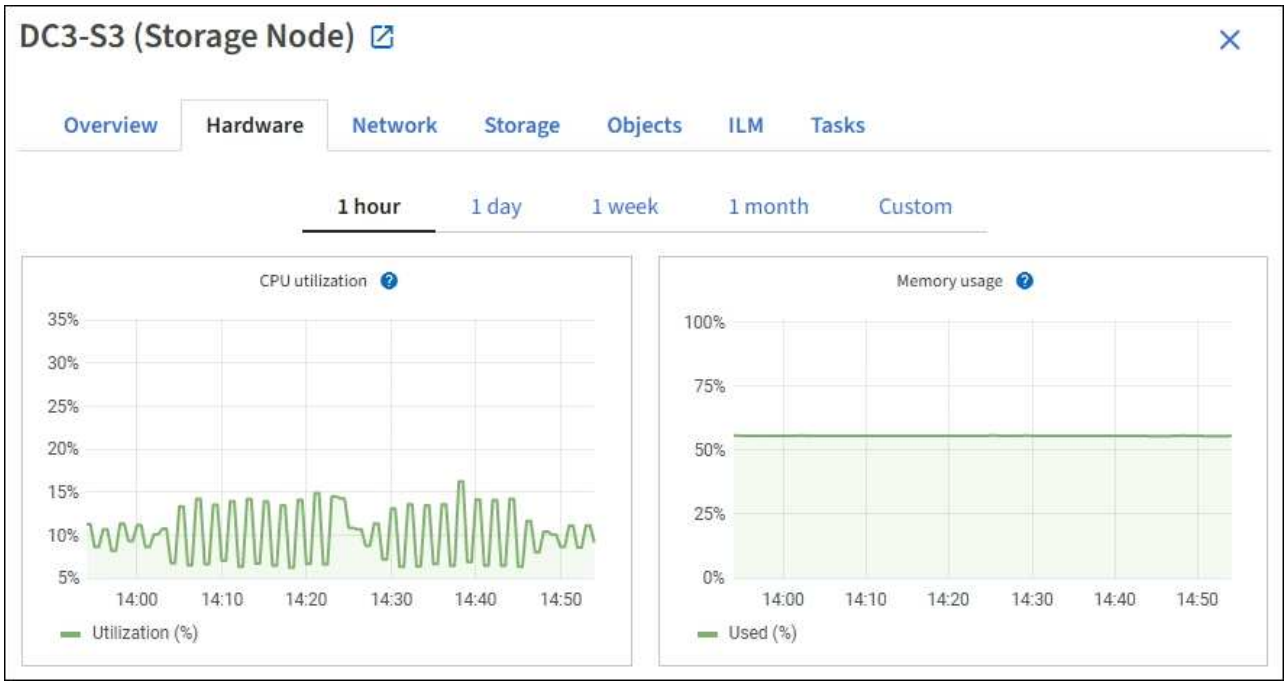
   - **Eth**: Red Grid, red de administración o red de cliente.
   - **Clic**: Uno de los puertos 10, 25 o 100 GbE físicos del aparato. Estos puertos se pueden unir y conectar a la red de cuadrícula de StorageGRID (eth0) y a la red de cliente (eth2).
   - * mtc*: Uno de los puertos físicos de 1 GbE del 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.

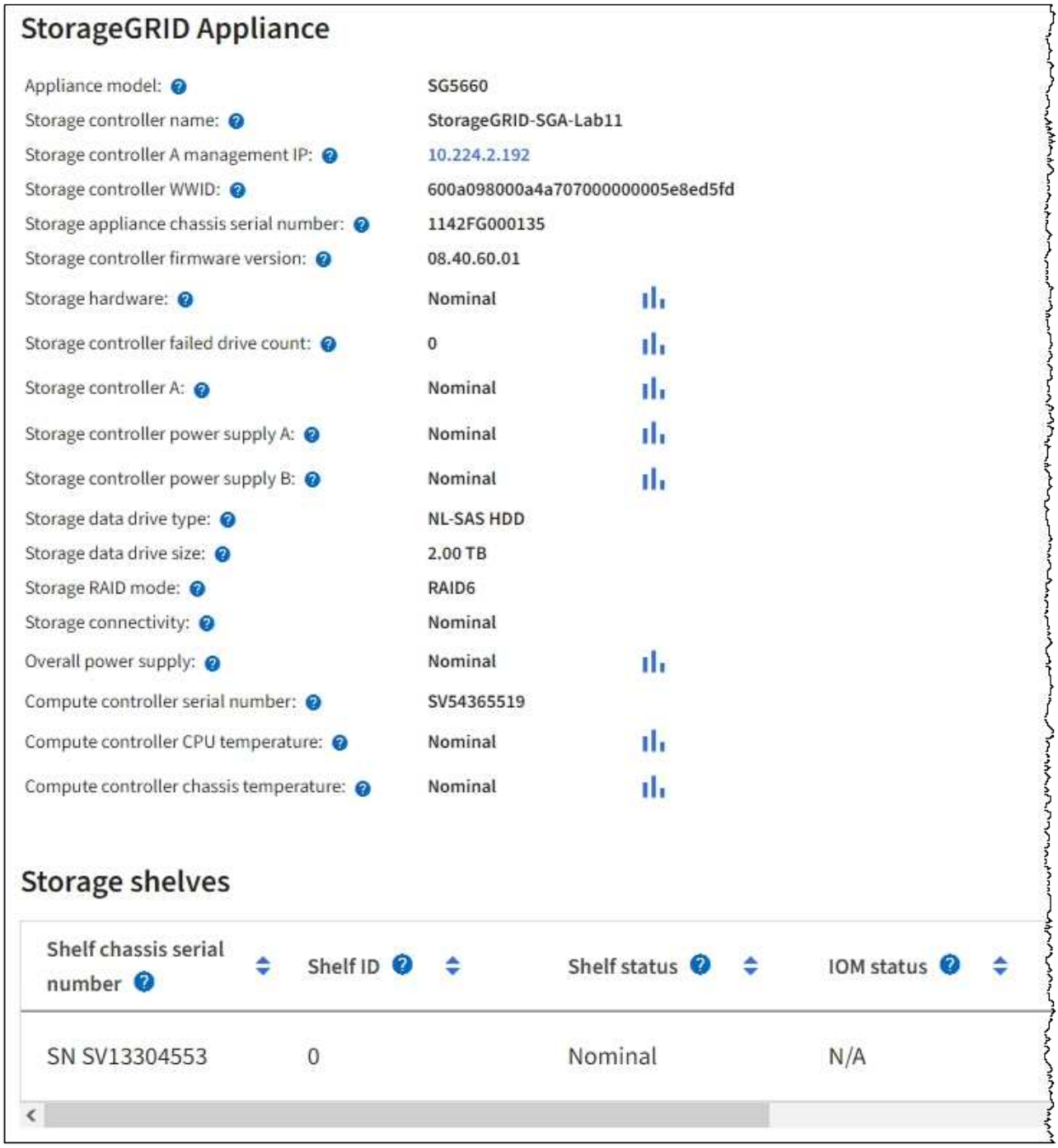
   a. Consulte los gráficos de utilización de CPU y memoria para determinar los porcentajes de uso de CPU y memoria a lo largo del tiempo. Para mostrar un intervalo de tiempo diferente, seleccione uno de los controles situados encima del gráfico o gráfico. Puede visualizar la información disponible para 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 el software SANtricity.
Nombre de la controladora de almacenamiento	El nombre del dispositivo StorageGRID que se muestra en el software 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 al software SANtricity a fin de 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 al software SANtricity a fin de solucionar problemas de almacenamiento. Algunos modelos de dispositivos no tienen una controladora de almacenamiento B.
WWID de la controladora de almacenamiento	El identificador mundial de la controladora de almacenamiento que se muestra en el software 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 el software SANtricity. 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 están 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 del 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 modelos de dispositivos que no contienen un 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 en modelos de dispositivos que no tienen hardware de computación y almacenamiento separados.
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 y SG6060X.
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.

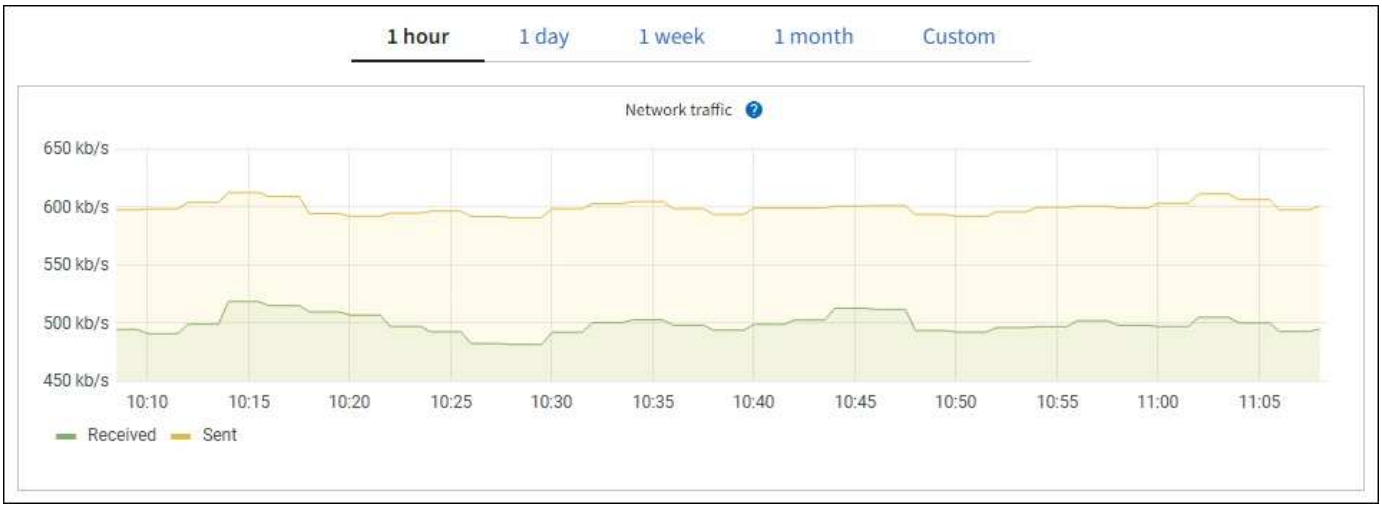
4. Confirmar que todos los Estados son «'nominales'».

   Si un estado no es "'nominal'", revise cualquier alerta actual. También puede usar System Manager de

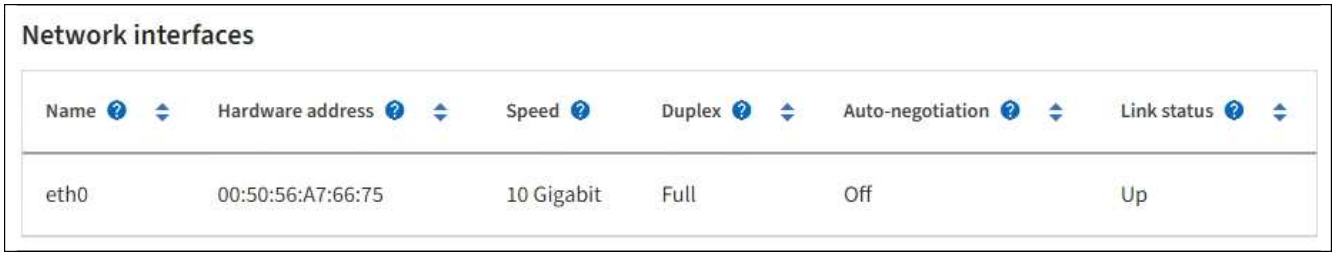
SANtricity para obtener más información acerca de estos valores de hardware. Consulte las instrucciones de instalación y mantenimiento del aparato.

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

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



1. Revise la sección Network interfaces.



Network interfaces

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

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

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

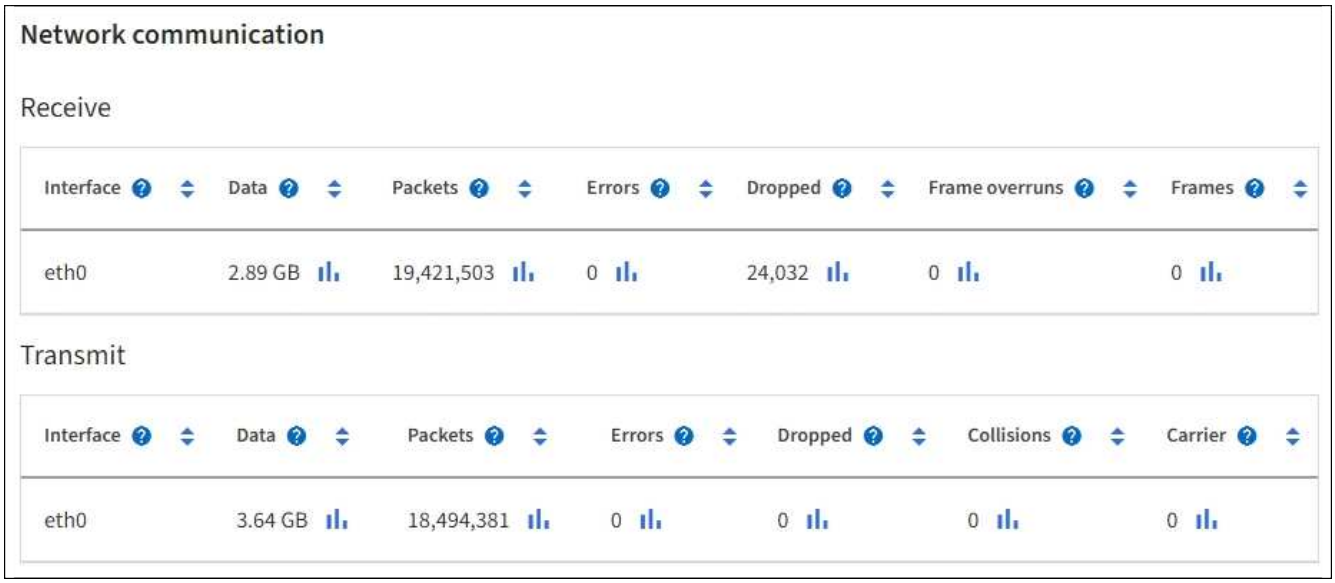
Modo de enlace	Modo de agregación	Velocidad de enlace de HIC individual (hipo 1, hipo 2, hipo 4)	Velocidad esperada de la red Grid/cliente (eth0,eth2)
Agregado	LACP	25	100
Fija	LACP	25	50
Fija	Activa/Backup	25	25
Agregado	LACP	10	40
Fija	LACP	10	20

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

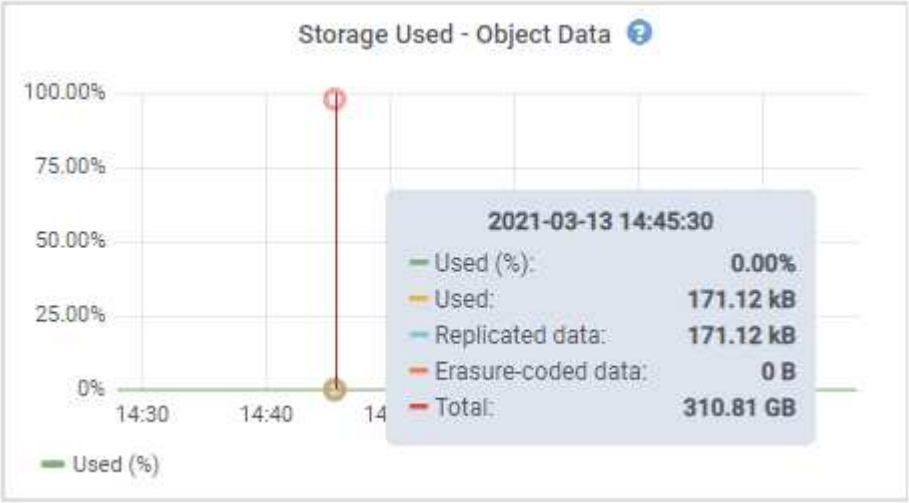
Consulte las instrucciones de instalación y mantenimiento del dispositivo para obtener más información acerca de la configuración de los puertos 10/25-GbE.

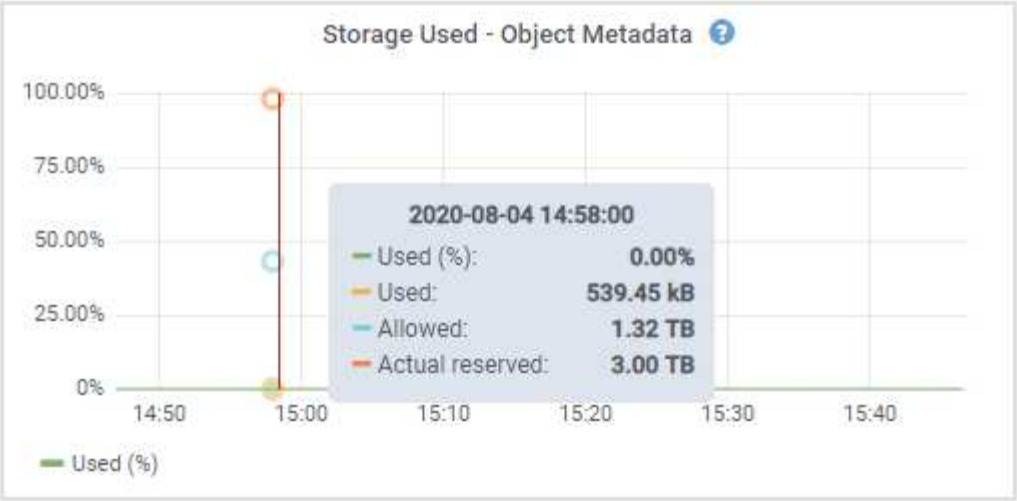
2. Revise la sección Comunicación de red.

   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.



3. 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) de volúmenes que se muestra cuando se ven propiedades de volumen estándar en el software 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
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

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG5600

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

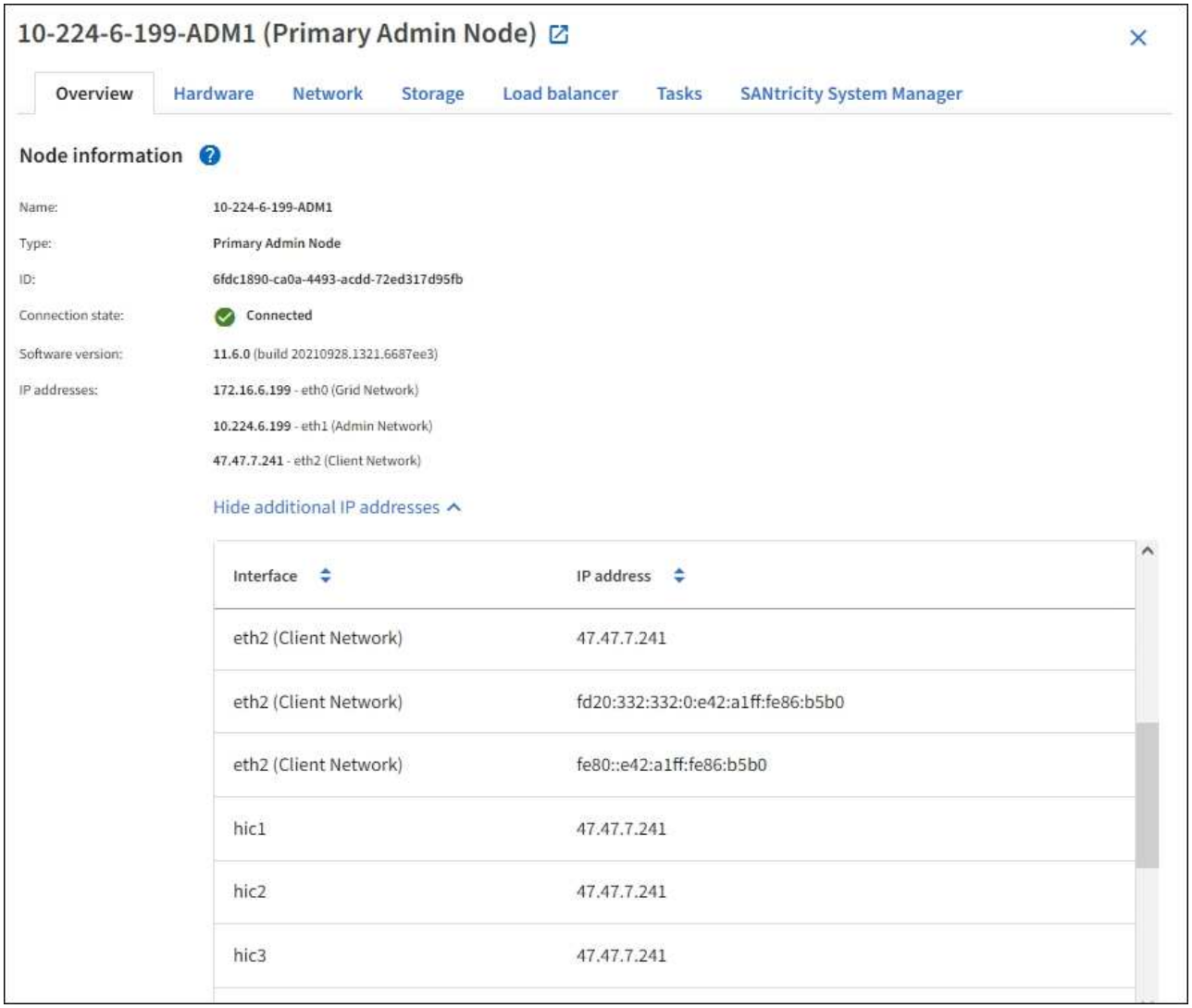
En la página Nodes, se incluye información sobre el estado del servicio y todos los recursos computacionales, de disco y de red para cada dispositivo de servicios que se utiliza como nodo de administración o nodo de puerta de enlace. También puede ver memoria, hardware de almacenamiento, recursos de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

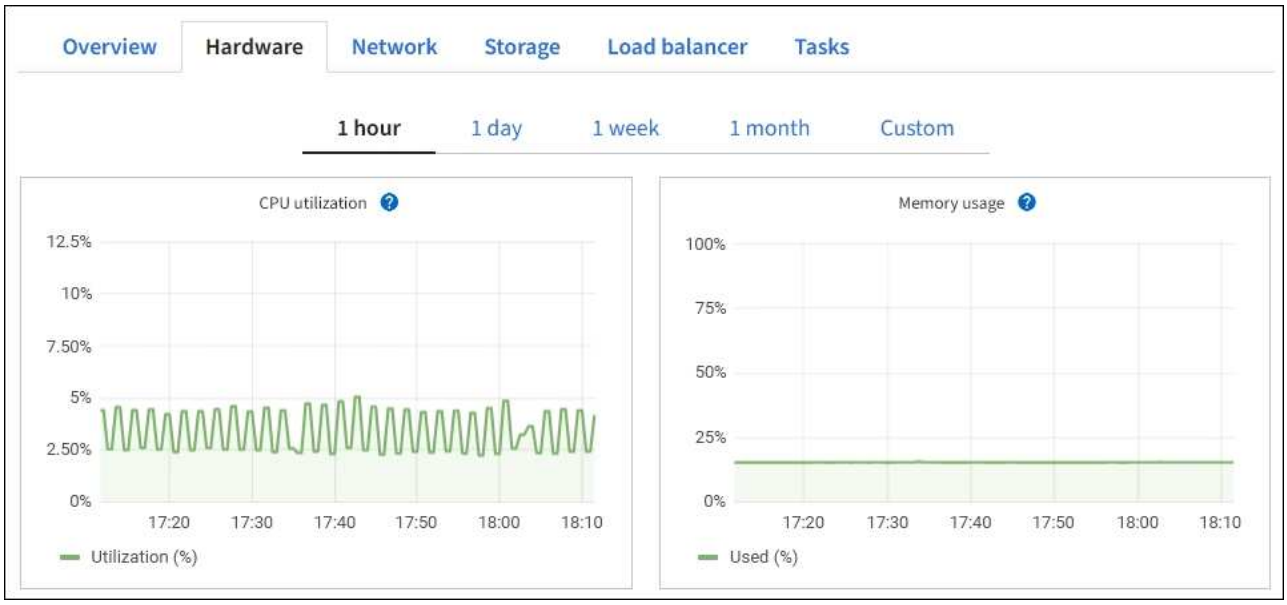
   - **Adllb** y **adlli**: Se muestra si se utiliza el enlace activo/de respaldo para la interfaz de red de administración
   - **Eth**: Red Grid, red de administración o red de cliente.
   - **Clic**: Uno de los puertos 10, 25 o 100 GbE físicos del aparato. Estos puertos se pueden unir y conectar a la 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.



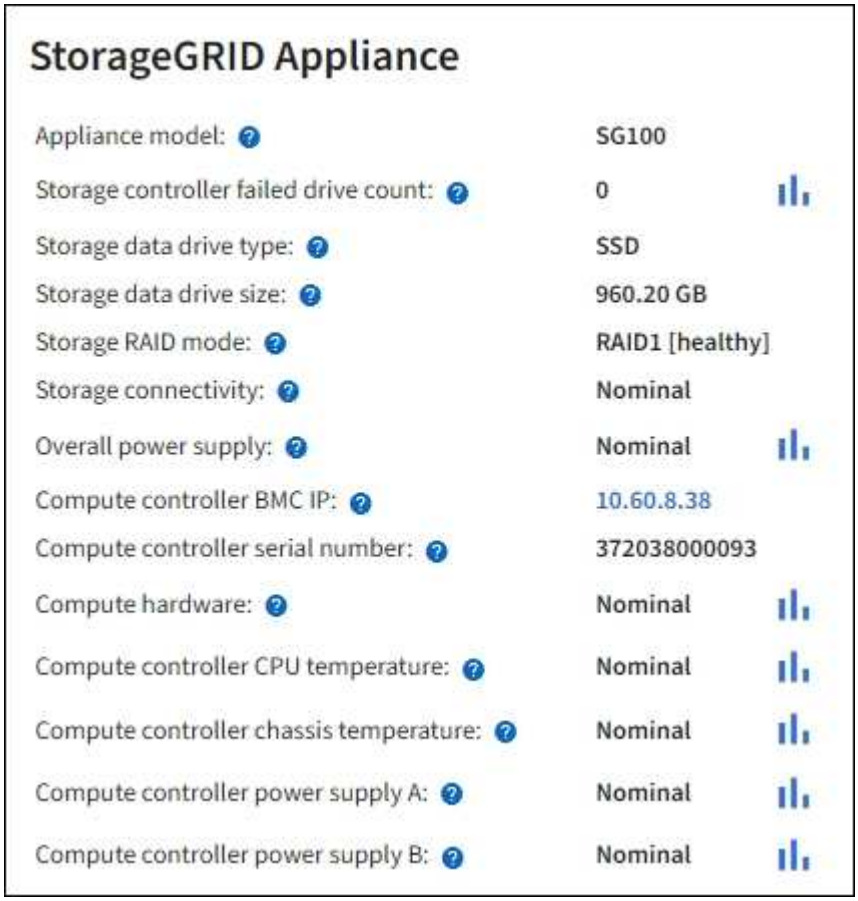
   En la sección Alerts de la pestaña Overview se muestran las alertas activas para el nodo.

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.



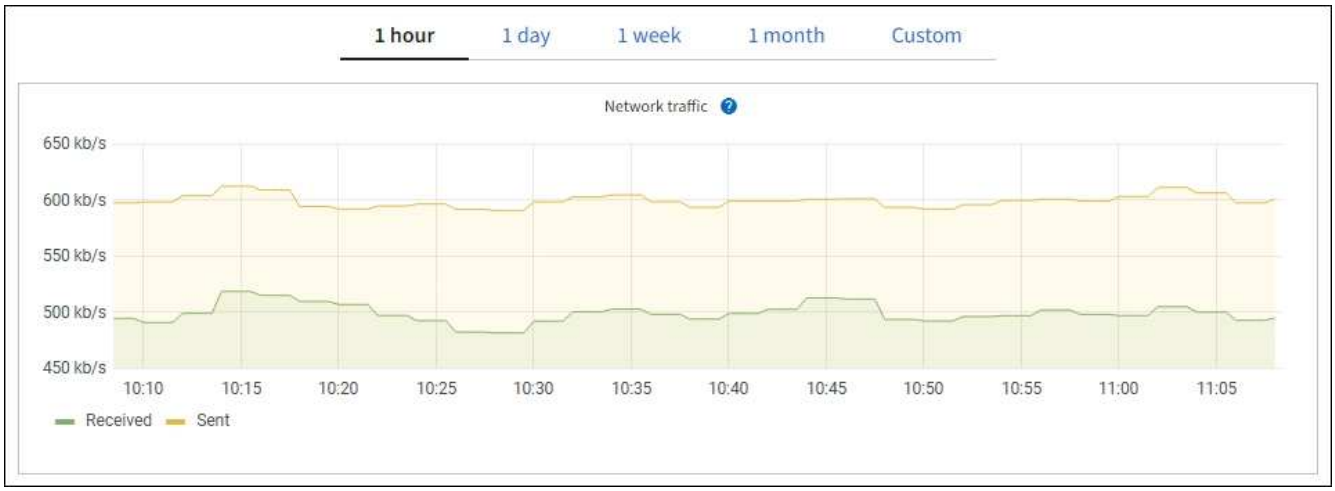
En la tabla dispositivo	Descripción
Modelo de dispositivo	El número de modelo para este dispositivo StorageGRID.
El número de unidades que la controladora de almacenamiento no pudo completar	La cantidad de unidades que no están en estado óptimo.
Tipo de unidad de datos de almacenamiento	El tipo de unidades del 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 modelos de dispositivos que no contienen un 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 cualquier alerta actual.

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

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



a. Revise la sección Network interfaces.

Network interfaces

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

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

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

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

b. Revise la sección Comunicación de red.

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

Network communication

Receive

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

Transmit

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

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

DO-REF-DC1-GW1 (Gateway Node)

Overview | Hardware | Network | Storage | Load balancer | Tasks

Disk devices

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

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.63 GB	Unknown

Información relacionada

Servicios de aplicaciones SG100 y SG1000

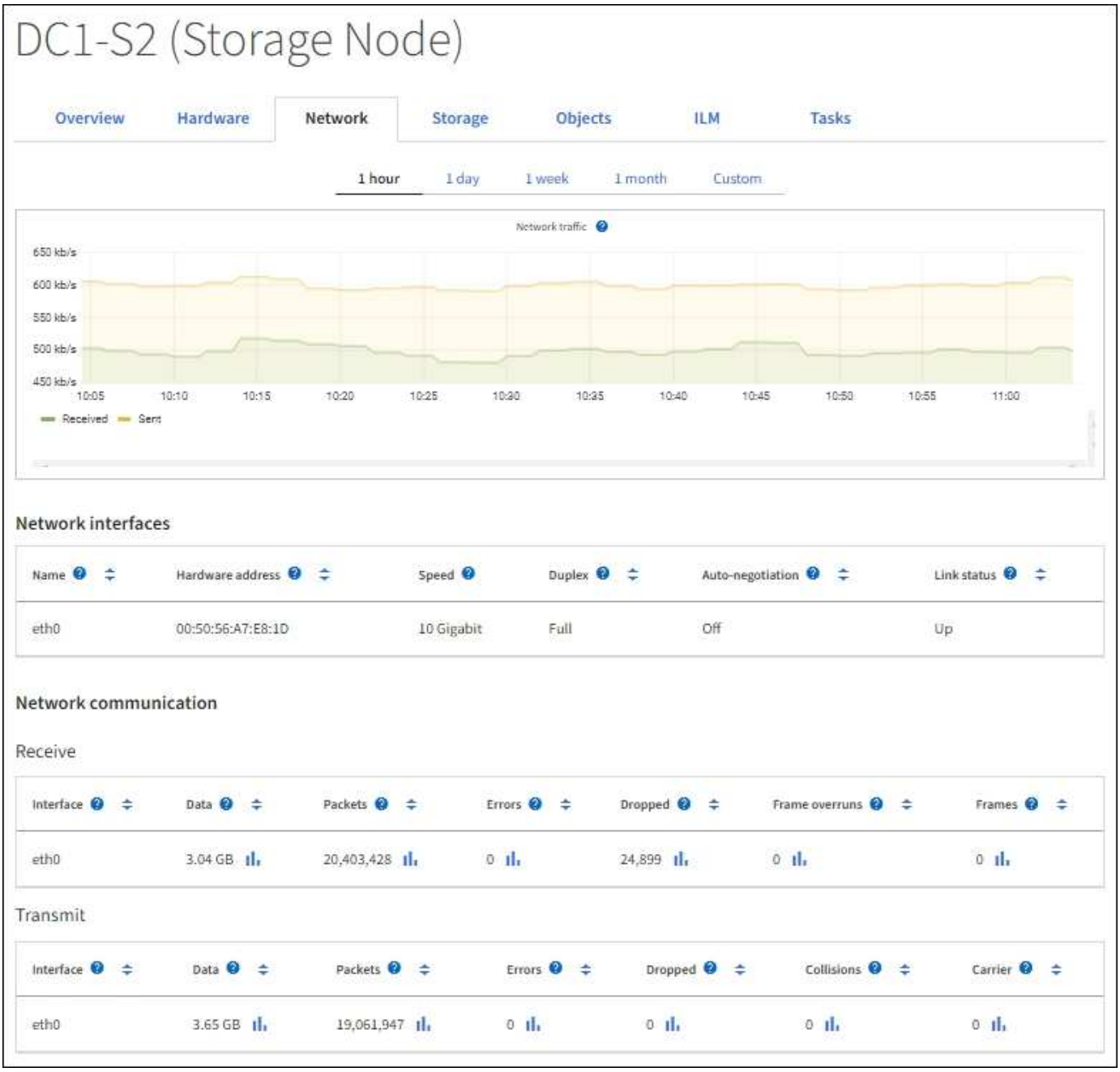
Abra la pestaña Network

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

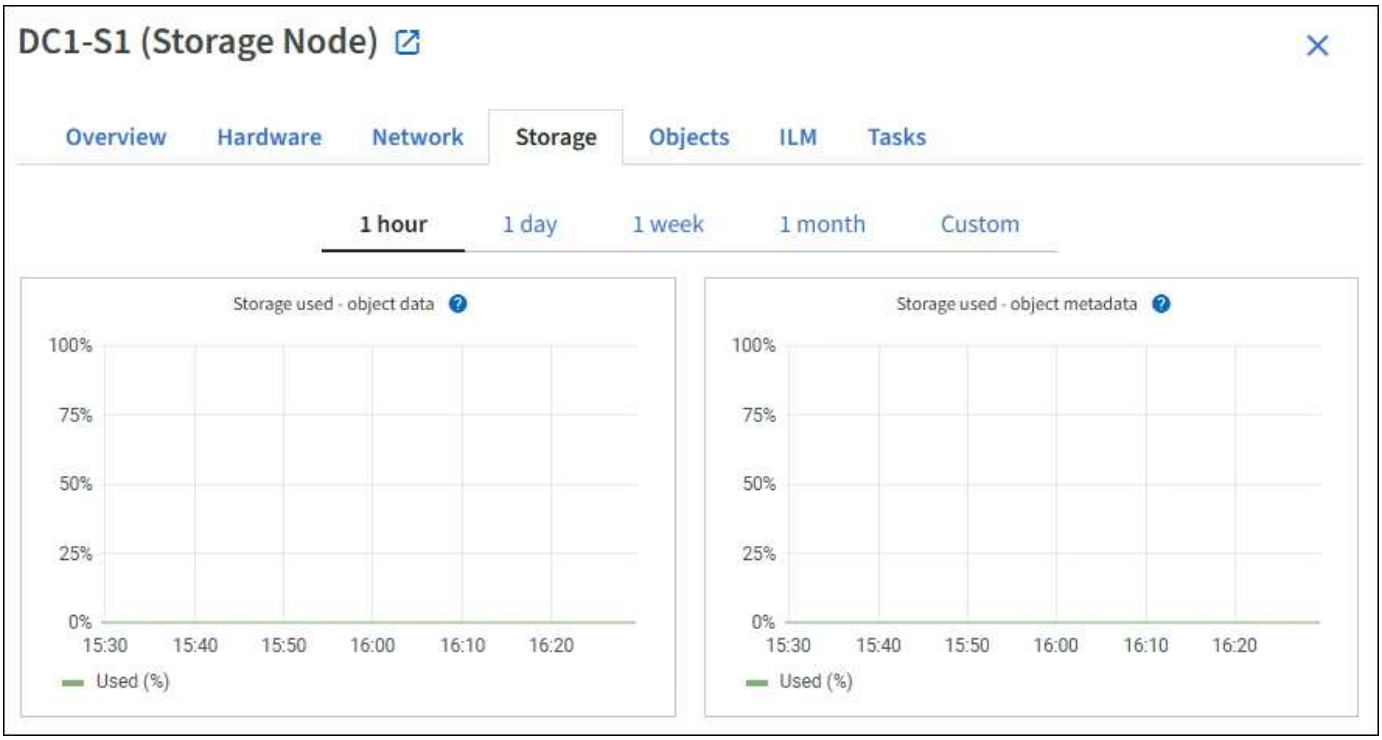
La pestaña almacenamiento resume la disponibilidad del almacenamiento y otras medidas relacionadas con él.

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.

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



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

Utilice la ficha tarea para reiniciar un nodo de cuadrícula

La ficha tarea le permite reiniciar el nodo seleccionado. La ficha tarea se muestra para todos los nodos.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

- Tiene el permiso de mantenimiento o acceso raíz.
- Tiene la clave de acceso de aprovisionamiento.

Acerca de esta tarea

Puede utilizar la ficha tarea para reiniciar un nodo. En el caso de los nodos del dispositivo, también puede utilizar la ficha tarea para colocar el dispositivo en modo de mantenimiento.

- Al reiniciar un nodo de cuadrícula desde la pestaña tarea se emite el comando de reinicio en el nodo de destino. Cuando reinicia un nodo, el nodo se apaga y se reinicia. Todos los servicios se reinician automáticamente.

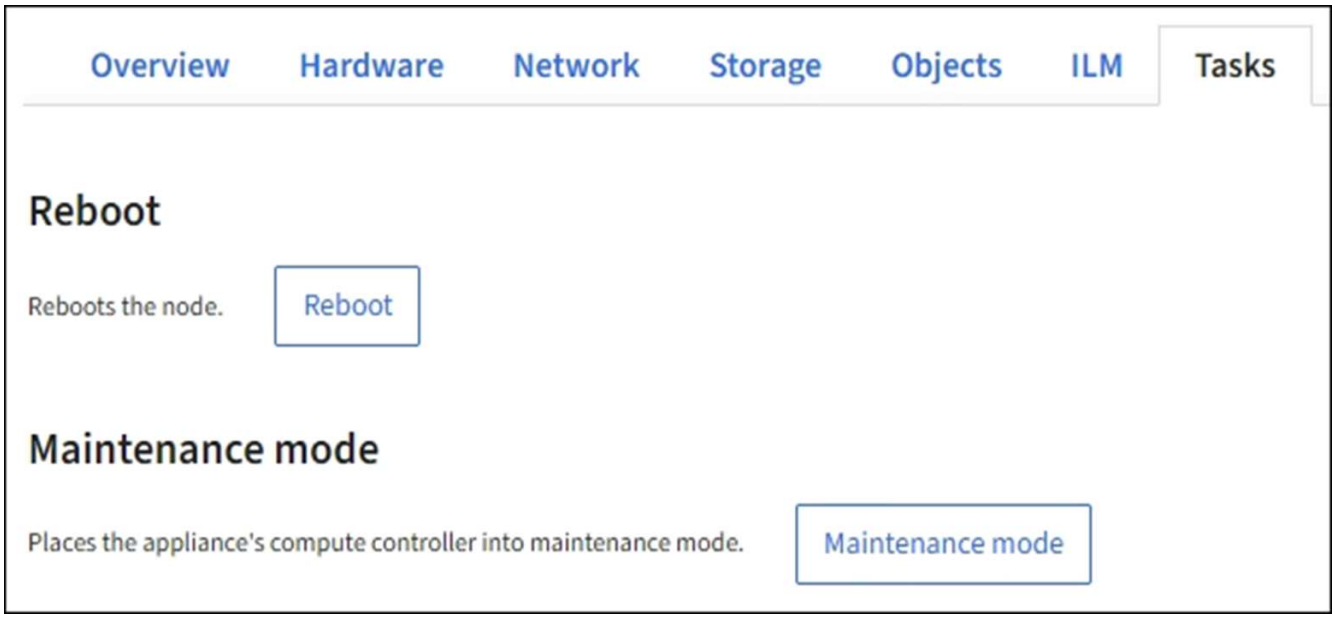
  Si planea reiniciar un nodo de almacenamiento, tenga en cuenta lo siguiente:

  - Si una regla de ILM especifica un comportamiento de procesamiento del COMMIT doble o la regla especifica un equilibrio y no es posible crear de inmediato todas las copias necesarias, StorageGRID confirma de inmediato cualquier objeto recién ingerido en dos nodos de almacenamiento en el mismo sitio y evalúa ILM más adelante. Si desea reiniciar dos o más nodos de almacenamiento en un sitio determinado, es posible que no pueda acceder a estos objetos durante el reinicio.
  - 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.
- Es posible que deba colocar un dispositivo StorageGRID en modo de mantenimiento para realizar determinados procedimientos, como cambiar la configuración del enlace o sustituir una controladora de almacenamiento. Para obtener instrucciones, consulte las instrucciones de instalación y mantenimiento del hardware del dispositivo.

  En raras ocasiones, una vez que se coloca un dispositivo StorageGRID en modo de mantenimiento puede hacer que el dispositivo no esté disponible para el acceso remoto.

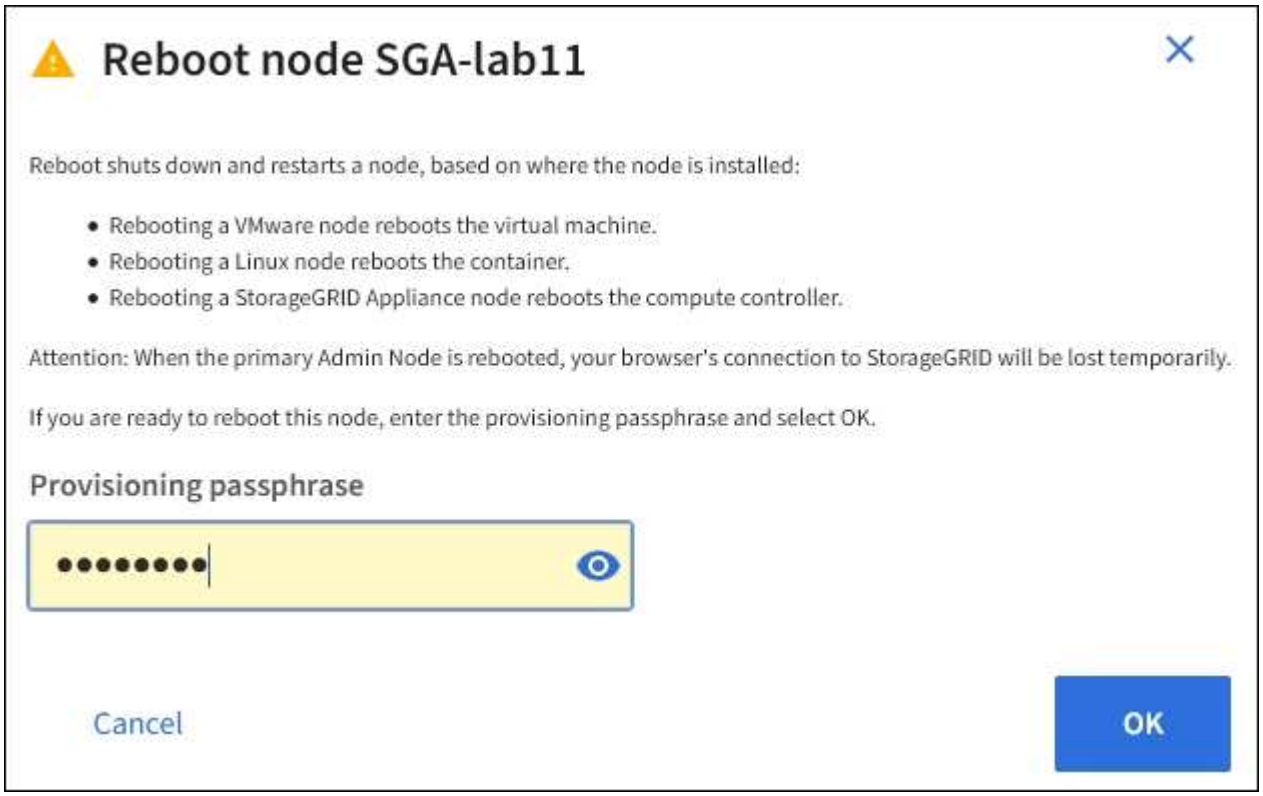
Pasos

1. Seleccione **NODES**.
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 haga clic en **Aceptar**.
6. Espere a que se reinicie el nodo.

El apagado de los servicios puede llevar cierto tiempo.

Cuando el nodo se está reiniciando, el icono gris (administrativamente abajo) aparece en el lado izquierdo de la página **Nodes**. Una vez que todos los servicios se han iniciado de nuevo y el nodo se ha conectado correctamente a la cuadrícula, la página * Nodes* debe mostrar un estado normal (no hay iconos a la izquierda del nombre del nodo), lo que indica que no hay alertas activas y que el nodo está conectado a la cuadrícula.

Información relacionada

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG5600

Servicios de aplicaciones SG100 y SG1000

Abra la pestaña objetos

La ficha objetos proporciona información acerca de S3 y.. Swift las tasas de procesamiento y recuperación.

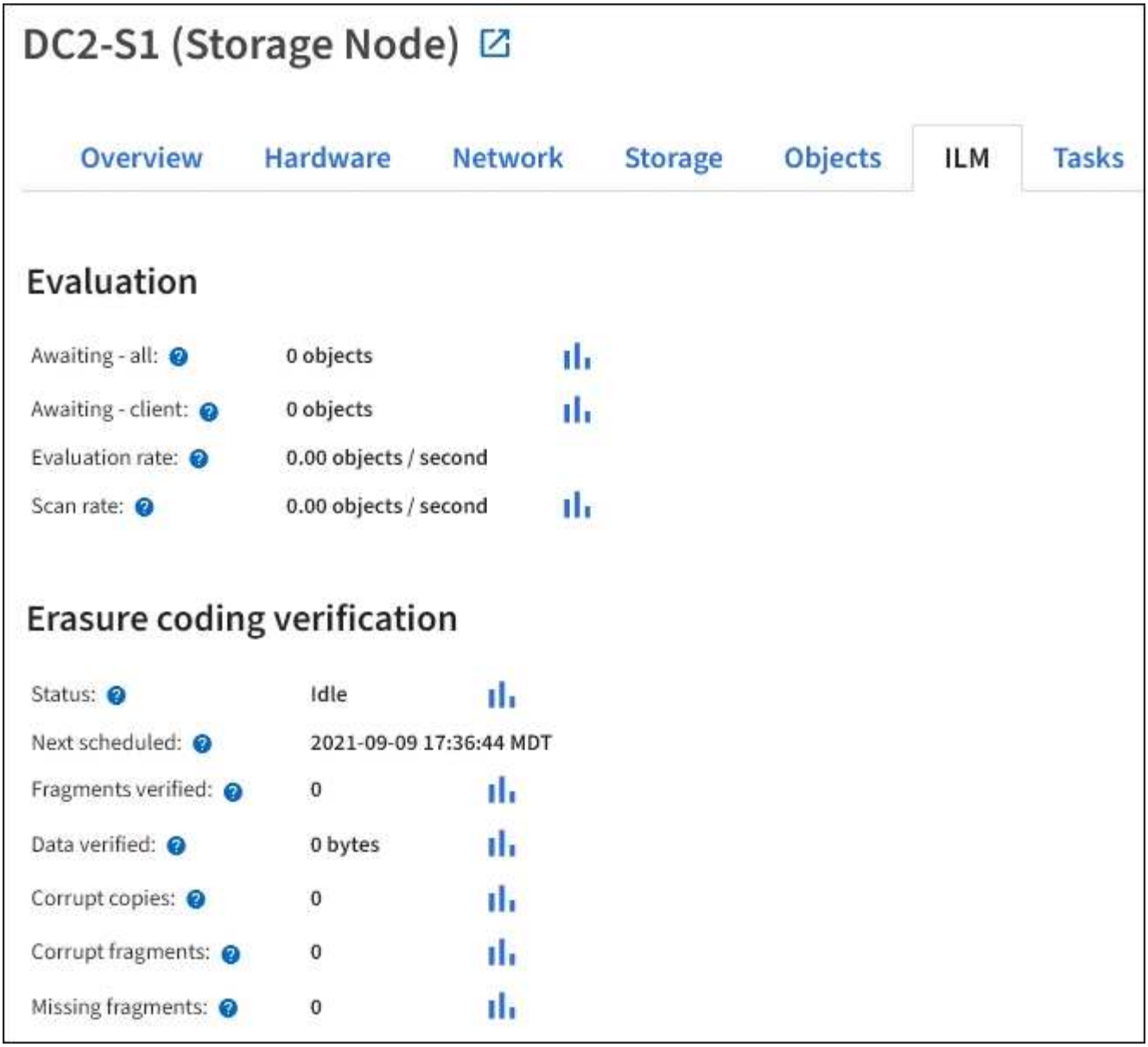
La pestaña Objects se muestra para cada nodo de almacenamiento, cada sitio y toda la cuadrícula. Para los nodos de almacenamiento, la pestaña Objects también proporciona información y recuentos de objetos acerca de consultas de metadatos y verificación en segundo plano.

Vea la pestaña ILM

La pestaña ILM proporciona información acerca de las operaciones de gestión del ciclo de vida 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 codificados de borrado.



Información relacionada

Supervise la gestión del ciclo de vida de la información

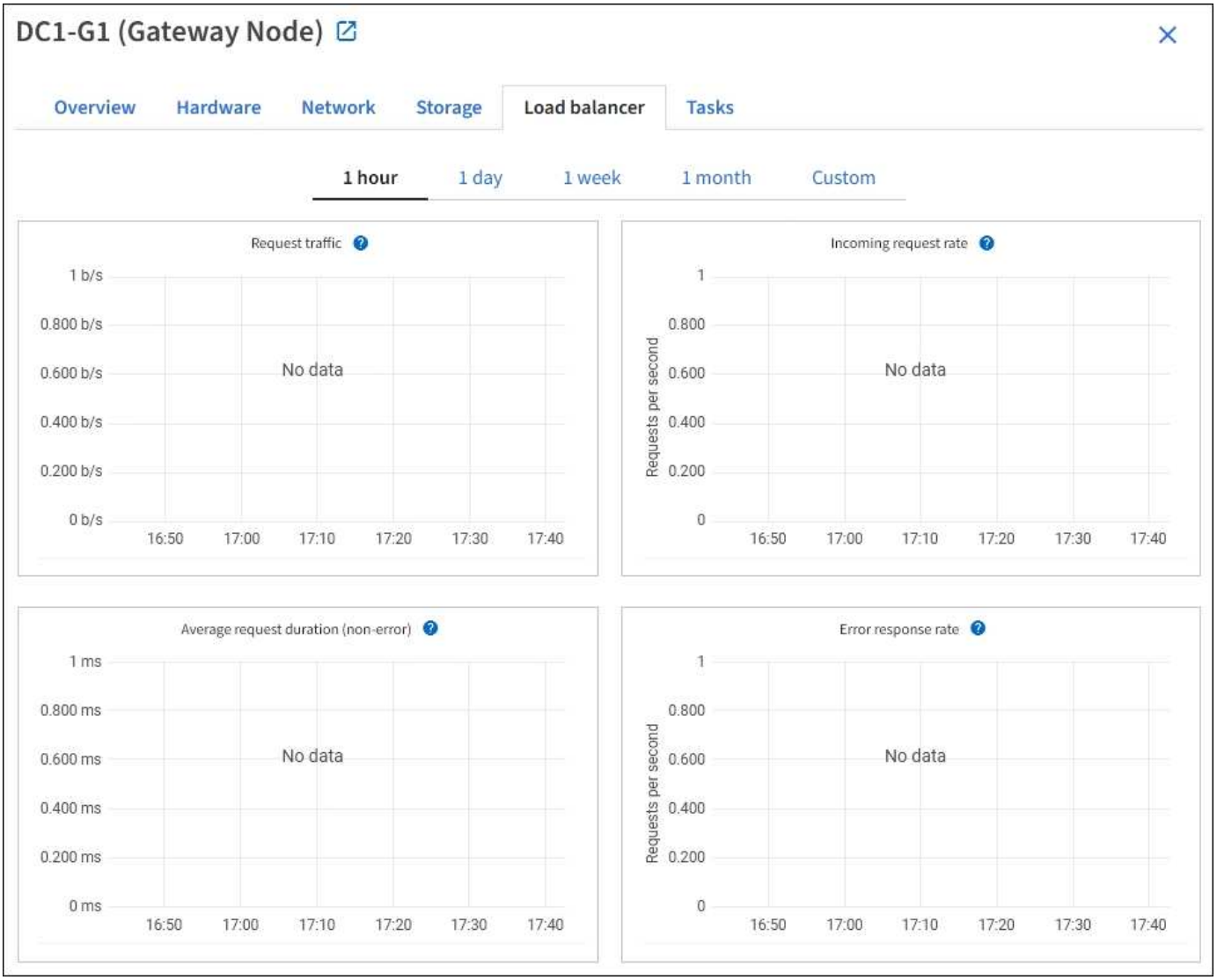
Administre StorageGRID

Vea la pestaña Load Balancer

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 ejecuta ninguna E/S a través del servicio Load Balancer o no hay ningún equilibrio de carga configurado, los gráficos muestran "'sin 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

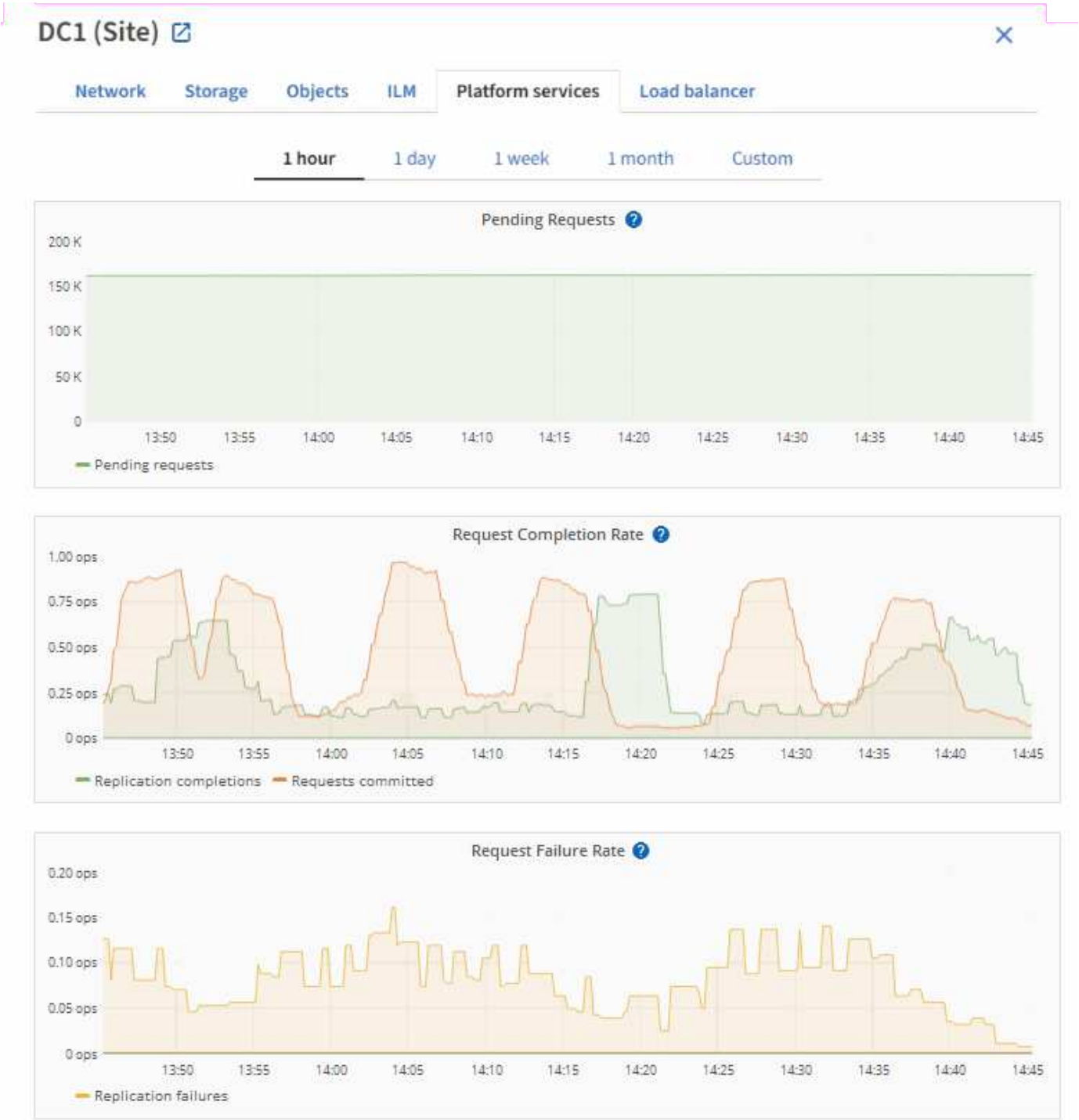
Supervisar las operaciones de equilibrio de carga

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.

Consulte la pestaña System Manager de SANtricity

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 se muestra para los nodos del dispositivo de almacenamiento.

Con SANtricity System Manager, puede hacer lo siguiente:

- Vea datos de rendimiento como el rendimiento en el nivel de la cabina de almacenamiento, la latencia de I/o, el uso de CPU de la controladora de almacenamiento y el rendimiento
- Comprobar el estado de los componentes de hardware
- Realice funciones de soporte, entre ellas, la visualización de datos de diagnóstico y la configuración de AutoSupport E-Series

> Para utilizar System Manager de SANtricity y configurar un proxy para la AutoSupport de E-Series, consulte las instrucciones descritas en administeringStorageGRID.

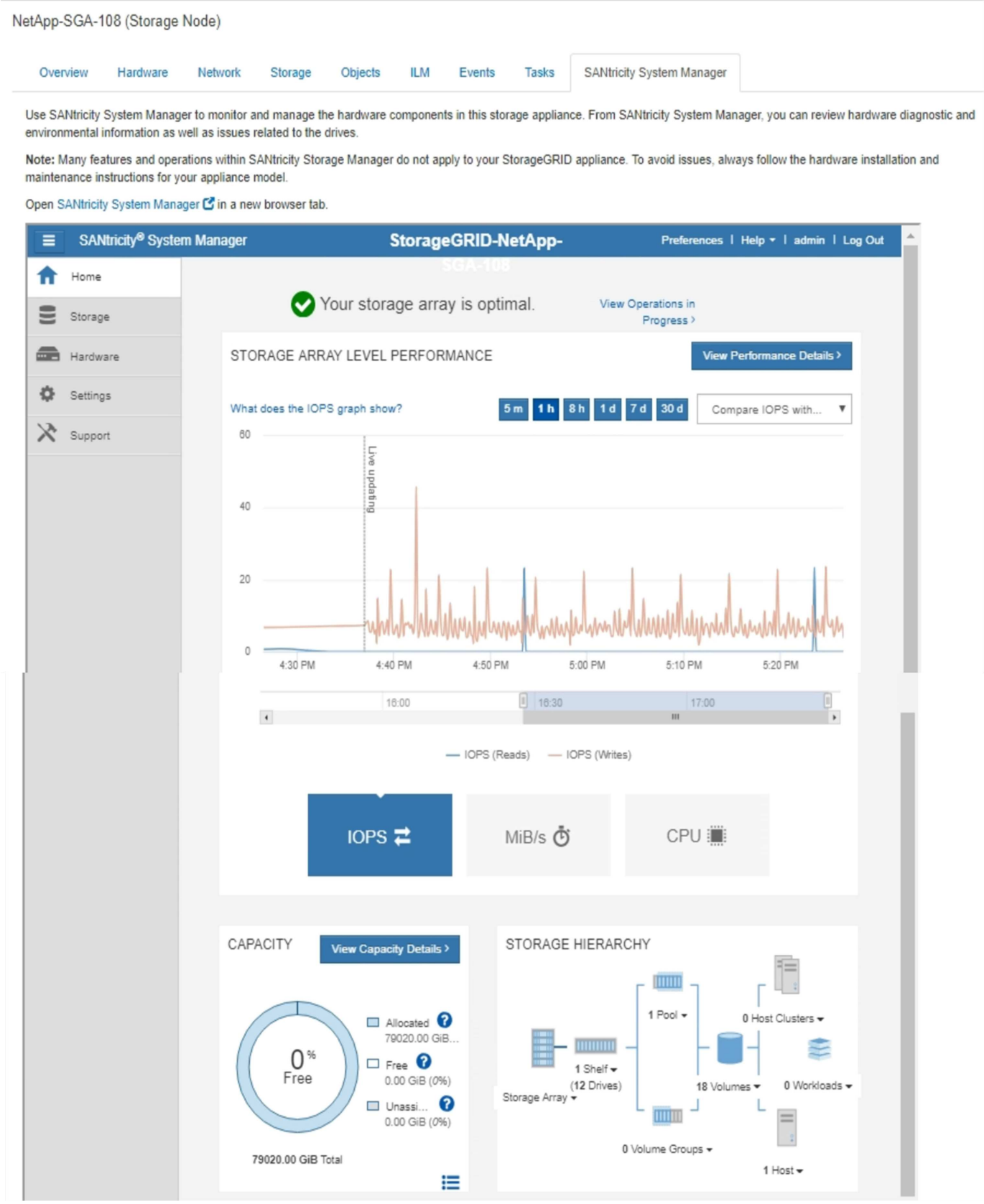
Administre StorageGRID

Para acceder a System Manager de SANtricity a través de Grid Manager, debe contar con permisos de administrador de dispositivos de almacenamiento o de acceso raíz.

> Debe tener el firmware 8.70 (11.70) 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 en SANtricity System Manager, como la actualización de firmware, no se aplican a la supervisión del dispositivo StorageGRID. Para evitar problemas, siga siempre las instrucciones de instalación y mantenimiento del hardware del 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 sobre el rendimiento de la cabina de almacenamiento y el uso de la capacidad, pase 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 que debe supervisar con regularidad

StorageGRID es un sistema de almacenamiento distribuido con tolerancia a fallos que está diseñado para continuar funcionando incluso cuando se producen errores, o cuando nodos o sitios no están disponibles. Debe supervisar de forma proactiva el estado del sistema, las cargas de trabajo y las estadísticas de uso para que pueda tomar medidas para abordar posibles problemas antes de que afecten a la eficiencia o la disponibilidad del grid.

Un sistema ocupado genera grandes cantidades de información. Esta sección proporciona orientación sobre la información más importante que se debe supervisar de forma continua.

Qué supervisar	Frecuencia
La datos de estado del sistema Se muestra en el Panel de Grid Manager. Tenga en cuenta que cualquier cosa ha cambiado con respecto al día anterior.	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
Rendimiento y conexiones de red	Semanal
Recursos en el nivel de nodo	Semanal
Actividad de inquilino	Semanal
Capacidad del sistema de almacenamiento de archivos externo	Semanal
Operaciones de equilibrio de carga	Tras la configuración inicial y tras cualquier cambio en la configuración
Disponibilidad de revisiones de software y actualizaciones de software	Mensual

Supervise el estado del sistema

Debe supervisar el estado general del sistema StorageGRID a diario.

Acerca de esta tarea

El sistema StorageGRID es tolerante a fallos y puede seguir funcionando incluso cuando no hay partes de la cuadrícula. Es probable que el primer signo de un problema potencial en el sistema de StorageGRID sea una

alerta o una alarma (sistema heredado) y no necesariamente un problema en el funcionamiento del sistema. Prestar atención al estado del sistema puede ayudarle a detectar problemas menores antes de que afecten a operaciones o a la eficiencia del grid.

El panel Estado del Panel de Grid Manager proporciona un resumen de los problemas que pueden afectar al sistema. Debe investigar los problemas que se muestran en la consola.

> Para recibir notificaciones de alertas en cuanto se activen, se pueden configurar notificaciones por correo electrónico para alertas o capturas SNMP.

Pasos

1. Inicie sesión en Grid Manager para ver el panel.
2. Revise la información del panel Estado.

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

Enlace	Lo que indica
Detalles de la cuadrícula	Aparece si hay nodos desconectados (estado de conexión desconocido o administrativamente inactivo). Haga clic en el enlace o haga clic en el icono azul o gris para determinar qué nodo o nodos están afectados.
Alertas actuales	Aparece si hay alguna alerta activa en ese momento. Haga clic en el enlace o haga clic en **crítico**, **mayor** o **menor** para ver los detalles en la página **ALERTAS** > **actual**.
Alertas resueltas recientemente	Aparece si se han resuelto todas las alertas activadas en la última semana. Haga clic en el enlace para ver los detalles en la página **ALERTS** > **Resolved**.
Licencia	Aparece si se produce un problema con la licencia de software de este sistema StorageGRID. Haga clic en el enlace para ver los detalles en la página **MANTENIMIENTO** > **sistema** > **Licencia**.

Información relacionada

- Administre StorageGRID

- Configure notificaciones por correo electrónico para las alertas
- Usar supervisión de SNMP

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. Debe supervisar los estados de conexión de los nodos y solucionar los problemas inmediatamente.

Lo que necesitará

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

Acerca de esta tarea

Los nodos pueden tener uno de los tres estados de conexión:

- **No conectado - Desconocido** : El nodo no está conectado a la cuadrícula por una razón desconocida. Por ejemplo, se ha perdido la conexión de red entre los nodos o se ha apagado el suministro eléctrico. 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.

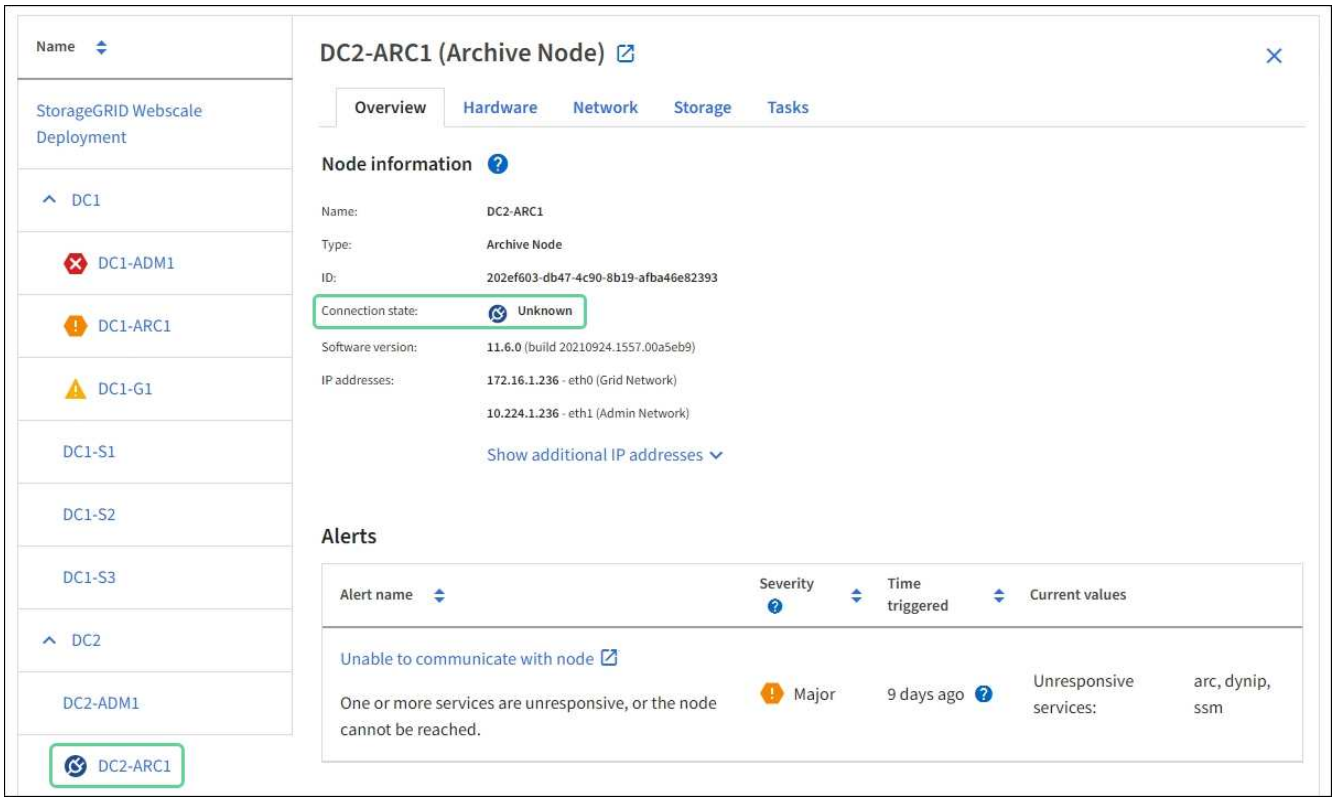
- **No conectado - administrativamente abajo** : El nodo no está conectado a la cuadrícula por un motivo esperado. Por ejemplo, el nodo o los servicios del nodo se han apagado correctamente, el nodo se está reiniciando o se está actualizando el software. Una o más alertas también pueden estar activas.
- **Conectado** : El nodo está conectado a la cuadrícula.

Pasos

1. Si aparece un icono azul o gris en el panel Estado del Panel de control, haga clic en el icono o haga clic en **Detalles de la cuadrícula**. (Los iconos azul o gris y el vínculo **Detalles de la cuadrícula** sólo aparecen si al menos un nodo está desconectado de la cuadrícula.)

   Aparece la página Descripción general del primer nodo azul del árbol de nodos. Si no hay nodos azules, aparece la página Descripción general del primer nodo gris del árbol.

   En el ejemplo, el nodo de almacenamiento llamado DC1-S3 tiene un icono azul. **Estado de conexión** en el panel Información del nodo es **Desconocido** y la alerta **no se puede comunicar con el nodo** está activa. La alerta indica que uno o varios servicios no responden o que no se puede acceder al nodo.



2. Si un nodo tiene un icono azul, siga estos pasos:
   a. Seleccione cada alerta de la tabla y siga las acciones recomendadas.

      Por ejemplo, es posible que deba reiniciar un servicio que haya detenido o reiniciar el host del nodo.

   b. Si no puede volver a conectar el nodo, póngase en contacto con el soporte técnico.
3. Si un nodo tiene un icono de color gris, siga estos pasos:

   Los nodos grises se esperan durante procedimientos de mantenimiento y podrían estar asociados a una o más alertas. Basándose en el problema subyacente, estos nodos «administrativamente inactivos» a menudo vuelven a estar online sin intervención.

   a. Revise la sección Alertas y determine si alguna alerta afecta a este nodo.
   b. Si una o más alertas están activas, seleccione cada alerta de la tabla y siga las acciones recomendadas.
   c. Si no puede volver a conectar el nodo, póngase en contacto con el soporte técnico.

Información relacionada

Referencia de alertas

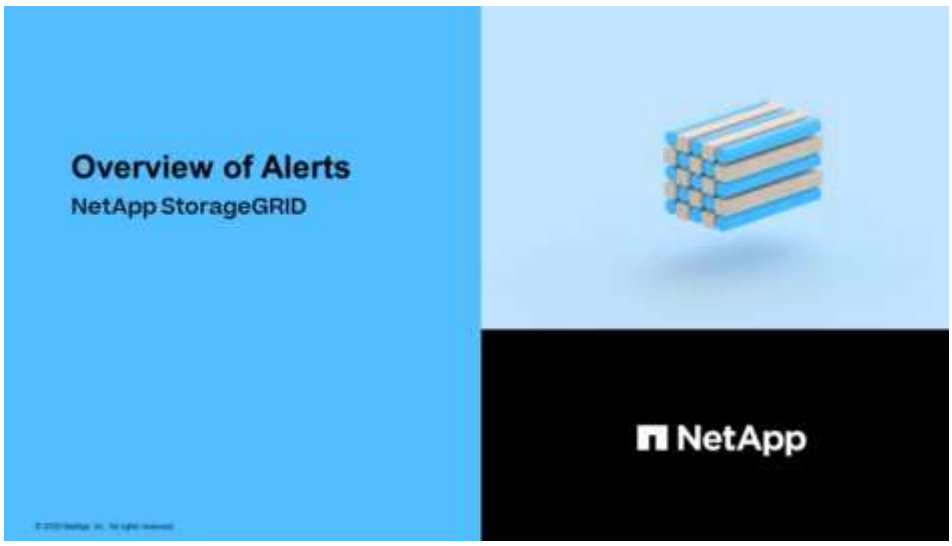
Recuperación y mantenimiento

Ver las alertas actuales

Cuando se activa una alerta, se muestra un icono de alerta en la Consola. También se muestra un icono de alerta para el nodo en la página Nodes. También es posible enviar una notificación por correo electrónico, a menos que se haya silenciado la alerta.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Opcionalmente, ha visto el vídeo: "Vídeo: Descripción general de las alertas".

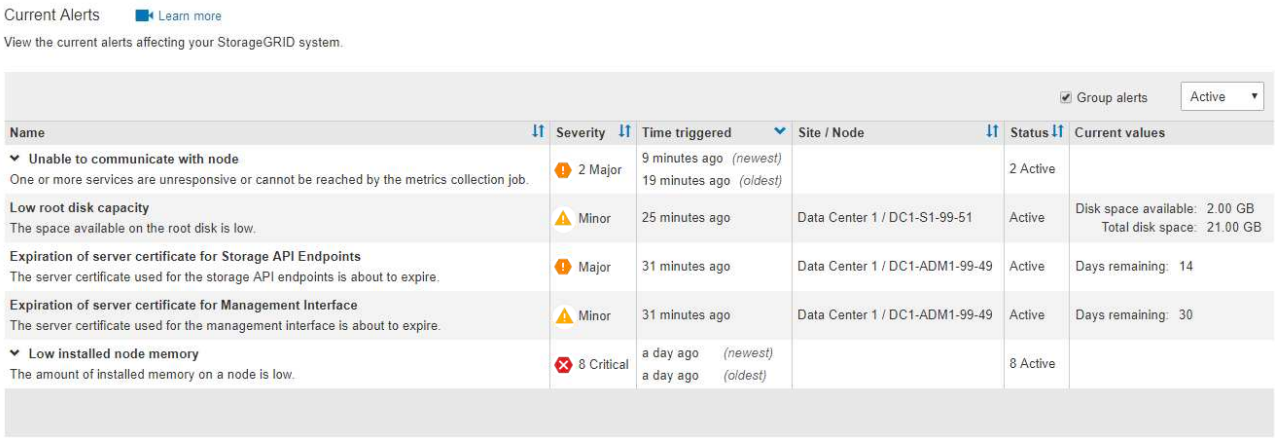


Pasos

1. Si una o más alertas están activas, realice una de las siguientes acciones:

   - En el panel Estado del Panel, haga clic en el icono de alerta o haga clic en **Alertas actuales**. (Un icono de alerta y el enlace **Alertas actuales** sólo aparecen si al menos una alerta está activa.)
   - Seleccione **ALERTS** > **Current**.

     Aparece la página Alertas actuales. Enumera todas las alertas que actualmente afectan a su sistema StorageGRID.



     De forma predeterminada, las alertas 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 que se han silenciado.
   - 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

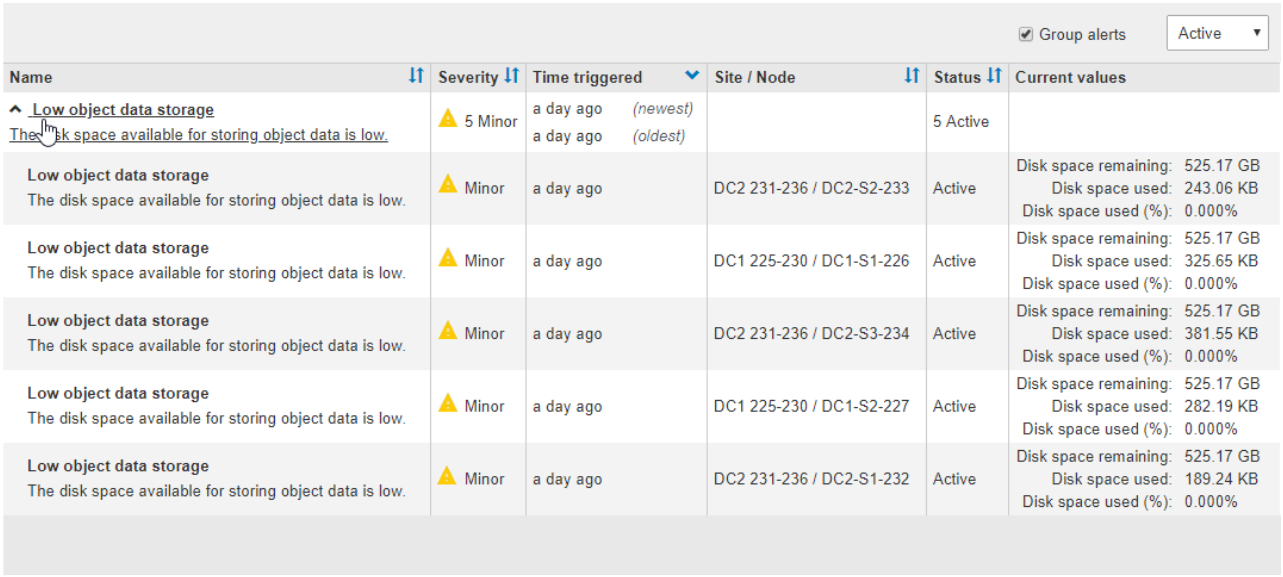
gravedades leve, grave y crítica, solo se muestra la alerta crítica.

La página Alertas actuales se actualiza cada dos minutos.

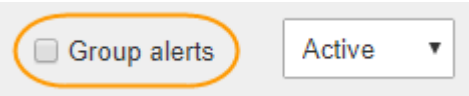
2. Revise la información de la tabla.

Encabezado de columna	Descripción
Nombre	El nombre de la alerta y su descripción.
Gravedad	La gravedad de la alerta. Si se agrupan varias alertas, la fila del 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 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. Deberá supervisar y resolver las alertas menores que no se despicen por sí mismas para asegurarse de que no provoquen un problema más grave.
Tiempo activado	¿Cuánto tiempo hace que se activó la alerta? 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*).
Sitio/nodo	El nombre del sitio y del nodo donde se produce la alerta. Si se agrupan varias alertas, los nombres de sitio y nodo no se muestran en la fila del título.
Estado	Si la alerta está activa o ha sido silenciada. 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.
Valores actuales	El valor actual de la métrica que provocó la 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, los valores actuales no se muestran en la fila de título.

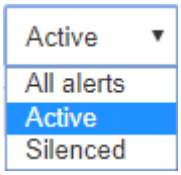
3. Para expandir y contraer grupos de alertas:
   - Para mostrar las alertas individuales de un grupo, haga clic en el signo de intercalación hacia abajo ⌄ en el encabezado o haga clic en el nombre del grupo.
   - Para ocultar las alertas individuales de un grupo, haga clic en el signo de intercalación arriba ⌃ en el encabezado o haga clic en el nombre del grupo.



4. Para mostrar alertas individuales en lugar de grupos de alertas, anule la selección de la casilla de verificación **Alertas de grupo** en la parte superior de la tabla.



5. Para ordenar las alertas o los grupos de alertas, haga clic en 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 **Alertas de grupo** no está seleccionada, 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.
6. Para filtrar las alertas por estado, use el menú desplegable que hay en la parte superior de la tabla.



   - Seleccione **todas las alertas** para ver todas las alertas actuales (alertas activas y silenciadas).
   - Seleccione **activo** para ver sólo las alertas actuales que están activas.
   - Seleccione **silenciado** para ver sólo las alertas actuales que se han silenciado. Consulte Silenciar notificaciones de alerta.
7. Para ver los detalles de una alerta específica, seleccione la alerta en la tabla.

Se muestra un cuadro de diálogo de la alerta. Consulte Ver una alerta específica.

Ver alertas resueltas

Es posible buscar y ver un historial de alertas que se han resuelto.

Lo que necesitará

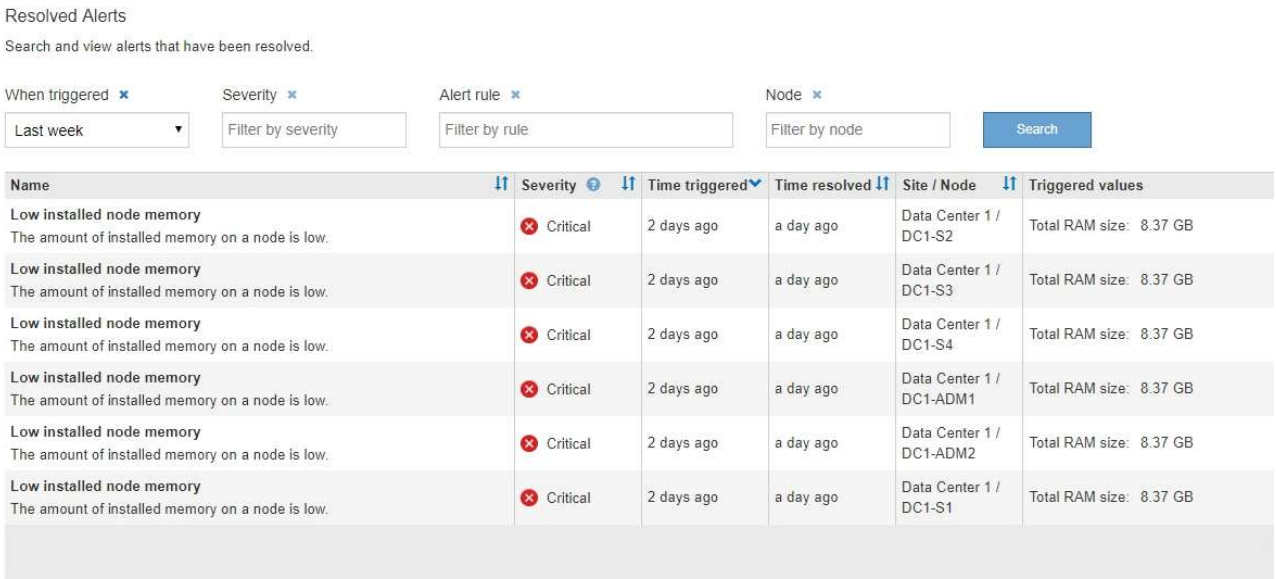
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.

Pasos

1. Para ver las alertas resueltas, realice una de las siguientes acciones:
   - En el panel Estado del Panel, haga clic en **Alertas resueltas recientemente**.

     El enlace **Alertas resueltas recientemente** aparece sólo si una o más alertas se han activado en la última semana y ahora se han resuelto.

   - Seleccione **ALERTS** > **Resolved**. Aparece la página Alertas resueltas. De forma predeterminada, se muestran las alertas resueltas que se activaron durante la última semana, y las alertas activadas más recientemente se muestran primero. Las alertas de esta página se mostraban previamente en la página Alertas actuales o en una notificación por correo electrónico.



2. Revise la información de la tabla.

Encabezado de columna	Descripción
Nombre	El nombre de la alerta y su descripción.

Encabezado de columna	Descripción
Gravedad	La gravedad de la alerta. • **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. Deberá supervisar y resolver las alertas menores que no se despicen por sí mismas para asegurarse de que no provoquen un problema más grave.
Tiempo activado	¿Cuánto tiempo hace que se activó la alerta?
Tiempo resuelto	Hace cuánto tiempo se resolvió la alerta.
Sitio/nodo	El nombre del sitio y del nodo donde se produjo la alerta.
Valores activados	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.

3. Para ordenar la lista completa de alertas resueltas, haga clic en las flechas arriba/abajo en cada encabezado de columna.

   Por ejemplo, es posible que desee ordenar las alertas resueltas por **Sitio/nodo** para ver las alertas que afectan a un nodo específico.

4. Opcionalmente, puede filtrar la lista de alertas resueltas utilizando los menús desplegables de la parte

superior de la tabla.

a. Seleccione un período de tiempo en el menú desplegable **cuando se activó** para mostrar alertas resueltas en función de cuánto tiempo se activaron.

   Puede buscar alertas que se hayan activado en los siguientes periodos de tiempo:

   - Última hora
   - Último día
   - Última semana (vista predeterminada)
   - El mes pasado
   - Cualquier período de tiempo
   - Personalizado (permite especificar la fecha de inicio y la fecha de finalización del período de tiempo)

b. Seleccione una o más gravedades en el menú desplegable **severidad** para filtrar las alertas resueltas de una gravedad específica.

c. 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.

d. Seleccione uno o más nodos en el menú desplegable **Node** para filtrar las alertas resueltas relacionadas con un nodo específico.

e. Haga clic en **Buscar**.

5. Para ver los detalles de una alerta resuelta específica, seleccione la alerta en la tabla.

   Se muestra un cuadro de diálogo de la alerta. Consulte Ver una alerta específica.

Ver una alerta específica

Puede ver información detallada sobre una alerta que afecta actualmente al sistema StorageGRID o una alerta que se ha resuelto. Los detalles incluyen acciones correctivas recomendadas, la hora en que se activó la alerta y el valor actual de las métricas relacionadas con esta alerta.

Opcionalmente, puede hacerlo silenciar una alerta actual o. actualice la regla de alerta.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

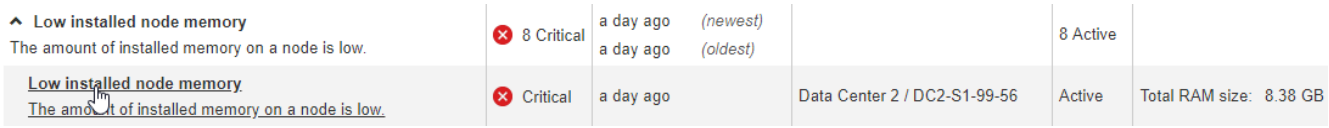
Pasos

1. Realice una de las siguientes acciones, según si desea ver una alerta actual o resuelta:

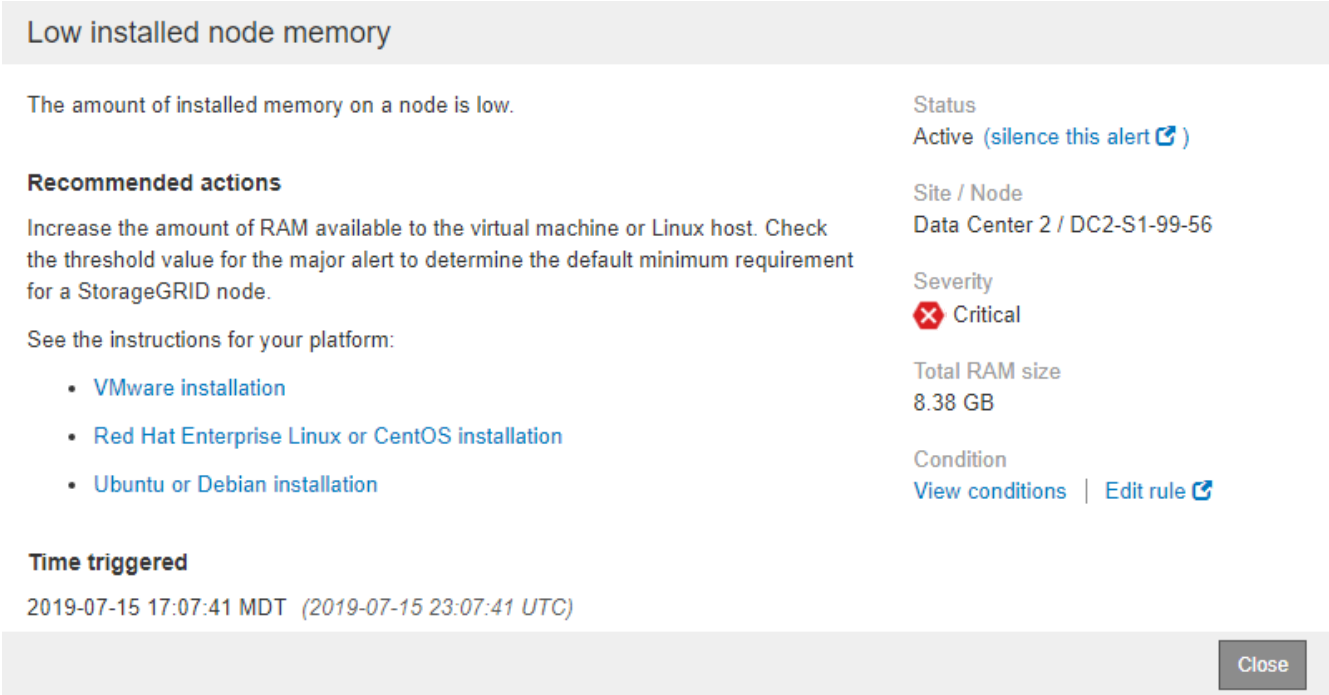
Encabezado de columna	Descripción
Alerta actual	• En el panel Estado del Panel, haga clic en el enlace **Alertas actuales**. Este enlace aparece solo si al menos una alerta está activa en ese momento. Este enlace se oculta si no hay alertas actuales o si se han silenciado todas las alertas actuales. • Seleccione **ALERTS** > **Current**. • En la página **NODES**, seleccione la ficha **Overview** para un nodo que tenga un icono de alerta. A continuación, en la sección Alertas, haga clic en el nombre de alerta.
Alerta resuelta	• En el panel Estado del Panel, haga clic en el enlace **Alertas resueltas recientemente**. (Este enlace aparece solo si se han activado una o varias alertas de la última semana y ahora se han resuelto. Este enlace está oculto si no se ha activado ninguna alerta ni se ha resuelto en la última semana.) • Seleccione **ALERTS** > **Resolved**.

2. Según sea necesario, expanda un grupo de alertas y seleccione la alerta que desee ver.

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



Se muestra un cuadro de diálogo con los detalles de la alerta seleccionada.



3. Revise los detalles de la alerta.

Información	Descripción
title	El nombre de la alerta.
primer párrafo	La descripción de la alerta.
Acciones recomendadas	Las acciones recomendadas para esta alerta.
Tiempo activado	Fecha y hora en la que se activó la alerta en la hora local y en UTC.
Tiempo resuelto	Solo para alertas resueltas, la fecha y la hora en que se resolvió la alerta en la hora local y en UTC.
Estado	El estado de la alerta: Activo, silenciado o resuelto.
Sitio/nodo	El nombre del sitio y el nodo afectados por la alerta.
Gravedad	La gravedad de la alerta. • **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. Deberá supervisar y resolver las alertas menores que no se despicen por sí mismas para asegurarse de que no provoquen un problema más grave.
valores de datos	El valor actual de la métrica de esta 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 metadatos bajo** incluyen el porcentaje de espacio en disco utilizado, la cantidad total de espacio en disco y la cantidad de espacio en disco utilizado.

4. De forma opcional, haga clic en **silenciar esta alerta** para silenciar la regla de alerta que provocó la activación de esta alerta.

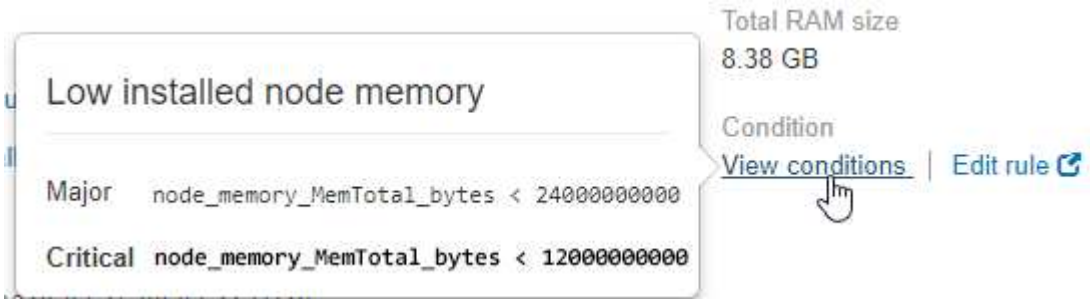
   Para silenciar una regla de alerta, debe tener el permiso Administrar alertas o acceso raíz.

> 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.

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

   a. En los detalles de la alerta, haga clic en **Ver condiciones**.

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



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

6. De forma opcional, haga clic en **Editar regla** para editar la regla de alerta que provocó la activación de esta alerta:

   Para editar una regla de alerta, debe tener el permiso Administrar alertas o acceso raíz.

   > 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.

7. Para cerrar los detalles de la alerta, haga clic en **Cerrar**.

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.

Lo que necesitará

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

Pasos

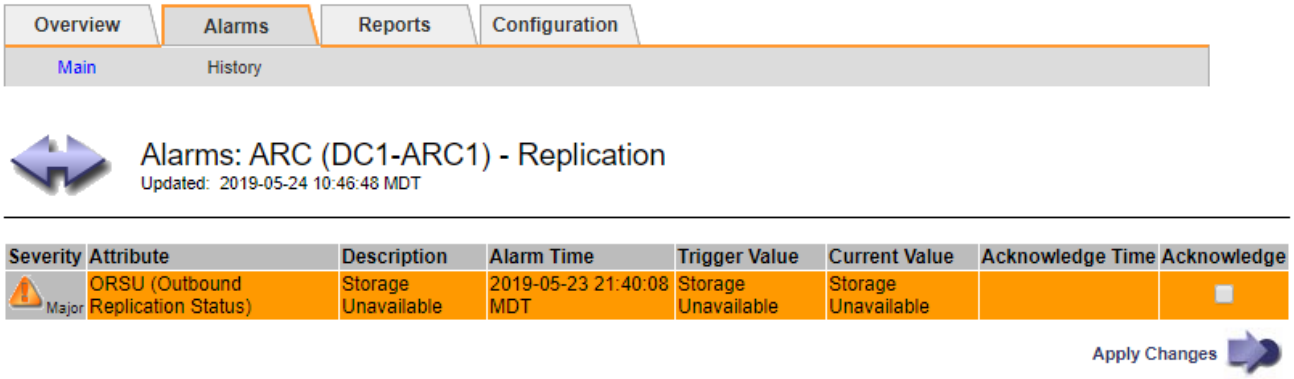
1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Current Alarms**.

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)

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

Debe supervisar la capacidad de almacenamiento general de su grid para garantizar que el espacio libre adecuado permanece 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.

Lo que necesitará

Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

Acerca de esta tarea

La consola de Grid Manager permite evaluar rápidamente cuánto almacenamiento hay 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.

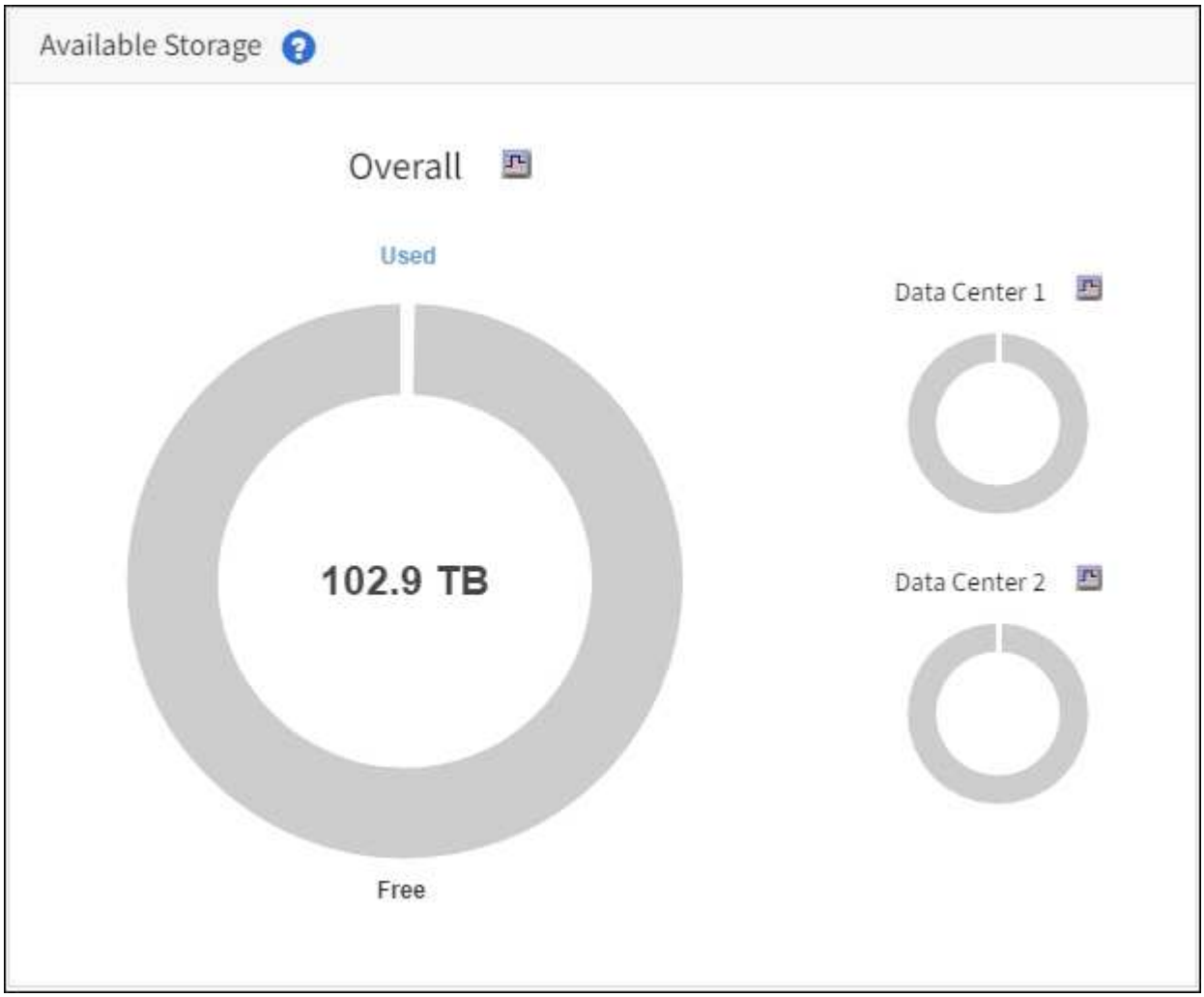
Pasos

1. Evaluar cuánto almacenamiento hay disponible para todo el grid y para cada centro de datos.

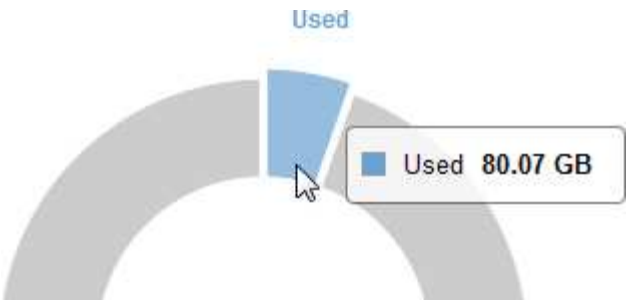
   a. Seleccione **Panel**.

   b. En el panel almacenamiento disponible, anote el resumen general de la capacidad de almacenamiento libre y utilizada.

   El resumen no incluye medios de archivado.



   a. Coloque el cursor sobre las secciones de capacidad libre o utilizada del gráfico para ver exactamente cuánto espacio está libre o utilizado.



b. En el caso de grids multisitio, revise el gráfico de cada centro de datos.

c. Haga clic en el icono del gráfico en el gráfico general o de un centro de datos individual para ver un gráfico donde se muestra el uso de la capacidad a lo largo del tiempo.

   Gráfico que muestra el porcentaje de capacidad de almacenamiento utilizada (%) frente a Hora aparece.

2. Determine cuánto almacenamiento se ha usado y cuánto almacenamiento queda disponible para los datos de objetos y los metadatos de objetos.

   a. Seleccione **NODES**.

   b. Seleccione ***grid*** > **almacenamiento**.

   c. Pase el cursor por los gráficos **almacenamiento usado - datos de objeto** 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 a lo largo del tiempo.

   > Los valores totales de un sitio o de la cuadrícula no incluyen los nodos sin especificar 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.

Si quiere más información sobre la planificación de una expansión del almacenamiento, consulte Instrucciones para ampliar StorageGRID.

Supervise la capacidad de almacenamiento para cada nodo de almacenamiento

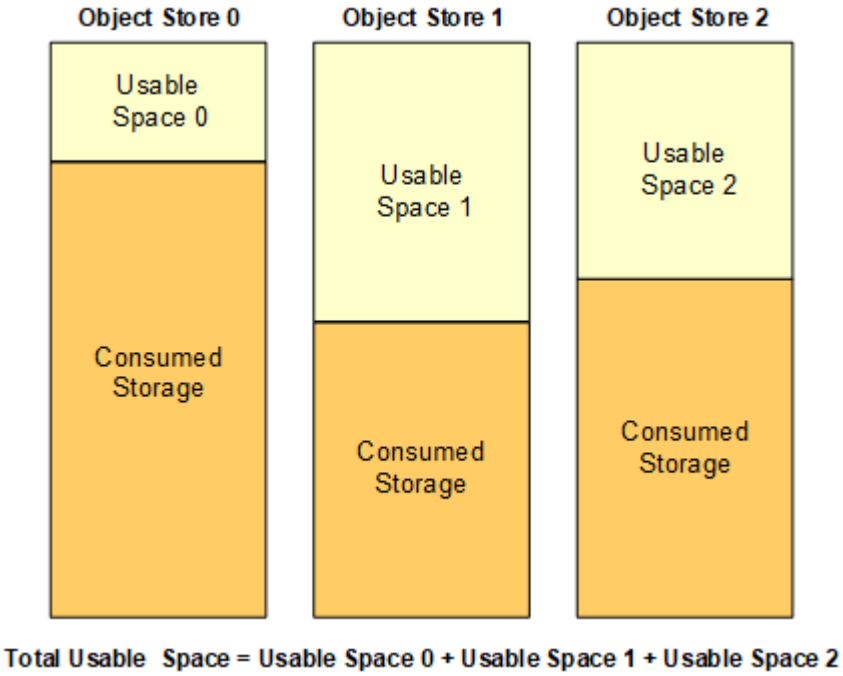
Supervise el espacio utilizable total de cada nodo de almacenamiento para garantizar que el nodo tenga suficiente espacio para los datos de objetos nuevos.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

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

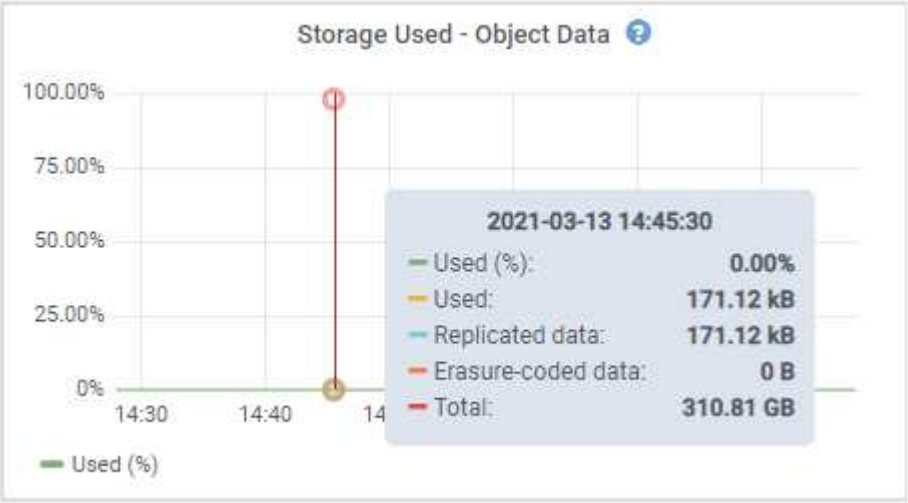
1. Seleccione **NODES** > ***Storage Node*** > **Storage**.

   Aparecen los gráficos y las tablas del nodo.

2. Pase el cursor sobre el gráfico Storage used - object data.

   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.

Si quiere más información sobre la planificación de una expansión del almacenamiento, consulte

Instrucciones para ampliar StorageGRID.

La **Almacenamiento de datos 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.

Acerca de esta tarea

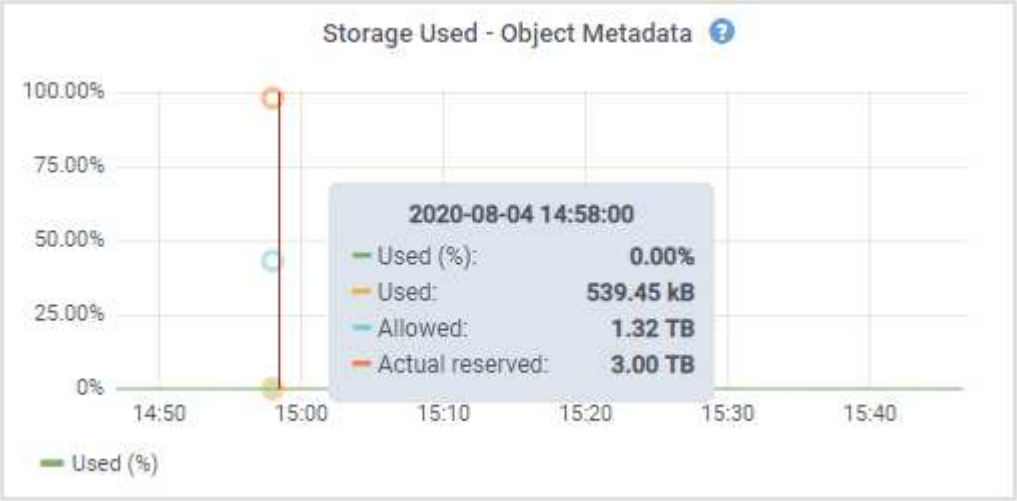
StorageGRID mantiene tres copias de metadatos de objetos en cada sitio para proporcionar redundancia y proteger los metadatos de objetos de la pérdida. Las tres copias se distribuyen uniformemente por todos los nodos de almacenamiento de cada sitio, utilizando el espacio reservado para los metadatos 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. Pase el cursor sobre el gráfico almacenamiento usado - metadatos de objetos para ver los valores de un momento específico.



Valor	Descripción	Métrica Prometheus
Utilizado (%)	El porcentaje de espacio de metadatos permitido que se utilizó en este nodo de almacenamiento.	`storagegrid_storage_utilization_metadata_bytes/ storagegrid_storage_utilization_metadata_allowed_bytes`
Utilizado	Los bytes del espacio de metadatos permitido que se usaron en este nodo de almacenamiento.	`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 Instrucciones para administrar StorageGRID.	`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 Instrucciones para administrar StorageGRID.	*Metric se añadirá en una versión futura.*

Los valores totales de un sitio o de la cuadrícula no incluyen los nodos sin especificar 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.

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 comprender si el grid puede gestionar la carga actual o si se necesitan más recursos.

Lo que necesitará

Debe iniciar sesión en Grid Manager mediante un navegador web compatible.

Acerca de esta tarea

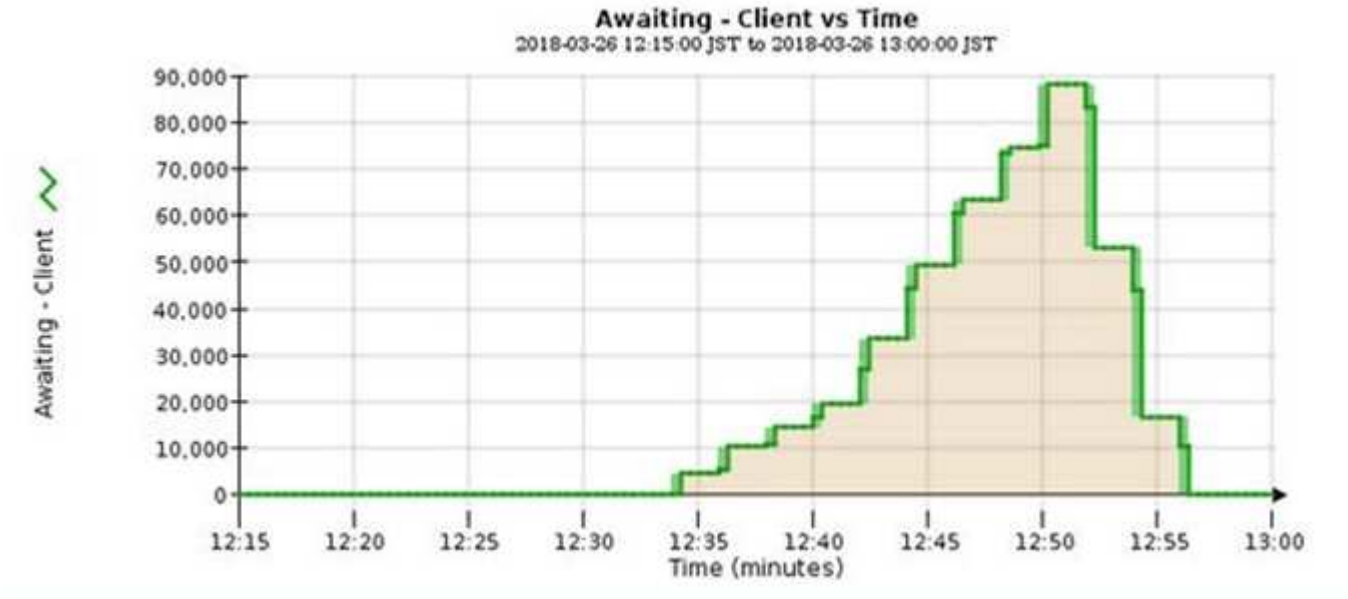
El sistema StorageGRID gestiona los objetos aplicando la política activa de ILM. La política de ILM y las reglas asociadas determinan cuántas copias se realizan, el tipo de copias que se crean, dónde se colocan las copias y el período de tiempo que se conserva cada copia.

El procesamiento de objetos y otras actividades relacionadas con objetos puede superar la velocidad a la que StorageGRID puede evaluar ILM, lo que provoca que el sistema ponga en cola objetos cuyas instrucciones de ubicación de ILM no se puedan completar prácticamente en tiempo real. Puede controlar si StorageGRID está siguiendo las acciones del cliente creando una entrada en el atributo esperando - cliente.

Para crear un gráfico de este atributo:

1. Inicie sesión en Grid Manager.
2. En el panel de control, busque la entrada **esperando - Cliente** en el panel Administración del ciclo de vida de la información (ILM).
3. Haga clic en el icono del gráfico .

El gráfico de ejemplo muestra una situación en la que el número de objetos que esperan la evaluación de ILM aumentó temporalmente de manera insostenible y luego disminuyó finalmente. Esta tendencia indica que el ILM no se cumplió temporalmente casi en tiempo real.



Picos temporales en el gráfico esperando: Se espera que el cliente. Pero si el valor que se muestra en el gráfico sigue aumentando y nunca se reduce, el grid requiere más recursos para funcionar de forma eficiente: Más nodos de almacenamiento o, si la política de ILM coloca objetos en ubicaciones remotas, más ancho de banda de red.

Puede investigar más a fondo las colas de ILM mediante la página **NODES**.

Pasos

1. Seleccione **NODES**.
2. Seleccione ***grid name*** > **ILM**.
3. Pase el cursor sobre el gráfico de la cola de ILM para ver el valor de los siguientes atributos en un momento específico:

- **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 ILM Queue se incluye solo para el grid. Esta información no se muestra en la pestaña ILM para un sitio o nodo de almacenamiento.

- **Período de exploración - 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.

- **Intento de reparación**: El número total de operaciones de reparación de objetos para los datos replicados que se han intentado realizar. 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 intentadas ha dejado de aumentar y se ha completado un análisis completo, es probable que la reparación haya finalizado.

Supervisar las conexiones de red y el rendimiento

Los nodos de red deben poder comunicarse entre sí para permitir que la red funcione. La integridad de la red entre los nodos y los sitios, y el ancho de banda de la red entre los sitios, son fundamentales para lograr operaciones eficientes.

Lo que necesitará

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

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 dar lugar a fallos de procesamiento (cuando se selecciona la opción de ingesta estricta para las reglas de ILM), o simplemente a un rendimiento de procesamiento deficiente y retrasos de ILM.

Puede utilizar Grid Manager para supervisar la conectividad y el rendimiento de la red, de forma que pueda

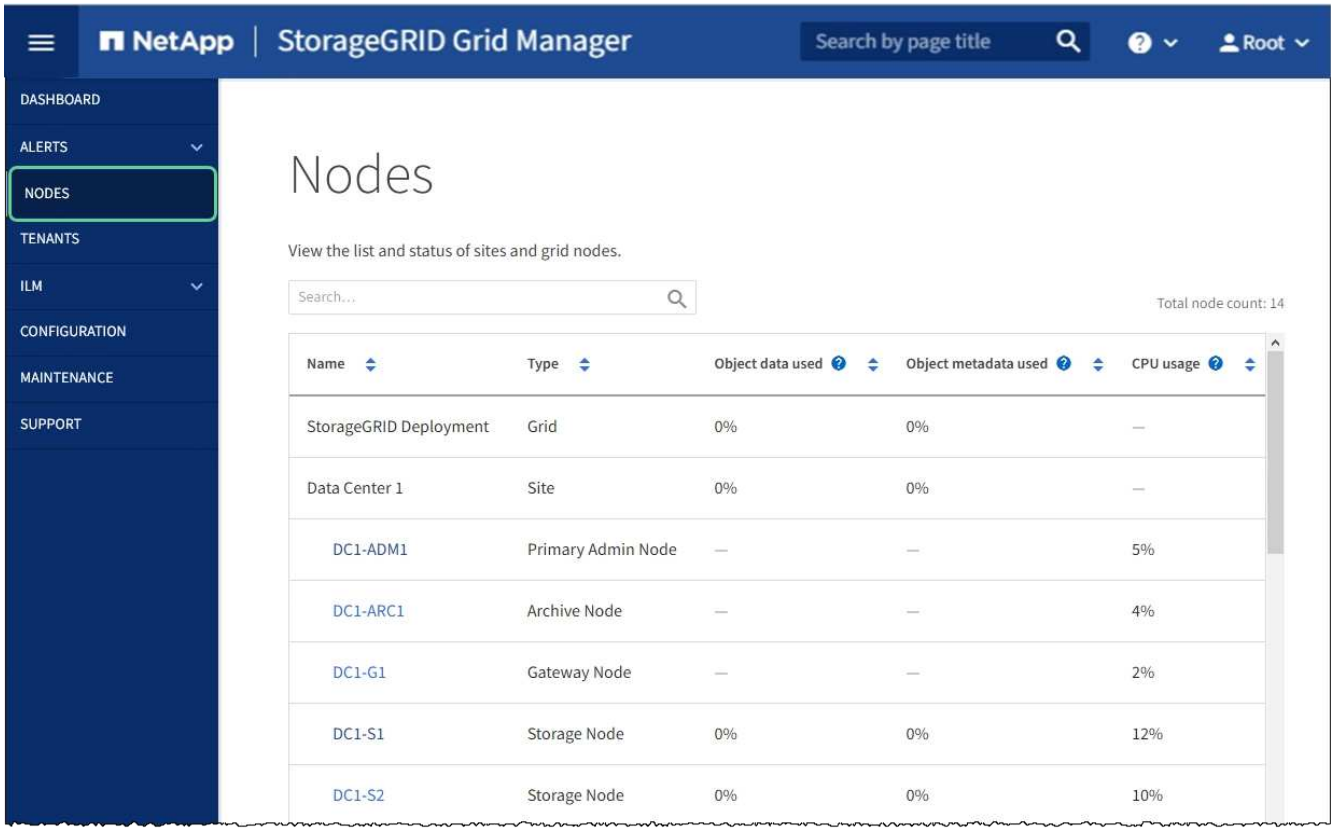
resolver cualquier problema con la mayor brevedad posible.

Además, considere la posibilidad de crear políticas de clasificación del tráfico de red para proporcionar supervisión y limitación del tráfico relacionado con inquilinos, bloques, subredes o extremos de equilibrador de carga específicos. Consulte Instrucciones para administrar StorageGRID.

Pasos

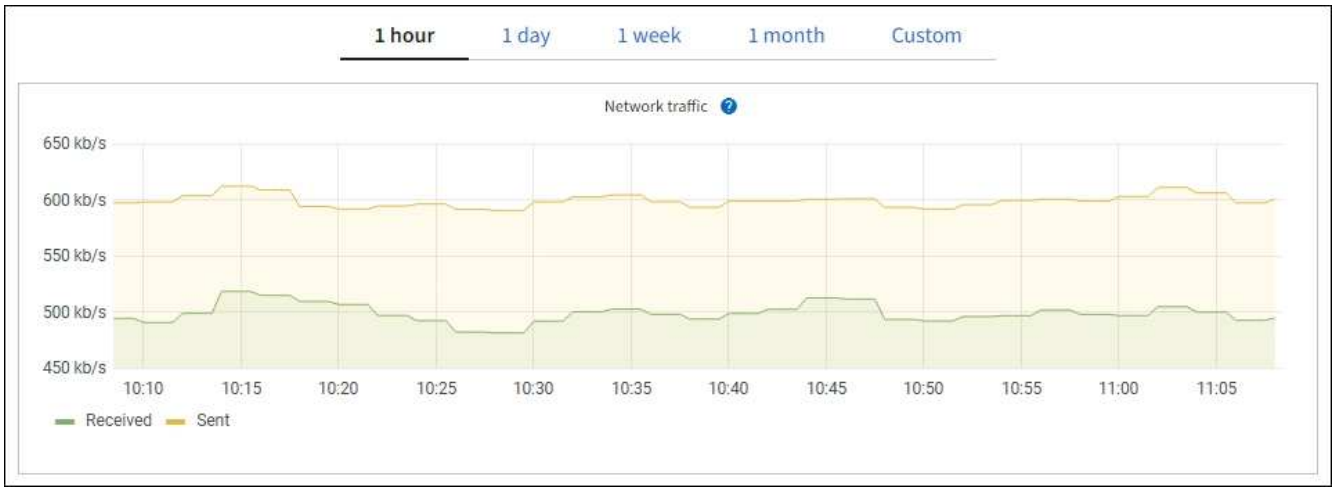
1. Seleccione **NODES**.

   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.

Network interfaces

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

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

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

Network communication

Receive

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

Transmit

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

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

a. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.

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

tabla.

Traffic Classification Policies

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

+ Create | Edit | Remove | Metrics

	Name	Description	ID
○	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
◉	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

b. 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**.

c. 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 directiva de clasificación del tráfico según sea necesario.

Para crear, editar o eliminar directivas de clasificación de tráfico, consulte Instrucciones para administrar StorageGRID.

Información relacionada

Abra la pestaña Network

Supervise los estados de conexión de los nodos

Supervise los recursos a nivel de nodo

Se deben supervisar los nodos de grid individuales para comprobar sus niveles de utilización de recursos.

Lo que necesitará

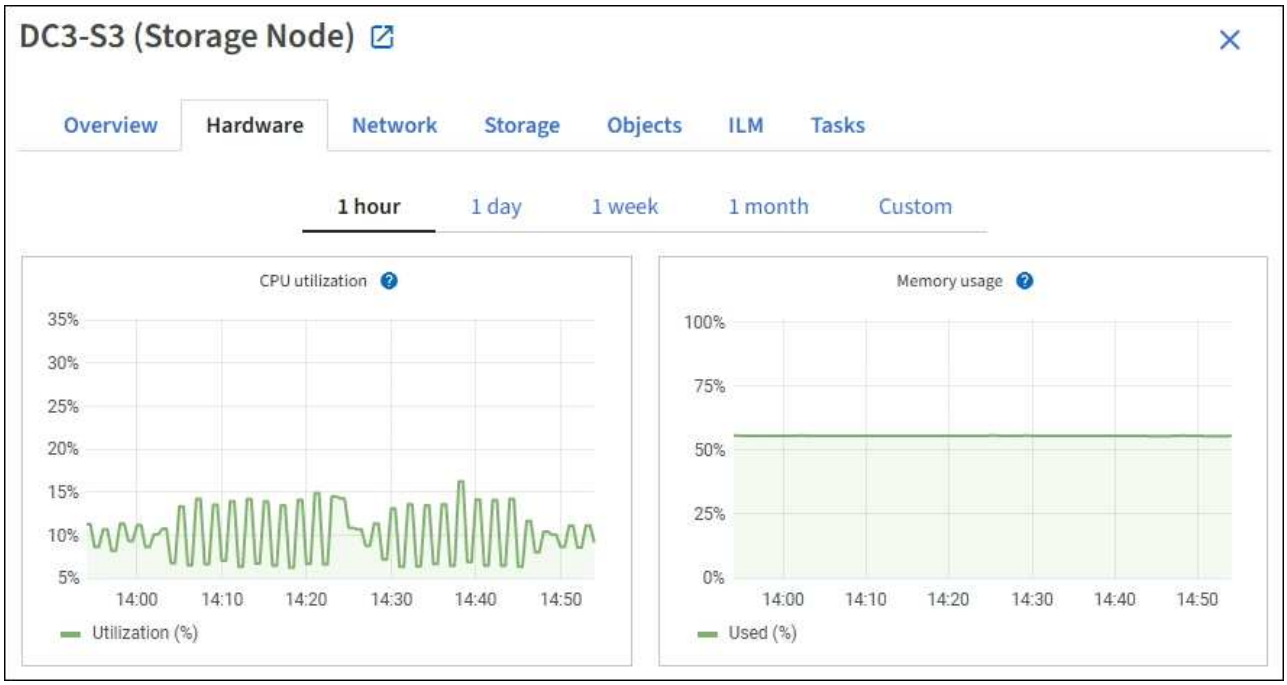
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.

Acerca de esta tarea

Si los nodos están sobrecargados de forma continua, es posible que se necesiten más nodos para realizar operaciones eficientes.

Pasos

1. Para ver información sobre el uso de hardware de un nodo de grid:
   a. En la página **NODES**, seleccione el nodo.
   b. Seleccione la ficha **hardware** para visualizar gráficos de utilización de CPU y uso de memoria.



c. 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.

d. 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 tengan cualquier 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 del cliente está asociada a una cuenta de inquilino. Puede usar el administrador de grid para supervisar el uso del almacenamiento de un cliente o el tráfico de red, o bien puede usar el registro de auditorías o los paneles de Grafana para recopilar información más detallada sobre cómo están usando StorageGRID los clientes.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz o Administrador.

Acerca de esta tarea

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.

Pasos

1. Seleccione **ARRENDATARIOS** para revisar la cantidad de almacenamiento que utilizan todos los inquilinos.

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 (—).

Puede iniciar sesión en una cuenta de inquilino seleccionando el vínculo de inicio de sesión En la columna **Iniciar sesión/Copiar URL** de la tabla.

Puede copiar la dirección URL de la página de inicio de sesión de un inquilino seleccionando el vínculo Copiar URL En la columna **Iniciar sesión/Copiar URL** de la tabla.

2. Opcionalmente, seleccione **Exportar a CSV** para ver y exportar un archivo .csv que contenga los valores de uso para todos los arrendatarios.

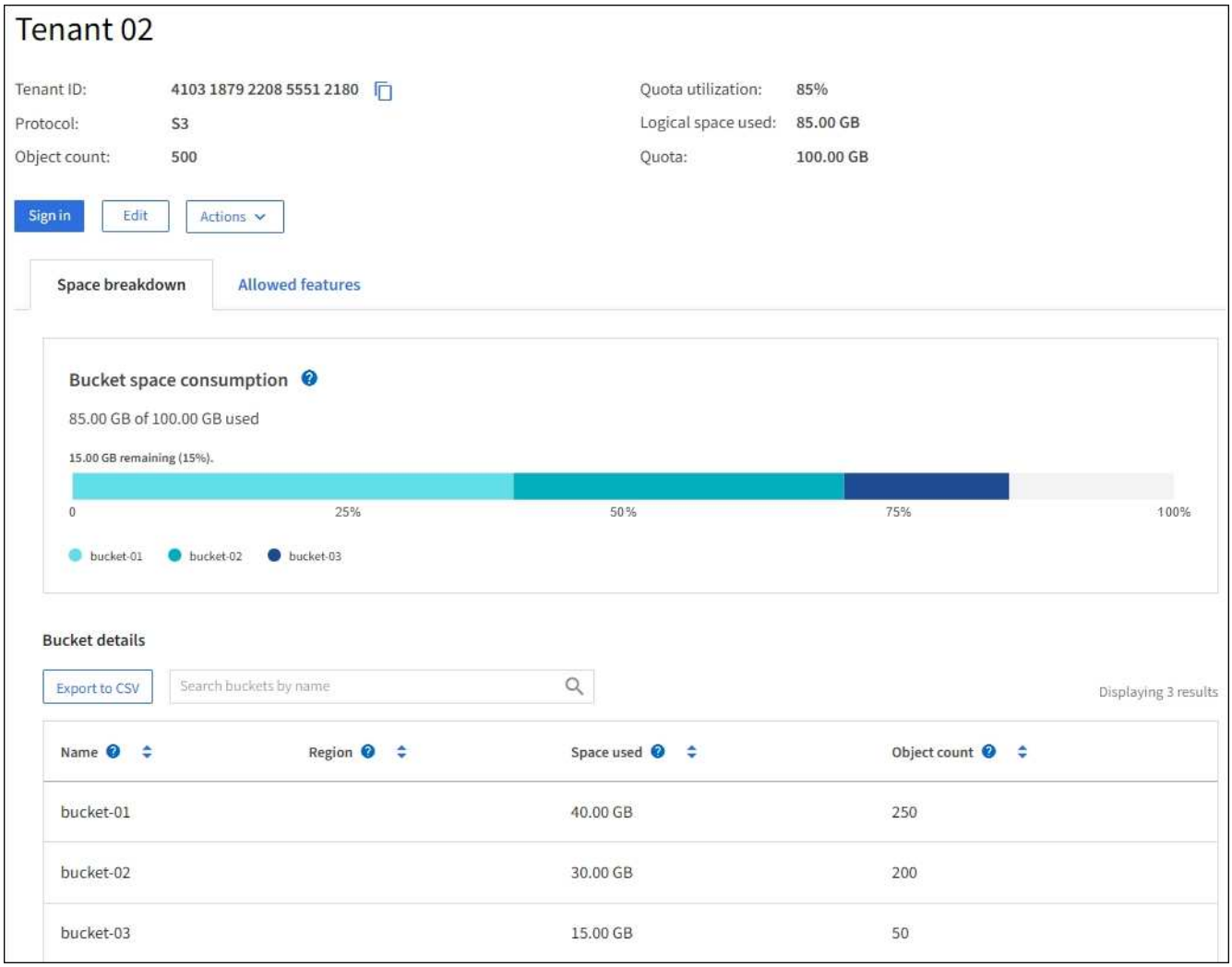
   Se le solicitará que abra o guarde el `.csv` archivo.

   El contenido de un archivo .csv tiene el 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 archivo .csv en una aplicación de hoja de cálculo o utilizarlo en automatización.

3. Para ver los detalles de un arrendatario específico, incluidos los gráficos de uso, seleccione el nombre de cuenta de arrendatario en la página arrendatarios.



- **Descripción general del inquilino**

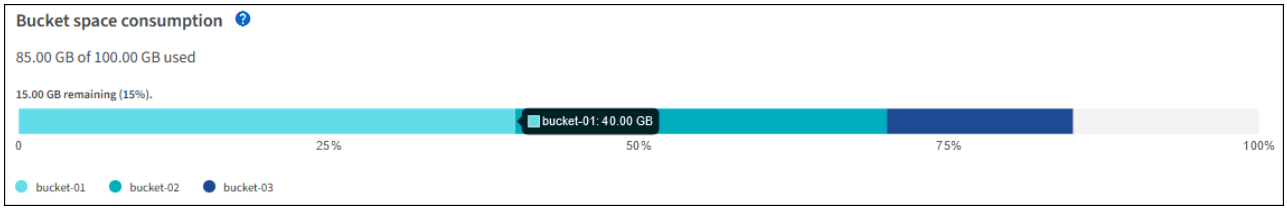
  El área de descripción general del inquilino contiene valores para el recuento de objetos, la utilización de cuotas, el espacio lógico utilizado y la configuración de cuota.

- **Desglose del espacio — consumo de espacio**

  La pestaña Space Breakdown incluye valores para el consumo total de espacio en bloques (S3) o contenedores (Swift), así como el espacio usado y el recuento de objetos para cada bloque o contenedor.

  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 activar la alerta * uso de cuota de inquilino alto* para determinar si los inquilinos están consumiendo sus cuotas. Si está habilitada, esta alerta se activa cuando un inquilino ha utilizado el 90% de su cuota. Para obtener más información, consulte la referencia de alertas.

- **Desglose del espacio — Detalles del cucharón o del contenedor**

  La tabla **Detalles del cucharón** (S3) o **Detalles del contenedor** (Swift) enumera los cubos o contenedores para el arrendatario. El espacio usado es la cantidad total de datos de objetos en el bloque o contenedor. Este valor no representa el espacio de almacenamiento necesario para las copias de ILM y los metadatos de objetos.

4. 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 del archivo .csv de un inquilino S3 tiene el 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 archivo .csv en una aplicación de hoja de cálculo o utilizarlo en automatización.

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

   a. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.

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

Traffic Classification Policies

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

+ Create | Edit | Remove | Metrics

	Name	Description	ID
○	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
◉	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

a. Revise la lista de políticas para identificar las que se aplican a un arrendatario específico.
b. Para ver las métricas asociadas a una directiva, seleccione el botón de opción situado a la izquierda de la directiva y, a continuación, haga clic en **métricas**.
c. Analice los gráficos para determinar con qué frecuencia la política limita el tráfico y si necesita ajustar la política.

   Para crear, editar o eliminar directivas de clasificación del tráfico, consulte las instrucciones para administrar StorageGRID.

6. De manera opcional, use 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 las instrucciones para comprender los mensajes de auditoría para obtener más información.

7. De manera opcional, utilice las métricas de Prometheus para generar informes sobre la actividad de inquilinos:
   - 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, seleccione el icono de ayuda y seleccione **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.

Información relacionada

Referencia de alertas

Revisar los registros de auditoría

Administre StorageGRID

Revisar las métricas de soporte

Supervise la capacidad de archivado

El sistema StorageGRID no permite supervisar directamente la capacidad de un sistema de almacenamiento de archivado externo. 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.

Lo que necesitará

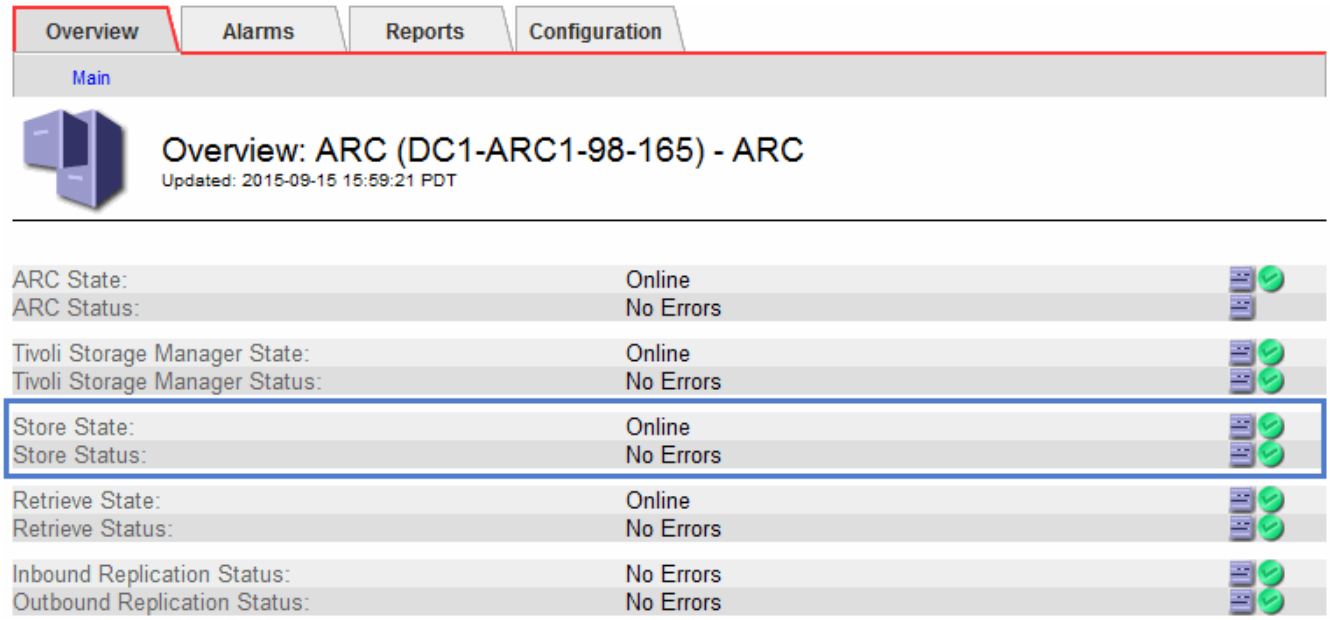
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener permisos de acceso específicos.

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.

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.

Lo que necesitará

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

Acerca de esta tarea

Puede utilizar el servicio Load Balancer en nodos de administración o de puerta de enlace, un equilibrador de carga de terceros externo o el servicio CLB en nodos de Gateway para distribuir solicitudes de cliente en varios nodos de almacenamiento.

> El servicio CLB está obsoleto.

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.

Consulte la sección sobre la configuración de conexiones de cliente en las instrucciones para administrar StorageGRID.

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. Seleccione **NODES**.
   b. Seleccione un nodo de puerta de enlace o un nodo de administrador.
   c. En la ficha **Descripción general**, compruebe si una interfaz de nodo está en un grupo ha y si la interfaz de nodo tiene la función Master.

      Los nodos con la función de nodo maestro y los nodos que no están en un grupo de alta disponibilidad deben distribuir activamente las solicitudes a los clientes.

   d. Para cada nodo que deba distribuir activamente solicitudes de cliente, seleccione la pestaña **Load Balancer**.
   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 del cliente.

   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. De manera opcional, utilice las políticas de clasificación de tráfico para ver un desglose más detallado del tráfico que presta el servicio Load Balancer.

2. Si los clientes S3 o Swift se conectan mediante el servicio CLB (obsoleto), realice las siguientes comprobaciones:

   a. Seleccione **NODES**.

   b. Seleccione un nodo de puerta de enlace.

   c. En la ficha **Descripción general**, compruebe si una interfaz de nodo está en un grupo ha y si la interfaz de nodo tiene la función de Master.

      Los nodos con la función de nodo maestro y los nodos que no están en un grupo de alta disponibilidad deben distribuir activamente las solicitudes a los clientes.

   d. Para cada nodo de puerta de enlace que debería distribuir activamente solicitudes de cliente, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.

   e. Seleccione ***Gateway Node*** > **CLB** > **HTTP** > **Descripción general** > **Principal**.

   f. Revise el número de **sesiones entrantes - establecidas** para comprobar que el nodo de puerta de enlace ha estado gestionando las solicitudes de forma activa.

3. 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.

Información relacionada

Administre StorageGRID

Vea la pestaña Load Balancer

Aplique correcciones urgentes o actualice el software si es necesario

Si hay una revisión o una nueva versión del software StorageGRID disponible, debe evaluar si la actualización es apropiada para su sistema e instalarla si es necesario.

Acerca de esta tarea

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.

Pasos

1. Vaya a la página de descargas de NetApp para StorageGRID.

   "Descargas de NetApp: StorageGRID"

2. Seleccione la flecha hacia abajo para el campo **Tipo/Seleccionar versión** para ver una lista de las actualizaciones disponibles para descargar:

- **Versiones de software de StorageGRID**: 11.*x.y*
- * StorageGRID hotfix*: 11.*x. y.z*

3. Revise los cambios que se incluyen en la actualización:
   a. Seleccione la versión en el menú desplegable y haga clic en **Ir**.
   b. Inicie sesión con el nombre de usuario y la contraseña de su cuenta de NetApp.
   c. Lea el contrato de licencia para usuario final, seleccione la casilla de verificación y, a continuación, seleccione **Aceptar y continuar**.

      Aparece la página de descargas de la versión seleccionada.

4. Obtenga información acerca de los cambios incluidos en la versión de software o la revisión.
   - Para obtener una nueva versión de software, consulte el tema «¿Qué hay de nuevo?» en las instrucciones para actualizar StorageGRID.
   - Para una revisión, descargue el archivo README para obtener un resumen de los cambios incluidos en la revisión.
5. Si decide que se requiere una actualización de software, busque las instrucciones antes de continuar.
   - Para una versión de software nueva, siga cuidadosamente las instrucciones para actualizar StorageGRID.
   - Para una revisión, busque el procedimiento de revisión en las instrucciones de recuperación y mantenimiento

Información relacionada

Actualizar el software de

Recuperación y mantenimiento

Gestionar 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 Grid Manager y aumenta el recuento de alertas actuales.
- 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 ni para las gravedades de alarma).

Comparar alertas y alarmas

Existen 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** del 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)

	Alertas	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 alertas 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)
¿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 Administrar alertas para gestionar las silencios, notificaciones de alerta y reglas de alerta. Administre StorageGRID	• Cualquier persona que pueda iniciar sesión en Grid Manager puede ver las alarmas heredadas. • Debe tener el permiso Confirmar alarmas para confirmar alarmas. • Debe tener tanto los permisos de configuración de página de topología de cuadrícula como de configuración de cuadrícula para gestionar las alarmas globales y las notificaciones por correo electrónico. Administre StorageGRID

	Alertas	Alarmas (sistema heredado)
¿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	Seleccione **CONFIGURACIÓN** > **Supervisión** > **Agente SNMP**. Usar supervisión de SNMP **Nota**: Las notificaciones SNMP no se envían para cada alarma o gravedad de alarma. Alarmas que generan notificaciones SNMP (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 solo nodo Admin (el "'emisor preferido'"). Administre StorageGRID	Un solo nodo Admin (el "'emisor preferido'"). Administre StorageGRID

	Alertas	Alarmas (sistema heredado)
¿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)
¿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	1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de pantalla**. 2. Active la casilla de verificación **Suprimir notificación todo**. **Nota**: La supresión de todo el sistema de notificaciones por correo electrónico también suprime los mensajes de correo electrónico AutoSupport activados por eventos. Gestionar alarmas (sistema heredado)
¿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)

	Alertas	Alarmas (sistema heredado)
¿Cómo puedo desactivar una alerta o alarma individual?	1. Seleccione **ALERTS** > **Reglas**. 2. Seleccione la regla y seleccione **Editar regla**. 3. Deseleccione la casilla de verificación **Activado**. Deshabilitar reglas de alerta	1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Global Alarms**. 2. Seleccione la regla y seleccione el icono Editar. 3. Deseleccione la casilla de verificación **Activado**. Gestionar alarmas (sistema heredado)

Gestionar alertas

Gestionar alertas: descripción general

Las alertas le permiten supervisar diversos eventos y condiciones dentro de su sistema StorageGRID. Puede gestionar alertas creando alertas personalizadas, editando o deshabilitando las alertas predeterminadas, configurando notificaciones por correo electrónico para alertas y silenciando las notificaciones de alertas.

Acerca de las alertas de StorageGRID

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.

- El sistema de alertas se centra en los problemas que pueden llevar a la práctica en el sistema. Se activan alertas para eventos que requieren su atención inmediata, no para eventos que se pueden ignorar de forma segura.
- La página Alertas actuales proporciona una interfaz sencilla para ver los problemas actuales. Puede ordenar el listado por alertas individuales y grupos de alertas. Por ejemplo, podría ordenar todas las alertas por nodo/sitio para ver qué alertas afectan a un nodo concreto. O bien, se pueden ordenar las alertas de un grupo por tiempo activadas para encontrar la instancia más reciente de una alerta específica.
- La página Resolved Alerts proporciona información similar a la de la página Current Alerts, pero permite buscar y ver un historial de las alertas que se han resuelto, incluida la hora en la que se activó la alerta y la fecha en que se resolvió.
- Se agrupan varias alertas del mismo tipo en un correo electrónico para reducir el número de notificaciones. Además, en la página Alertas se muestran varias alertas del mismo tipo como un grupo. Puede expandir y contraer grupos de alertas para mostrar u ocultar las alertas individuales. Por ejemplo, si varios nodos notifican la alerta **no se puede comunicar con el nodo** aproximadamente a la vez, sólo se envía un correo electrónico y la alerta se muestra como un grupo en la página Alertas.
- Las alertas utilizan nombres y descripciones intuitivos que le ayudan a entender rápidamente el problema. Las notificaciones de alerta incluyen detalles sobre el nodo y el sitio afectado, la gravedad de alerta, la hora en la que se activó la regla de alerta y el valor actual de las métricas relacionadas con la alerta.
- Las notificaciones por correo electrónico de alertas y los listados de alertas de las páginas actuales de Alertas y Alertas resueltas ofrecen acciones recomendadas para resolver una alerta. Estas acciones recomendadas suelen incluir enlaces directos al centro de documentación de StorageGRID para facilitar la búsqueda y el acceso a procedimientos más detallados para la solución de problemas.

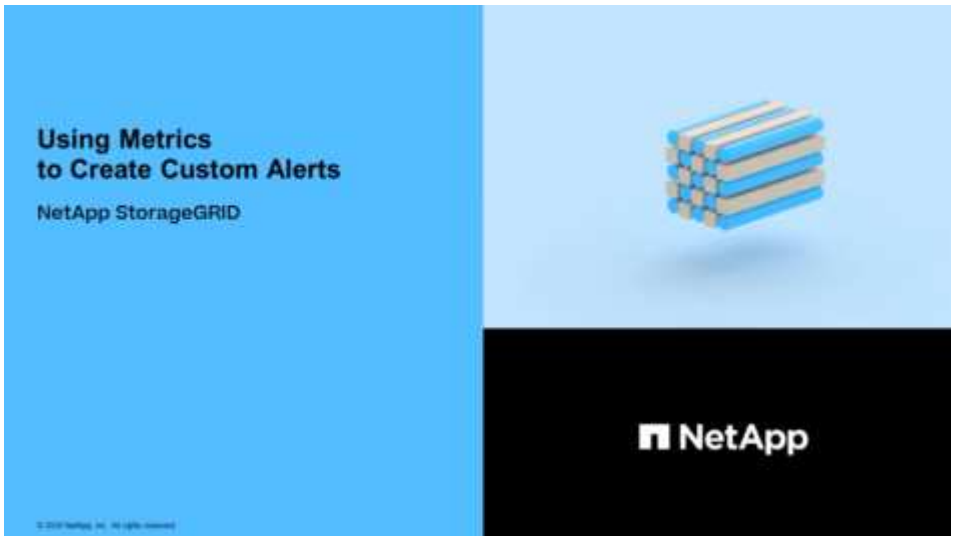
- Si necesita suprimir temporalmente las notificaciones de una alerta en uno o más niveles de gravedad, puede silenciar fácilmente una regla de alerta específica durante una duración especificada y para todo el grid, un solo sitio o un solo nodo. También puede silenciar todas las reglas de alerta, por ejemplo, durante un procedimiento de mantenimiento planificado, como una actualización de software.
- Puede editar las reglas de alerta predeterminadas si es necesario. Puede deshabilitar una regla de alerta por completo o cambiar sus condiciones de activación y duración.
- Puede crear reglas de alerta personalizadas para tener en cuenta las condiciones específicas que son relevantes para su situación y para proporcionar sus propias acciones recomendadas. Para definir las condiciones de una alerta personalizada, debe crear expresiones mediante las métricas Prometheus disponibles en la sección Metrics de la API de gestión de grid.

Leer más

Para obtener más información, consulte estos vídeos:

- "Vídeo: Descripción general de las alertas"

- "Vídeo: Uso de métricas para crear alertas personalizadas"



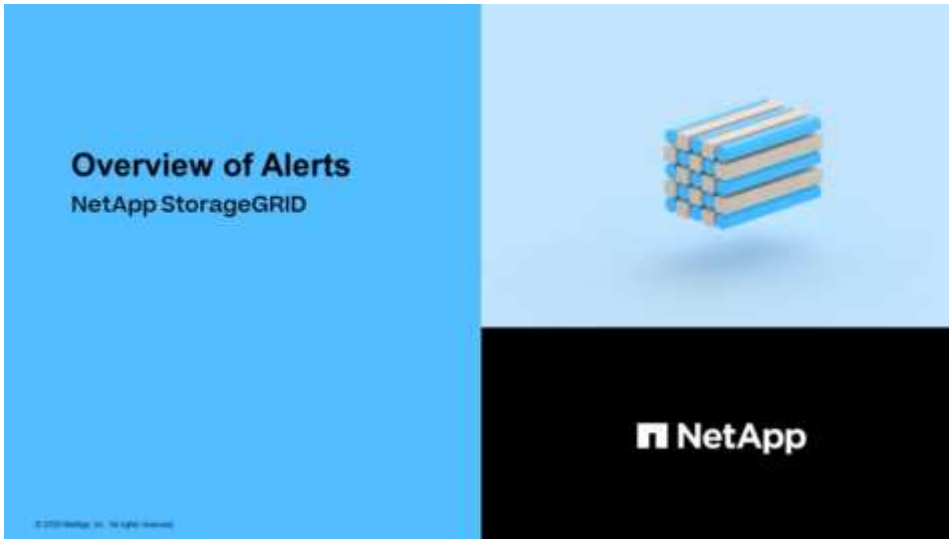
Ver reglas de alerta

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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso Administrar alertas o acceso raíz.
- Opcionalmente, ha visto el vídeo: "Vídeo: Descripción general de las alertas"



Pasos

1. Seleccione **ALERTS** > **Reglas**.

   Aparecerá la página Reglas de alerta.

Alert Rules Learn more

Alert rules define which conditions trigger specific alerts.

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

+ Create custom rule Edit rule Remove custom rule

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

Displaying 62 alert rules.

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

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

Encabezado de columna	Descripción
Condiciones	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. Deberá supervisar y resolver las alertas menores que no se despicen por sí mismas para asegurarse de que no provoquen 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 se 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. Las condiciones para las reglas de alerta desactivadas no se evalúan, por lo que no se activan alertas.

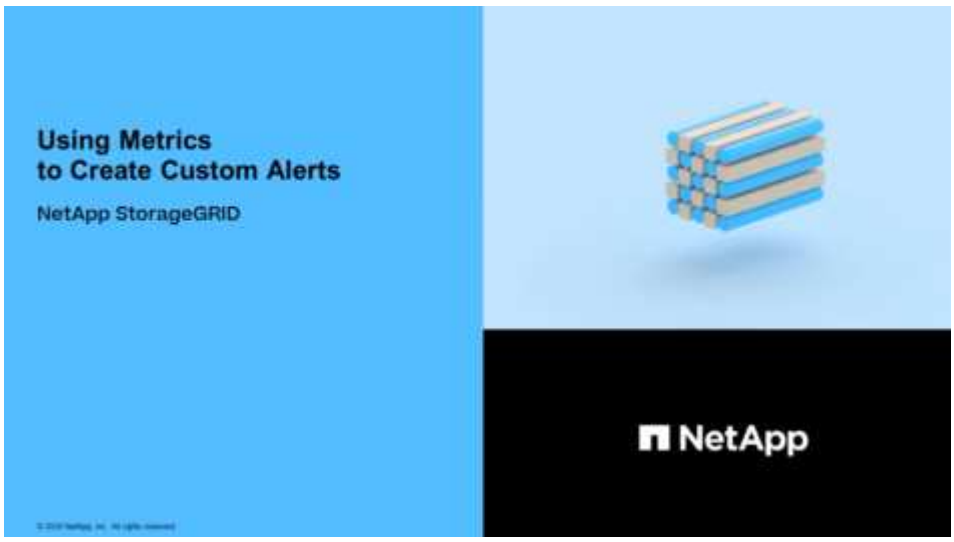
Crear reglas de alerta personalizadas

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

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible
- Tiene el permiso Administrar alertas o 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: Uso de métricas para crear alertas personalizadas"



Acerca de esta tarea

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

- Observe las condiciones de las reglas de alerta predeterminadas y utilícela como ejemplos para sus reglas de alerta personalizadas.
- Si define más de una condición para una regla de alerta, utilice la misma expresión para todas las condiciones. A continuación, cambie el valor del umbral para cada condición.
- Compruebe con cuidado cada condición en busca de errores tipográficos y lógicos.
- Utilice sólo las métricas enumeradas en la API de gestión de grid.
- Cuando pruebe una expresión utilizando la API de gestión de grid, tenga en cuenta que una respuesta «correcta» podría ser simplemente 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 cuando se espera.

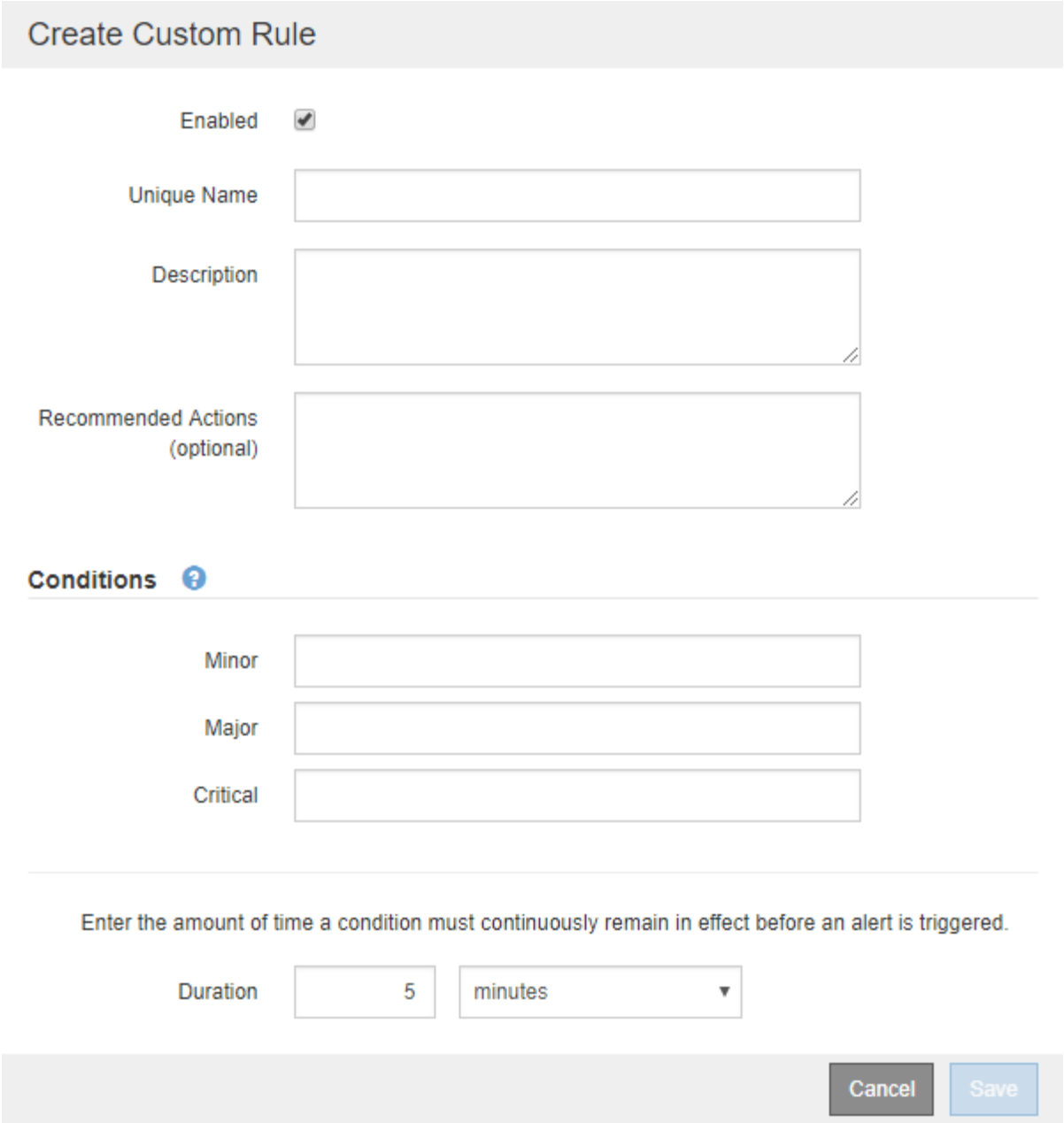
Pasos

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 anule la selección de la casilla de verificación **Activado** para determinar si esta regla de alerta está activada actualmente.

   Si una regla de alerta está deshabilitada, sus expresiones no se evalúan y no se activan alertas.

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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso Administrar alertas o 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.

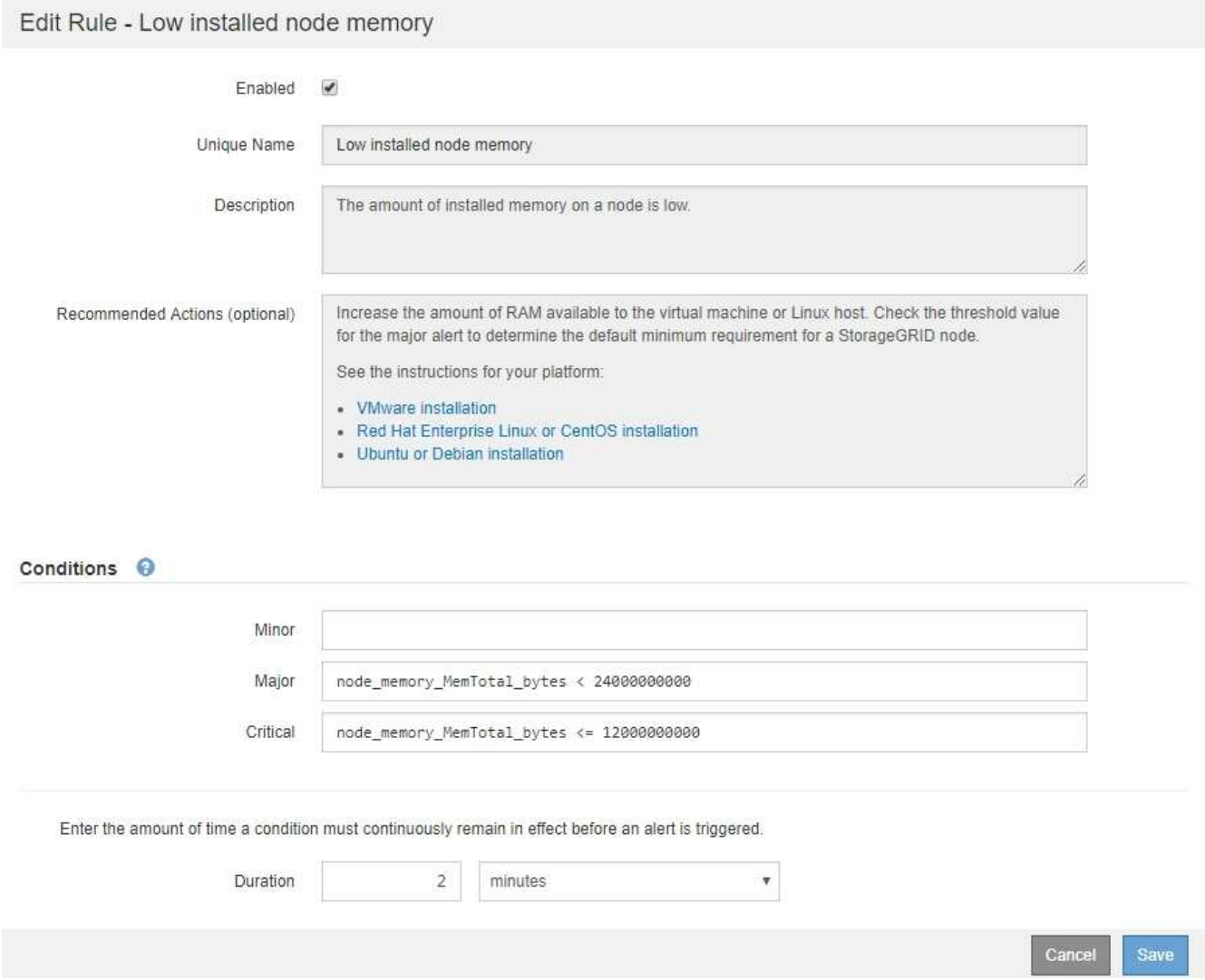
Pasos

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. En este ejemplo se muestra una regla de alerta predeterminada: Los campos Nombre único, Descripción y acciones recomendadas están desactivados y no se pueden editar.



4. Active o anule la selección de la casilla de verificación **Activado** para determinar si esta regla de alerta está activada actualmente.

   Si una regla de alerta está deshabilitada, sus expresiones no se evalúan y no se activan alertas.

   > 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.

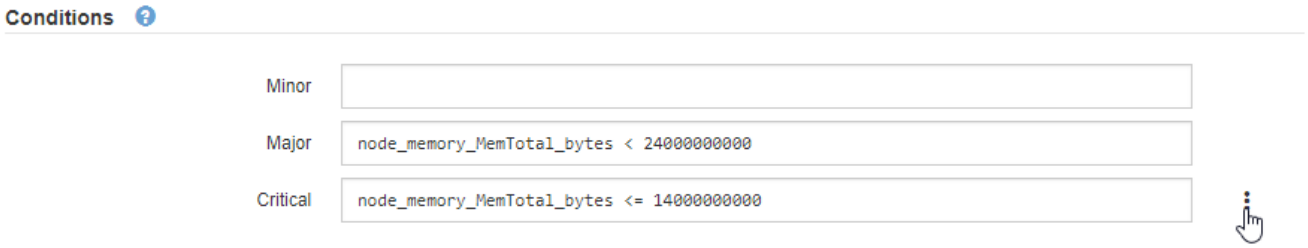
5. En el caso de reglas de alerta personalizadas, actualice la siguiente información según sea necesario.

   > Esta información no se puede editar 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso Administrar alertas o acceso raíz.

Acerca de esta tarea

Cuando una regla de alerta está deshabilitada, sus expresiones no se evalúan y no se activan alertas.

> 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 anule la selección de la casilla de verificación **Activado** para determinar si esta regla de alerta está activada actualmente.

   Si una regla de alerta está deshabilitada, sus expresiones no se evalúan y no se activan alertas.

   > 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso Administrar alertas o 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 se 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:

- Los solapamientos son notificaciones enviadas por el agente SNMP que no requieren confirmación por parte del sistema de administración. 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.

Las notificaciones de alerta se envían mediante el nodo de administrador que esté configurado para que sea el remitente preferido. De manera predeterminada, se selecciona el nodo de administración principal. Consulte Instrucciones para administrar StorageGRID.

> Las notificaciones Trap e inform también se envían cuando determinadas alarmas (sistema heredado) se activan en niveles de gravedad especificados o superiores; sin embargo, las notificaciones SNMP no se envían para cada alarma o para cada gravedad de alarma. Consulte Alarmas que generan notificaciones SNMP (sistema heredado).

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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso Administrar alertas o acceso raíz.

Acerca de esta tarea

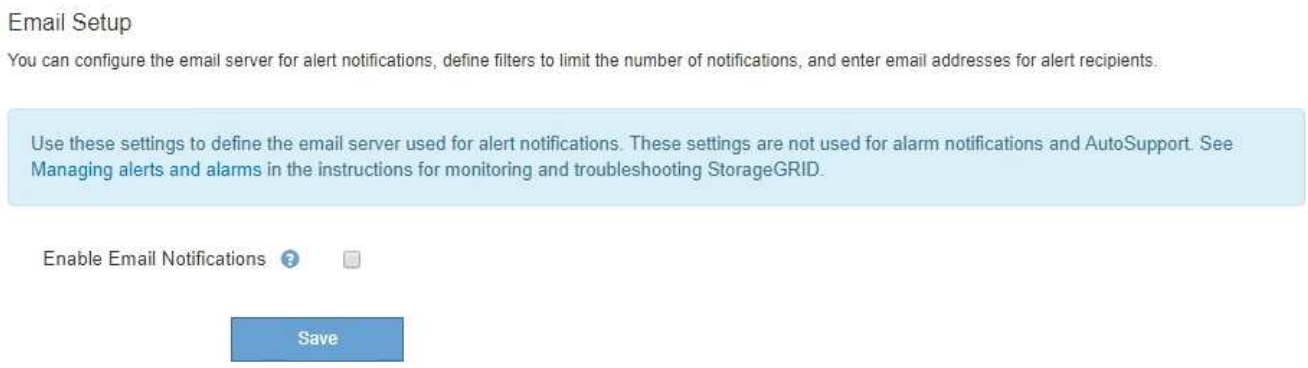
Dado que las alarmas y las alertas son sistemas independientes, la configuración de correo electrónico que se utiliza para las notificaciones de alerta no se utiliza para las notificaciones de alarma ni los mensajes de AutoSupport. Sin embargo, puede utilizar el mismo servidor de correo electrónico para todas las notificaciones.

Si la implementación de StorageGRID incluye varios nodos de administrador, puede seleccionar qué nodo de administrador debe ser el remitente preferido de notificaciones de alerta. También se utiliza el mismo «"remitente preferido» para las notificaciones de alarma y los mensajes de AutoSupport. De manera predeterminada, se selecciona el nodo de administración principal. Para obtener más detalles, consulte Instrucciones para administrar StorageGRID.

Pasos

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

   Aparece la página Configuración de correo electrónico.



2. Active la casilla de verificación **Activar notificaciones por correo electrónico** para indicar que desea

enviar correos electrónicos de notificación cuando las alertas alcancen 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. Active la casilla de verificación **Enviar certificado de cliente** si el 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.

Transport Layer Security (TLS)

Require TLS ☑

CA Certificate

```
-----BEGIN CERTIFICATE-----
1234567890abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
-----END CERTIFICATE-----
```

Browse

Send Client Certificate ☑

Client Certificate

```
-----BEGIN CERTIFICATE-----
1234567890abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
-----END CERTIFICATE-----
```

Browse

Private Key

```
-----BEGIN PRIVATE KEY-----
1234567890abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
-----BEGIN PRIVATE KEY-----
```

Browse

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. Las notificaciones no se envían 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 importantes.

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 contrasta con la prueba de notificaciones de alarma y mensajes de AutoSupport, donde todos los nodos del administrador envían el correo electrónico de prueba.

8. Seleccione **Guardar**.

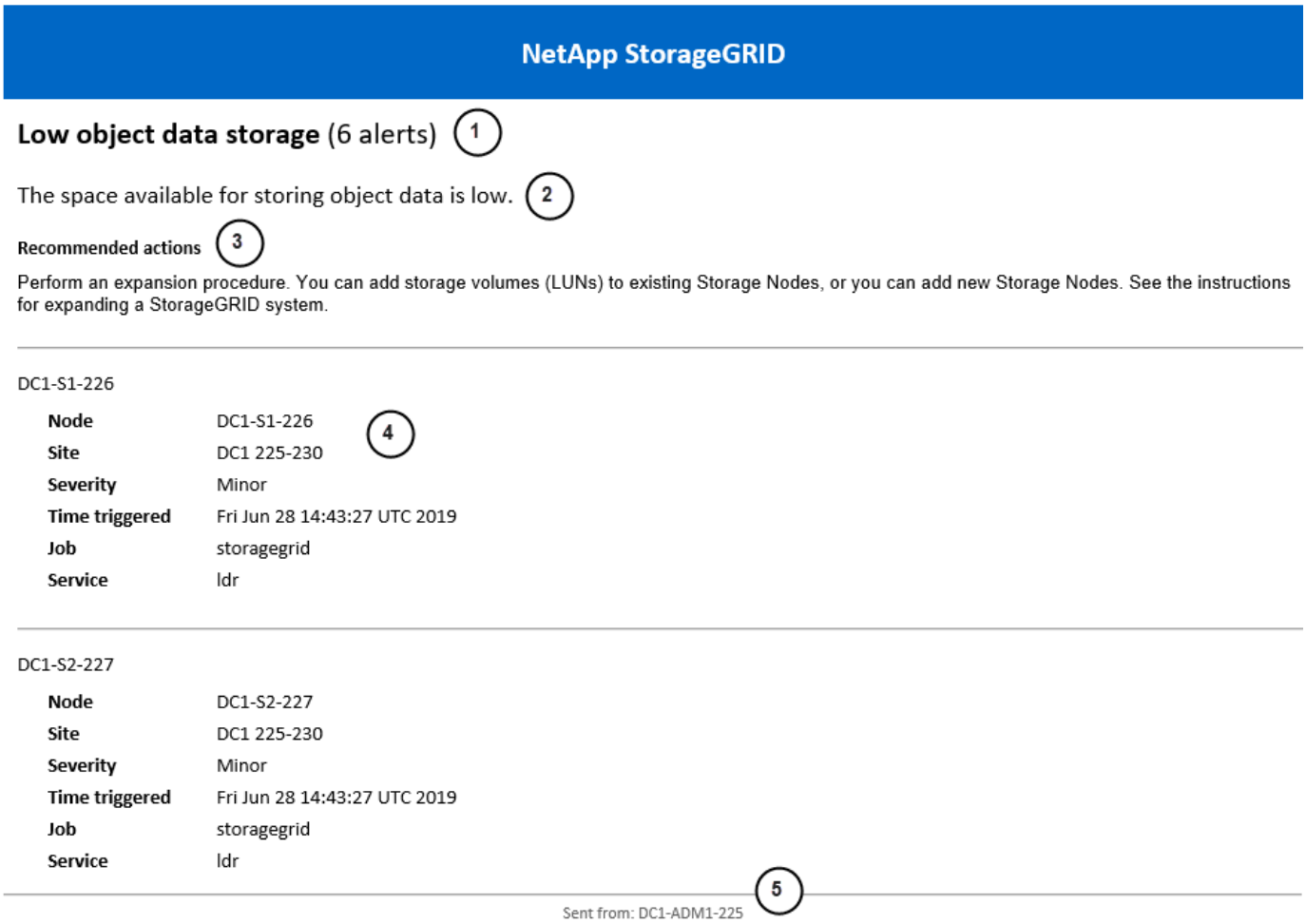
   El envío de un mensaje de correo electrónico de prueba no guarda la configuración. Debe seleccionar **Guardar**.

   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. La alerta A se activa 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso Administrar alertas o 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. Solicite al administrador de correo electrónico que confirme que los correos electrónicos de la dirección del remitente no están 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso Administrar alertas o 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.

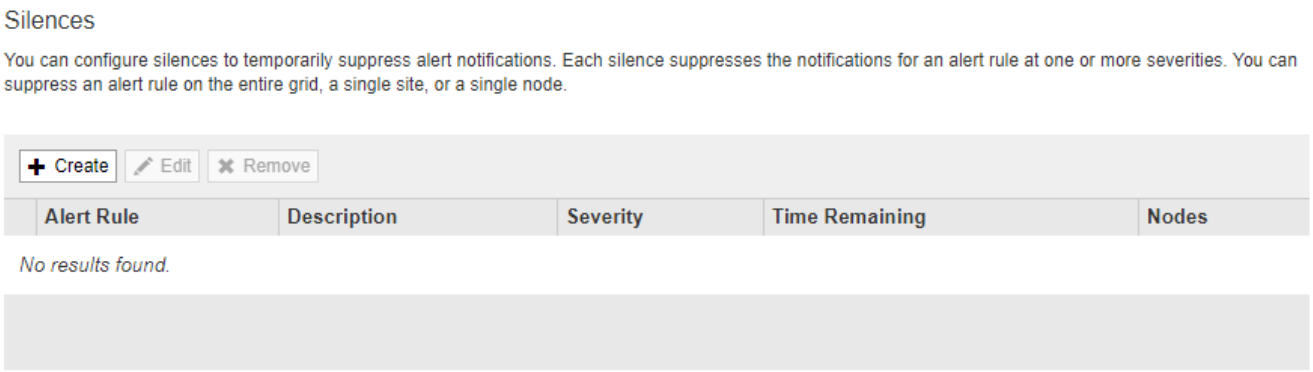
> Tenga cuidado al decidir silenciar una regla de alerta. Si silencia una alerta, es posible que no detecte un problema subyacente hasta que impida que se complete una operación crítica.

> Puesto que las alarmas y alertas son sistemas independientes, no puede utilizar esta función para suprimir las notificaciones de alarma.

Pasos

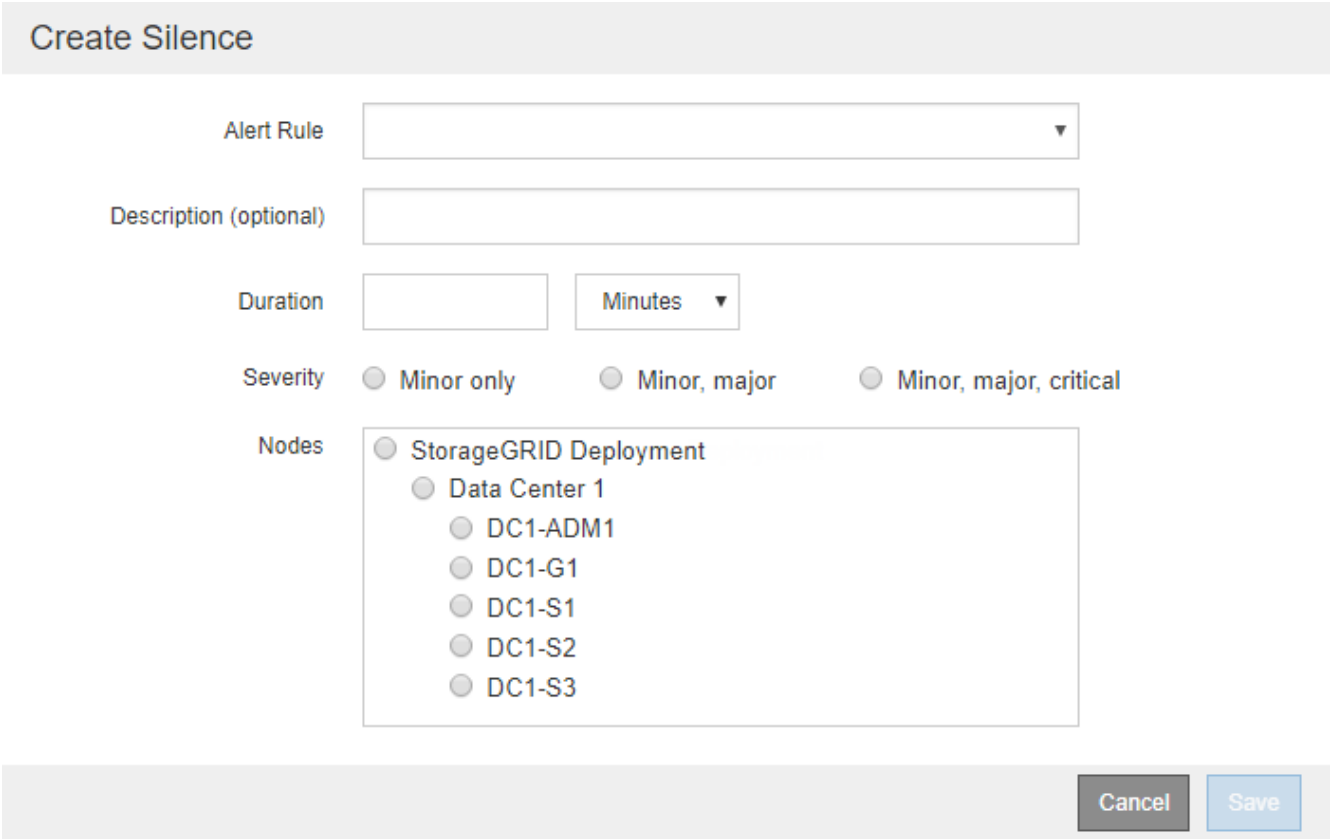
1. Seleccione **ALERTS** > **silencios**.

   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 puede 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

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.

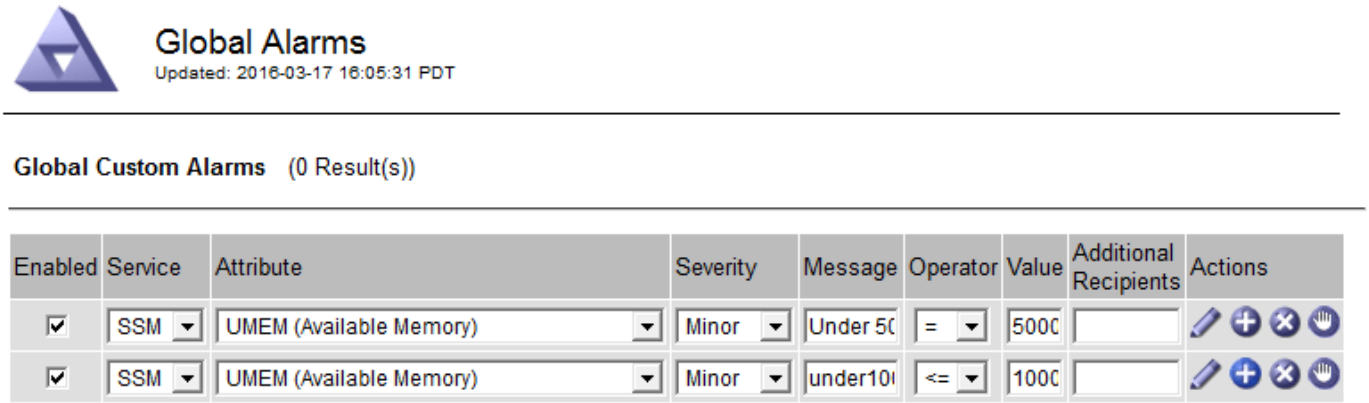
Después de la situación anterior, si la alarma Global Custom está desactivada, no cambia nada. El valor del atributo se debe volver a evaluar antes de que se active un nuevo nivel de alarma.

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.

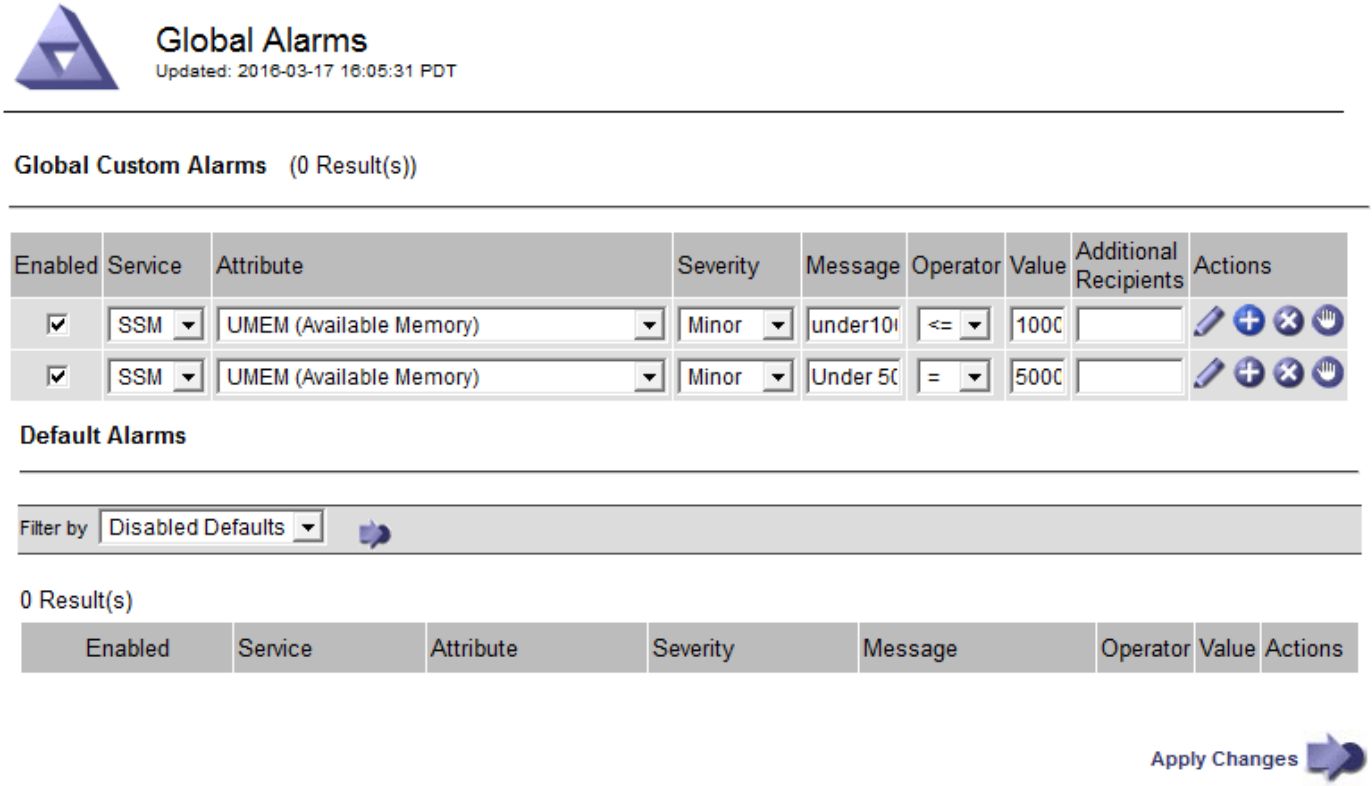
Alarmas de la misma gravedad

Si dos alarmas personalizadas globales para el mismo atributo tienen la misma gravedad, las alarmas se evalúan con una prioridad "'top down'".

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 del VMFI para que no se active la alarma del VMFI de nivel crítico (las dos alarmas críticas actuales aparecerán en la tabla de color verde); Sin embargo, no puede desactivar una única alarma en una fila de tabla de modo que una alarma VMFI se muestre como una alarma de nivel crítico mientras que la otra permanece en 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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener el permiso Confirmar 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. Normalmente, puede ignorar las alarmas (ya que las alertas proporcionan una mejor vista del sistema) o puede reconocer 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**.

The alarm system is the legacy system. The alert system offers significant benefits and is easier to use. See Managing alerts and alarms in the instructions for monitoring and troubleshooting StorageGRID.

Current Alarms

Last Refreshed: 2020-05-27 09:41:39 MDT

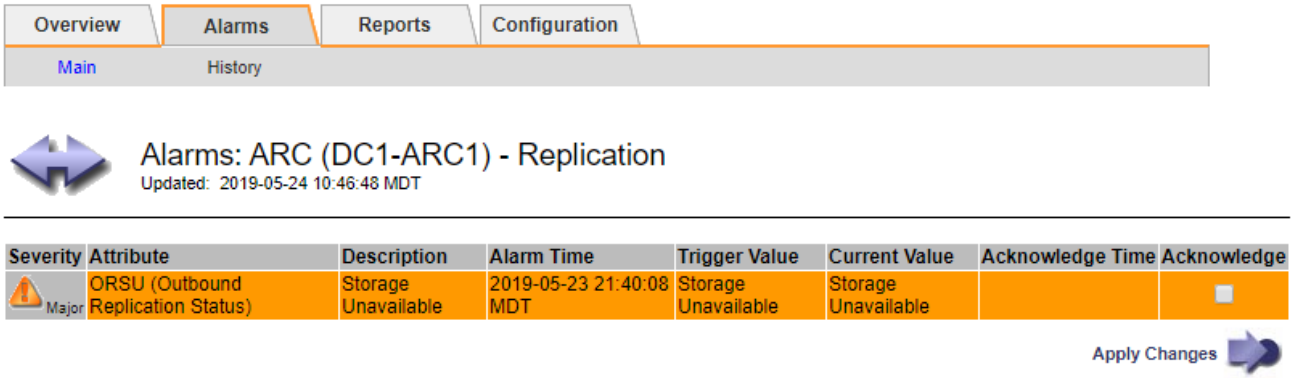
Show Acknowledged Alarms (1 - 1 of 1)

Severity	Attribute	Service	Description	Alarm Time	Trigger Value	Current Value
Major	ORSU (Outbound Replication Status)	Data Center 1/DC1-ARC1/ARC	Storage Unavailable	2020-05-26 21:47:18 MDT	Storage Unavailable	Storage Unavailable

Show 50 Records Per Page Refresh Previous « 1 » Next

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 **Confirmar** de la alarma y haga clic en **aplicar cambios**.

   La alarma ya no aparece en el panel o en la página Alarmas actuales.

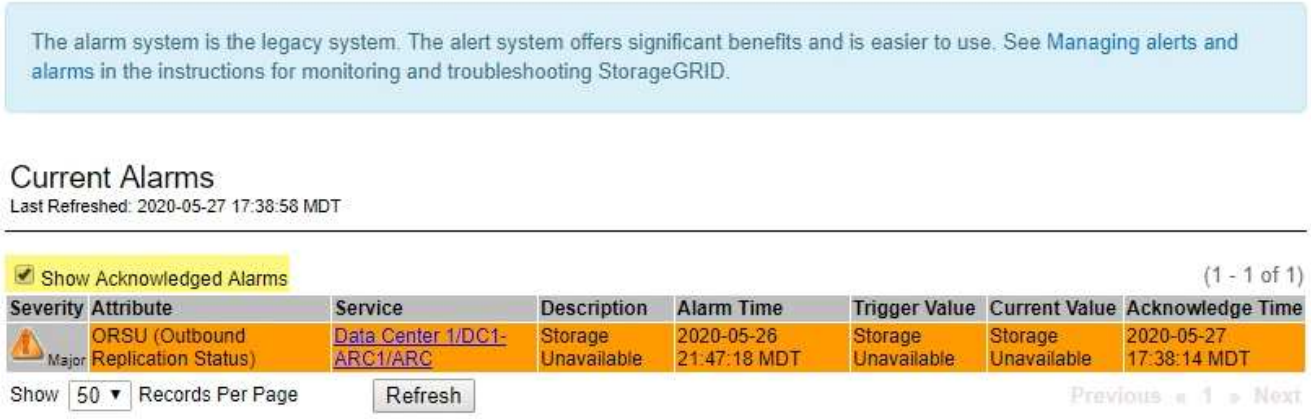
   > Cuando reconoce una alarma, la confirmación no se copia en otros nodos de administración. Por este motivo, si ve la consola desde otro nodo de administración, podría continuar viendo la alarma activa.

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.

Lo que necesitará

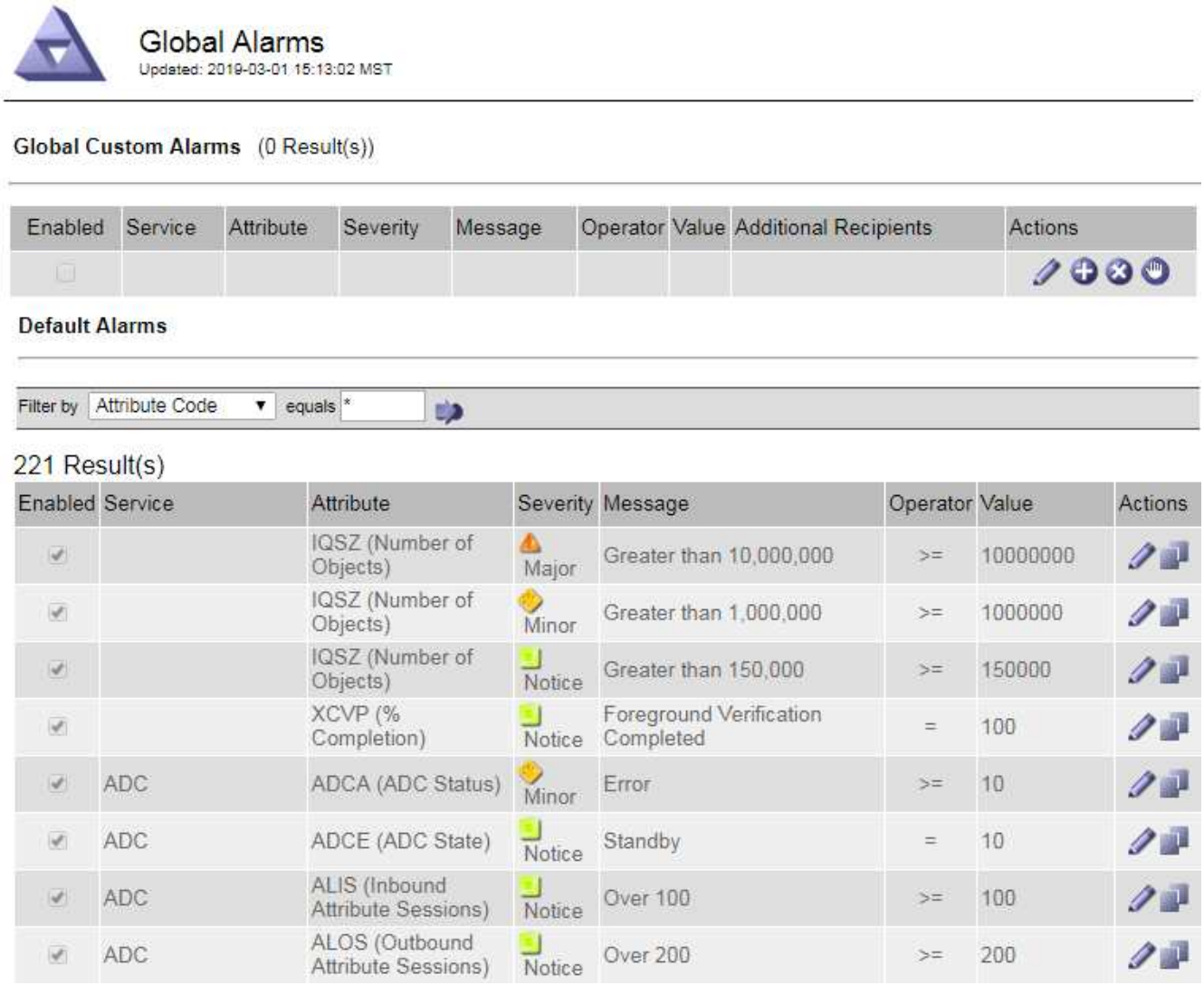
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener permisos de acceso específicos.

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.

Lo que necesitará

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

- Debe tener 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.

Lo que necesitará

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

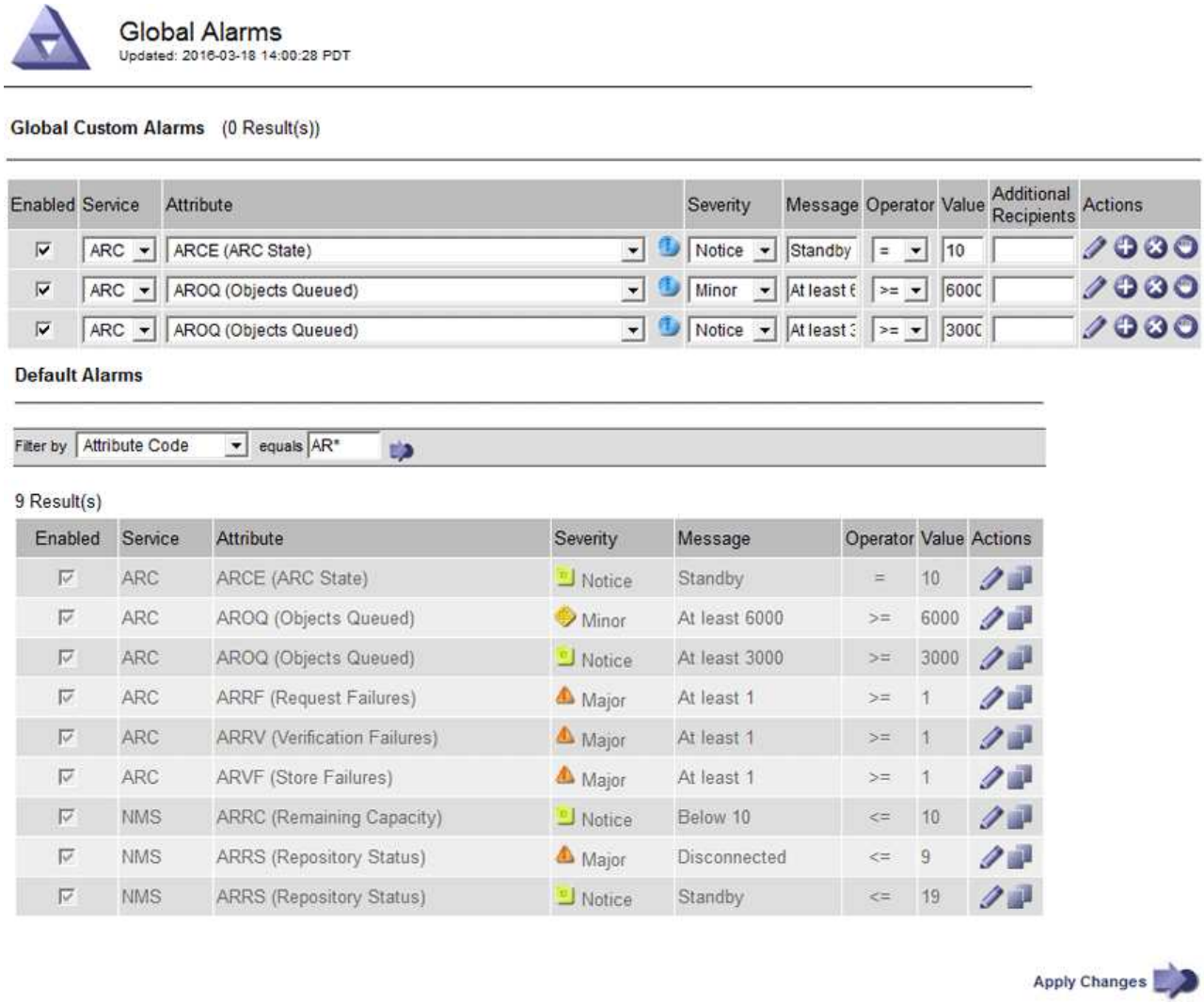
> Aunque el sistema de alarma heredado sigue siendo compatible, el sistema de alerta ofrece importantes ventajas y es más fácil de usar.

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 mucho 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 poder 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 y suelte 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 antiguas 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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener 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 desactive ninguna de las alarmas heredadas hasta que haya pasado completamente 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

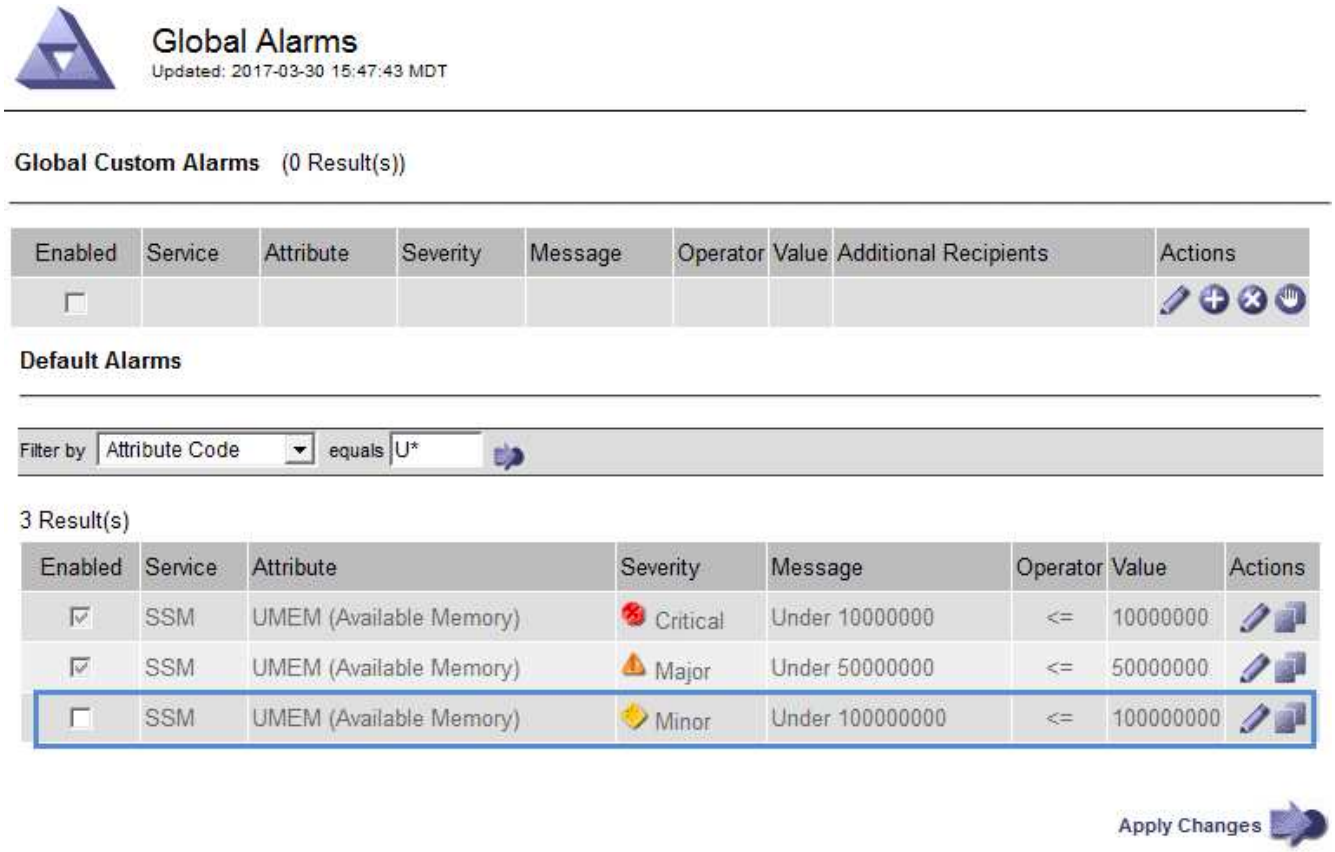
1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Global Alarms**.
2. Busque la alarma predeterminada para desactivarla.
   a. En la sección Alarmas predeterminadas, seleccione **Filtrar por** > **Código de atributo** o **Nombre de atributo**.
   b. Escriba una cadena de búsqueda.

      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 **Activado** para la alarma seleccionada se activa.

4. Deseleccione la casilla de verificación **Activado**.
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.

Lo que necesitará

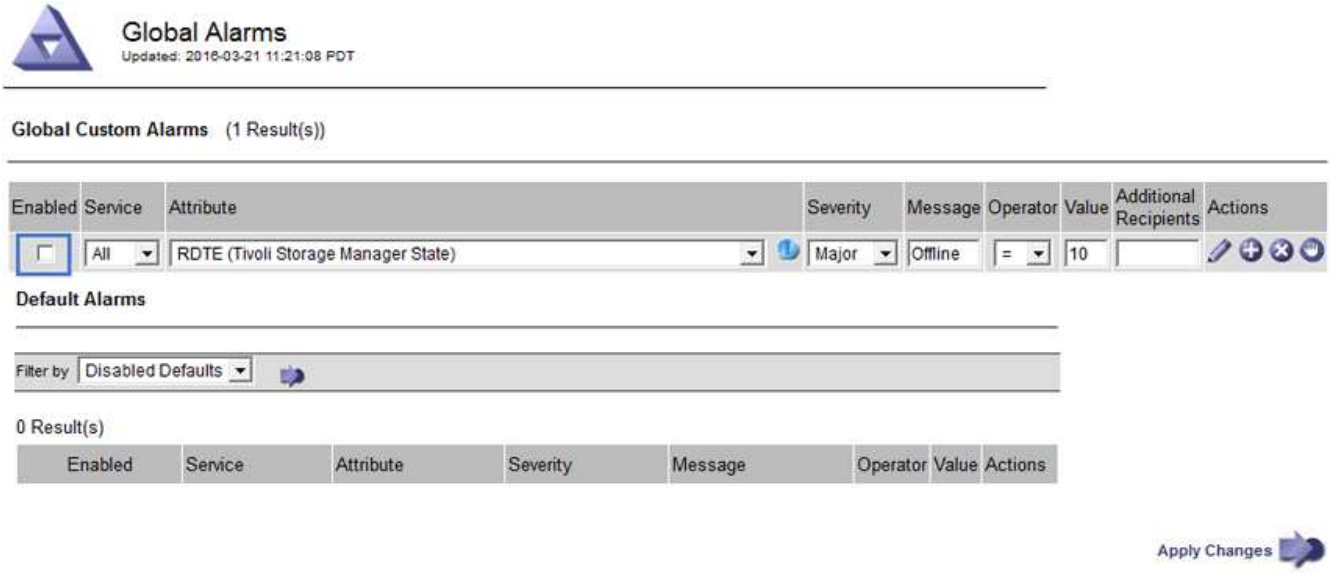
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener permisos de acceso específicos.

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. Deseleccione la casilla de verificación **Activado**.



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.

Lo que necesitará

- 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 el correo electrónico; no puede recibir el correo electrónico.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener 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 usa para notificaciones de alerta.

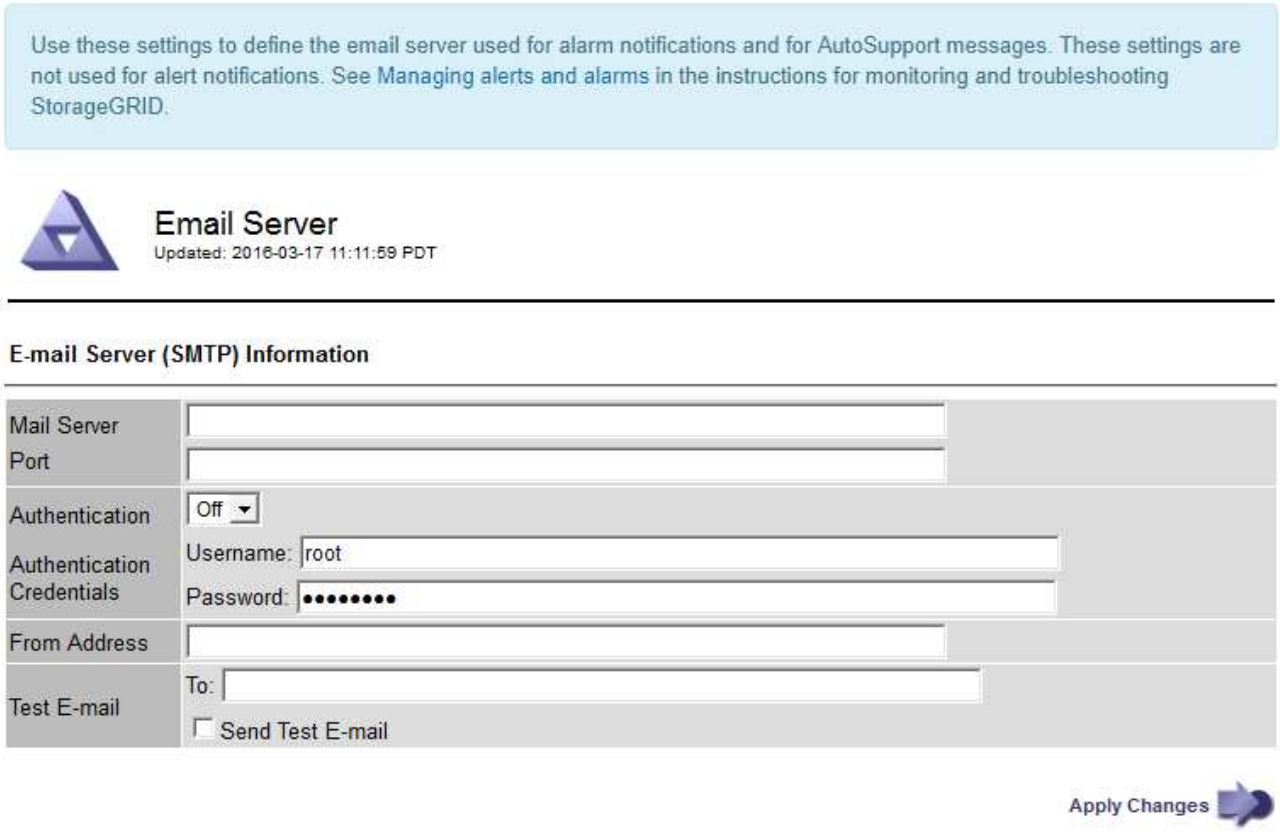
> Si utiliza SMTP como protocolo para mensajes de AutoSupport, es posible que ya haya configurado un servidor de correo SMTP. El mismo servidor SMTP se utiliza para notificaciones de correo electrónico de alarma, por lo que puede omitir este procedimiento. Consulte Instrucciones para administrar StorageGRID.

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 mensajes de 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 inmediatamente al servidor de correo electrónico 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.

Lo que necesitará

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

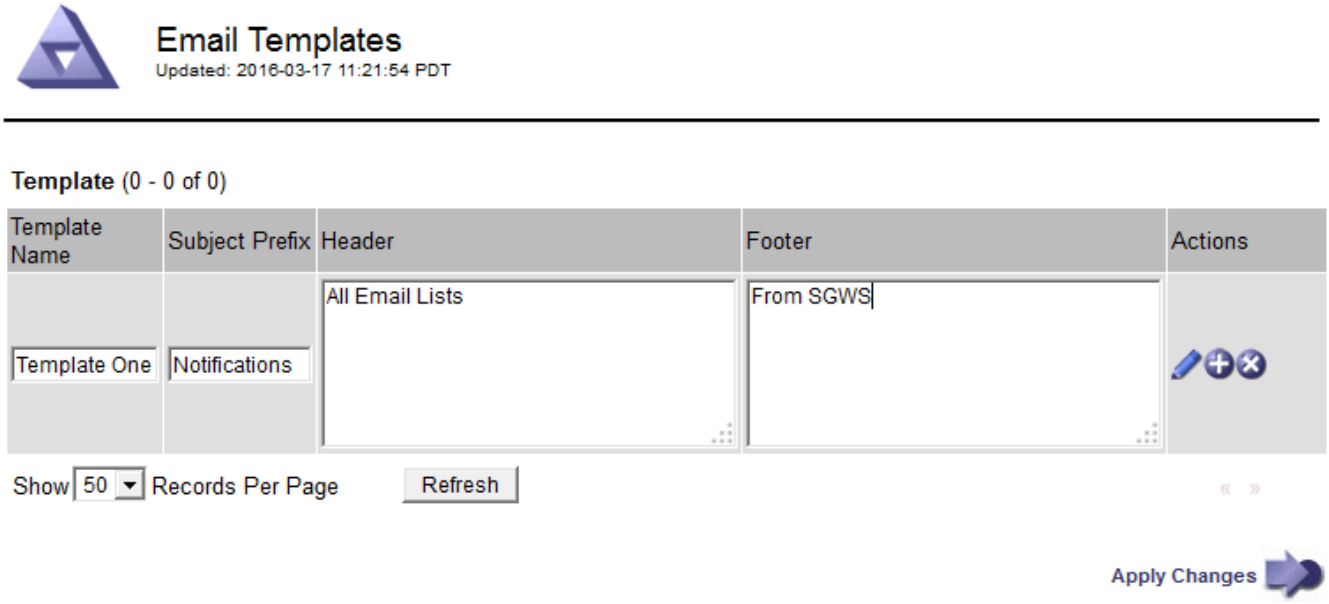
Acerca de esta tarea

Utilice estos ajustes para definir las plantillas de correo electrónico utilizadas para las notificaciones de alarmas heredadas. Esta configuración no se usa para notificaciones de alerta.

Las diferentes listas de correo pueden requerir otra información de contacto. Las plantillas no incluyen el texto principal 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 las plantillas 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.

Elemento	Descripción
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.

Lo que necesitará

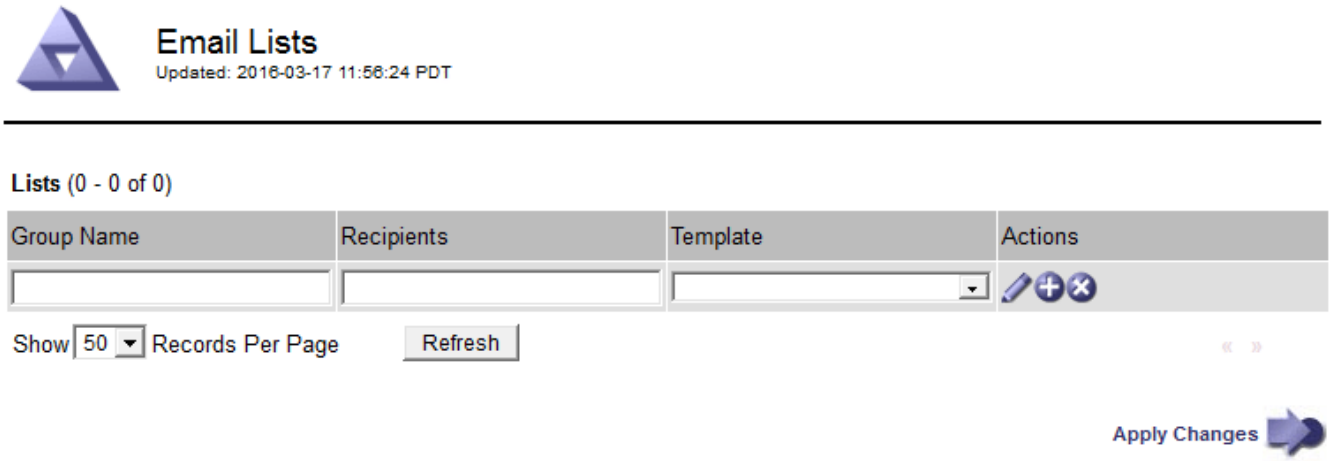
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener permisos de acceso específicos.
- Si desea especificar una plantilla de correo electrónico para la lista de correo (encabezado personalizado, pie de página y línea de asunto), debe haber creado la plantilla.

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 usa para 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.
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 alarmas heredado, los destinatarios deben ser miembros de una lista de correo y dicha lista debe agregarse 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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener 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 usa para 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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener 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 alerta.

> 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.

Suprimir las notificaciones por correo electrónico en todo el sistema

Es posible bloquear la capacidad del sistema StorageGRID para enviar notificaciones por correo electrónico de alarmas heredadas y mensajes de AutoSupport activados por eventos.

Lo que necesitará

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

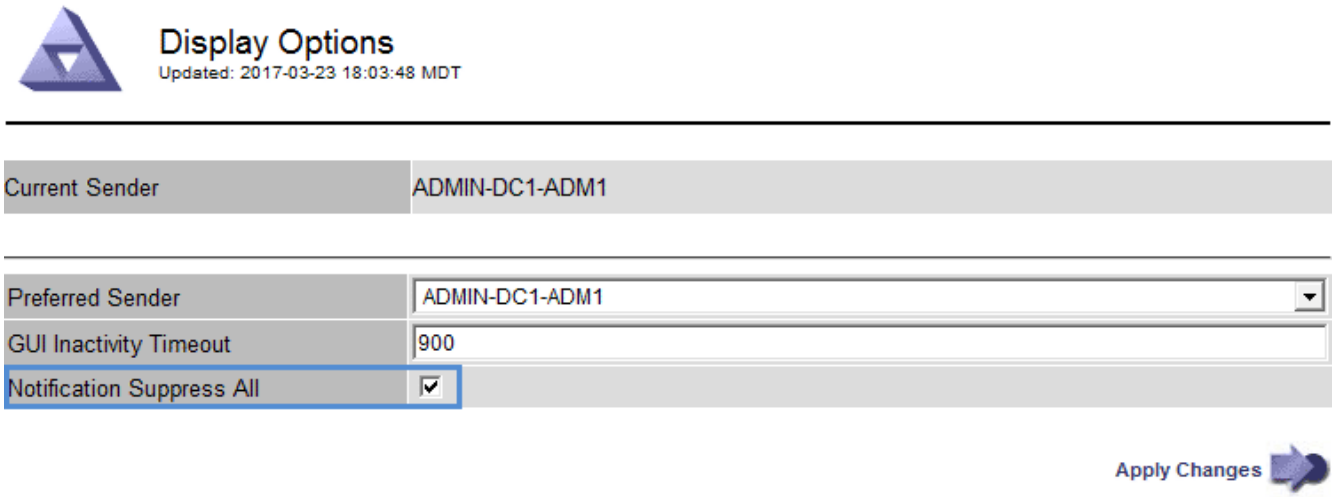
Acerca de esta tarea

Utilice esta opción para suprimir las notificaciones por correo electrónico de alarmas heredadas y mensajes de AutoSupport activados por eventos.

> Esta opción no suprime las notificaciones por correo electrónico de alerta. Tampoco suprime los mensajes de AutoSupport semanales o activados por el usuario.

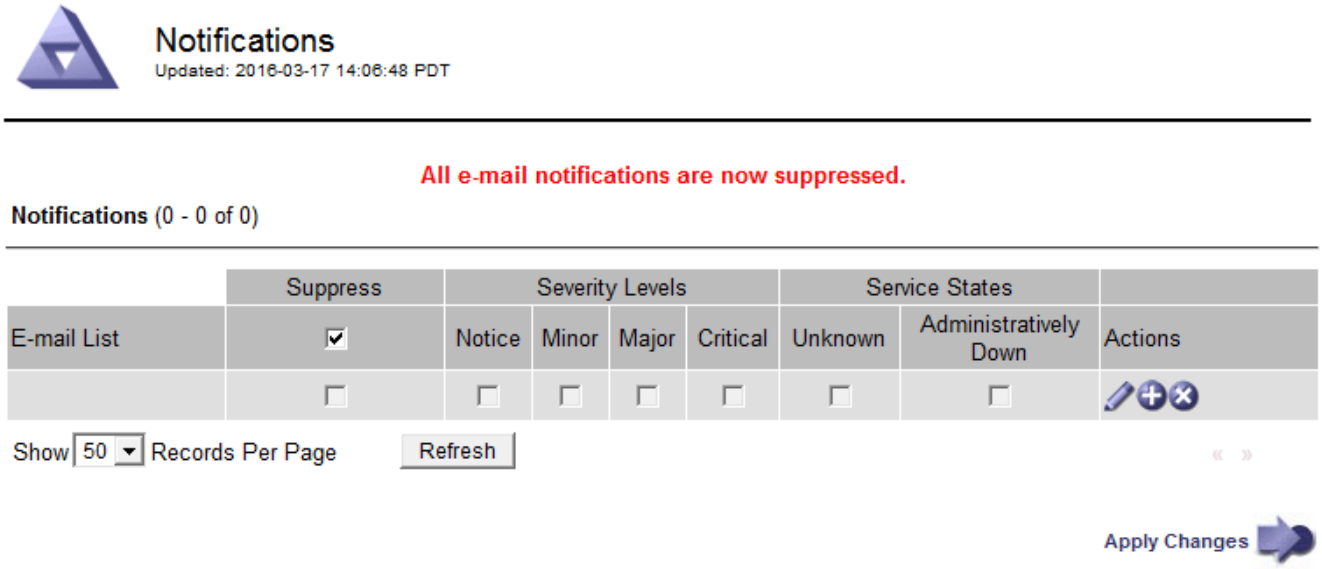
Pasos

1. Seleccione **CONFIGURACIÓN** > **Ajustes del sistema** > **Opciones de pantalla**.
2. En el menú Opciones de pantalla, seleccione **Opciones**.
3. Seleccione **notificación Suprimir todo**.



4. Haga clic en **aplicar cambios**.

   La página Notificaciones (**Configuración** > **Notificaciones**) muestra el siguiente mensaje:



Configurar los mensajes de auditoría y los destinos de registro

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. Puede ajustar los niveles de auditoría para aumentar o disminuir el tipo y el número de mensajes de auditoría registrados. Opcionalmente, puede definir los encabezados de solicitud HTTP que desee incluir en los mensajes de auditoría de lectura y escritura del cliente. También es posible configurar un servidor de syslog externo y modificar el destino de la información de auditoría.

Para obtener más información sobre los mensajes de auditoría, consulte Revisar los registros de auditoría.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso raíz o de mantenimiento.

Acerca de esta tarea

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 predeterminada, se envía la información de auditoría al registro de auditoría en los nodos admin. Se pueden ajustar los niveles de auditoría para aumentar o disminuir el tipo y el número de mensajes de auditoría registrados en el registro de auditoría. De manera opcional, se puede configurar el envío de la información de auditoría a un servidor de syslog remoto o que se almacene temporalmente en los nodos de origen para la recogida manual.

Cambiar los niveles de mensajes de auditoría en el registro de auditoría

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

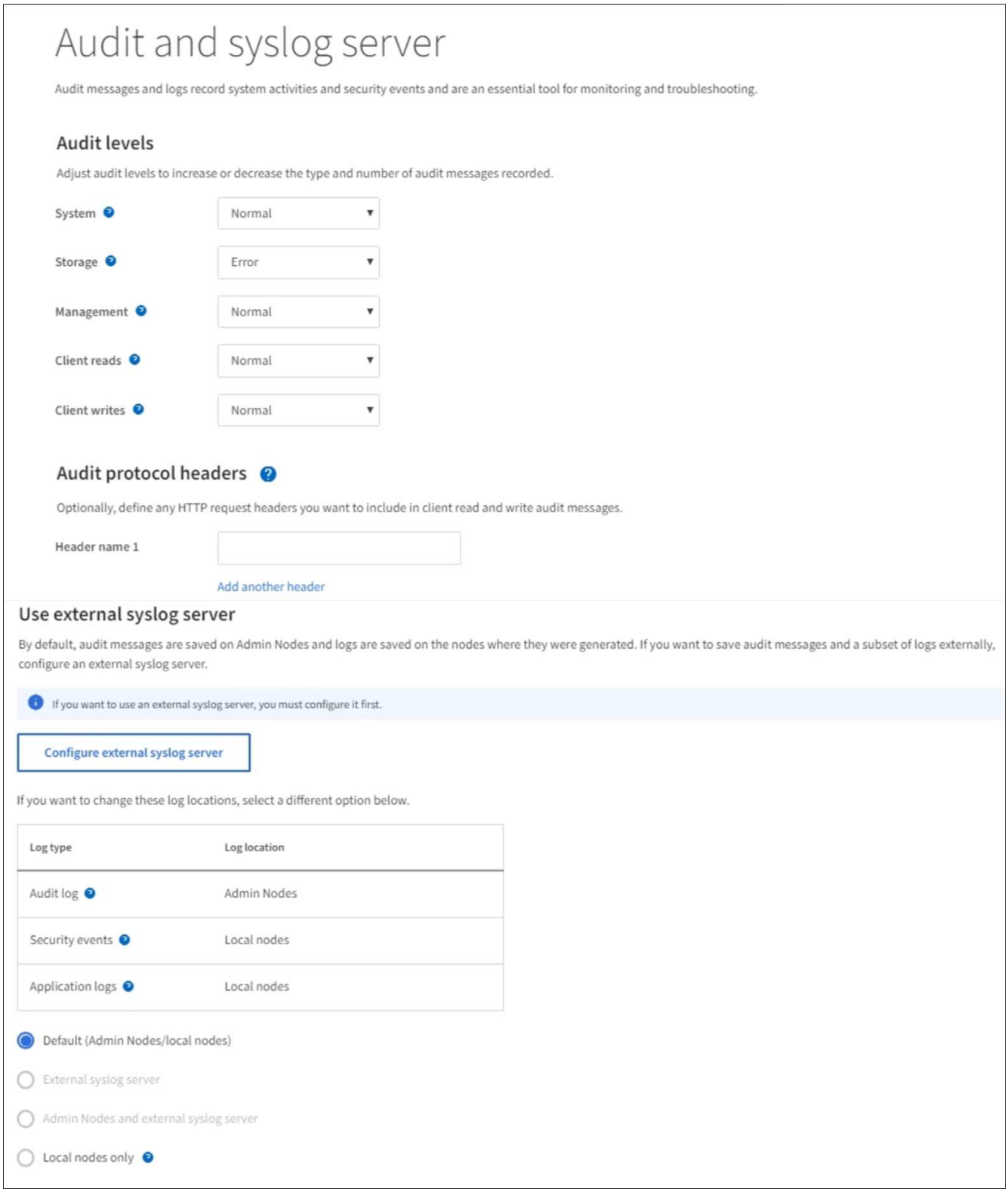
Categoría de auditoría	Descripción
Sistema	De forma predeterminada, este nivel se establece en normal. Consulte Mensajes de auditoría del sistema.
Reducida	De forma predeterminada, este nivel se establece en error. Consulte Mensajes de auditoría del almacenamiento de objetos.
Gestión	De forma predeterminada, este nivel se establece en normal. Consulte Mensaje de auditoría de gestión.
Lee el cliente	De forma predeterminada, este nivel se establece en normal. Consulte El cliente lee los mensajes de auditoría.
Escribe el cliente	De forma predeterminada, este nivel se establece en normal. Consulte El cliente escribe mensajes de auditoría.

Estos valores predeterminados se aplican si instaló inicialmente StorageGRID con la versión 10.3 o posterior. Si ha actualizado desde una versión anterior de StorageGRID, la opción predeterminada 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.

3. Opcionalmente, en **encabezados de protocolo de auditoría**, defina los encabezados de solicitud HTTP que desee 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.

   Los encabezados de protocolo de auditoría se aplican solo a solicitudes S3 y Swift.

4. 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**.

5. Seleccione **Guardar**

   Aparece un banner verde que indica que la configuración se ha guardado correctamente.

Use un servidor de syslog externo

Es posible configurar un servidor de syslog externo para guardar información de auditoría de manera remota.

- Si desea guardar información de auditoría en un servidor de syslog externo, vaya a. Configure un servidor de syslog externo.
- Si no utiliza un servidor de syslog externo, vaya a. Seleccione destinos de información de auditoría.

Seleccione destinos de información de auditoría

Es posible especificar dónde se envían los registros de auditoría, los registros de eventos de seguridad y los registros de aplicaciones.

Algunos destinos solo están disponibles si se utiliza un servidor de syslog externo. Consulte Configure un servidor de syslog externo para configurar un servidor de syslog externo.

Para obtener más información sobre los registros del software StorageGRID, consulte Registros del software StorageGRID.

1. En la página Audit and syslog Server, seleccione el destino para la información de auditoría de las opciones que aparecen:

Opción	Descripción
Predeterminado (nodos de administrador/nodos locales)	Se envían mensajes de auditoría al registro de auditoría (`audit.log`) En el nodo Admin, y los registros de eventos de seguridad y de aplicaciones se almacenan en los nodos en los que se generaron (también denominado "nodo local").
Servidor de syslog externo	La información de auditoría se envía a un 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.
Nodo de administrador y servidor de syslog externo	Se envían mensajes de auditoría al registro de auditoría (`audit.log`) En el nodo Admin, y la información de auditoría se envía al servidor 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.
Solo nodos locales	No se envía información de auditoría a un nodo de administrador ni al servidor de syslog remoto. La información de auditoría solo se guarda en los nodos que la generaron. **Nota**: StorageGRID elimina periódicamente estos registros locales en 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.

La información de auditoría generada en cada nodo local se almacena en `/var/local/log/localaudit.log`

1. Seleccione **Guardar**.

Aparecerá un mensaje de advertencia:

¿Desea cambiar el destino del registro?

1. Confirme que desea cambiar el destino de la información de auditoría seleccionando **Aceptar**.

   Aparece un mensaje de cabecera verde en el que se le notifica que la configuración de auditoría se ha

guardado correctamente.

Los nuevos registros se envían a los destinos seleccionados. Los registros existentes permanecen en su ubicación actual.

Información relacionada

Consideraciones sobre el servidor de syslog externo

Administre StorageGRID

Solucione problemas en el servidor de syslog externo

Use un servidor de syslog externo

Consideraciones sobre el servidor de syslog externo

Use las siguientes directrices para calcular el tamaño del servidor de syslog externo que necesita.

¿Qué es 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 configurar los destinos de la información de auditoría para poder reducir el tráfico de red en los nodos de administración y gestionar la información de manera más eficiente. 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

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	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 bloques no incluyen este campo.

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

Usemos K para representar el tamaño medio de la suma de los nombres de cuenta de S3, 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). No están disponibles fórmulas detalladas para estimar la tasa y el tamaño medio de los mensajes de auditoría para los ajustes de nivel de auditoría no predeterminados. Sin embargo, el cuadro siguiente puede ser utilizado para hacer una estimación aproximada de la tarifa; puede utilizar la fórmula de tamaño medio proporcionada para los registros de auditoría, pero tenga en cuenta que es probable que tenga como resultado una sobreestimación porque los mensajes de auditoría “adicionales” son, en promedio, menores 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 = tasa de operaciones de 8 x S3
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	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 bloques 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
- Código 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 nombres de cuenta de S3, 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 nombres de cuenta de S3, 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
```

Por ejemplo, si el tamaño de su grid se ajusta a 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 syslog externo debe ser compatible con 2,250 registros de aplicación por segundo y debe poder recibir y recibir (y normalmente almacenar) datos de aplicación a una velocidad de 0.6 MB por segundo.

Para obtener más información sobre la configuración de niveles de mensajes de auditoría y un servidor de syslog externo, consulte lo siguiente:

- Configure un servidor de syslog externo
- Configurar los mensajes de auditoría y los destinos de registro

Configure un servidor de syslog externo

Si desea guardar registros de auditoría, registros de aplicaciones y registros de eventos de seguridad en una ubicación fuera de la cuadrícula, utilice este procedimiento para configurar un servidor de syslog externo.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene permisos de acceso raíz o de mantenimiento.
- Tiene un servidor de syslog con la capacidad para recibir y almacenar los archivos de registro. Para obtener más información, consulte Consideraciones sobre el servidor de syslog externo.
- Tiene las certificaciones de servidor y cliente correctas si tiene previsto utilizar TLS o RELP/TLS.

Acerca de esta tarea

Si desea enviar información de auditoría a un servidor de syslog externo, primero debe configurar el servidor externo.

El envío de información de auditoría a un servidor de syslog externo permite:

- Recopilar y gestionar información de auditoría, como mensajes de auditoría, registros de aplicaciones y eventos de seguridad, de forma más eficiente
- Reduzca el tráfico de red en los nodos de administrador, ya que la información de auditoría se transfiere directamente de los distintos nodos de almacenamiento al servidor de syslog externo, sin tener que atravesar un nodo de administración

> Cuando se envían registros a un servidor de syslog externo, los registros únicos superiores a 8192 bytes se truncarán al final del mensaje para ajustarse a las limitaciones comunes en las implementaciones de servidores de syslog externos.

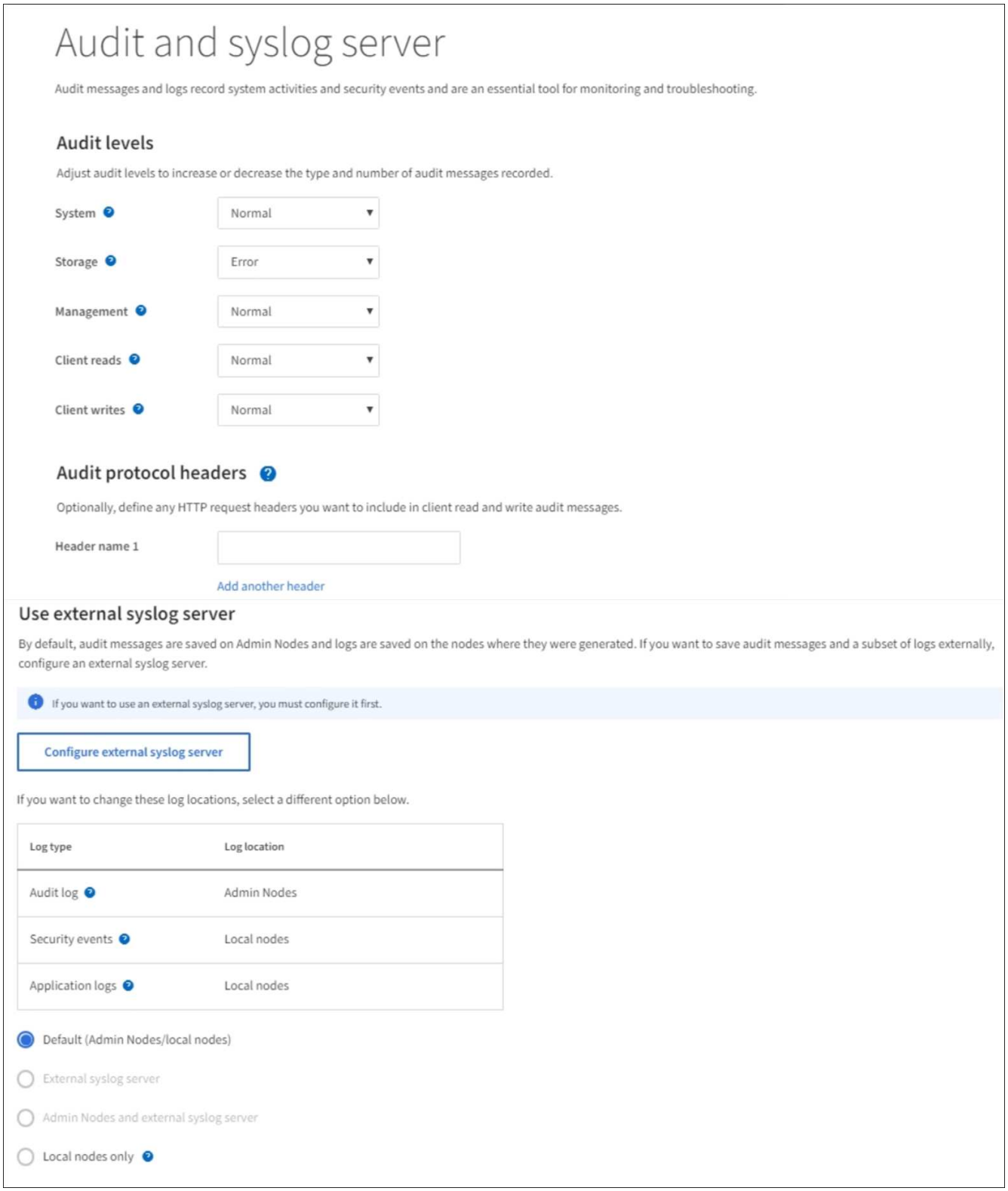
> Para maximizar las opciones de recuperación completa de datos en caso de un fallo del servidor de syslog externo, se mantienen hasta 20 GB de registros locales de registros de auditoría (localaudit.log) en cada nodo.

> 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 la API privada `audit-destinations` puntos finales. Por ejemplo, es posible usar diferentes servidores de syslog para diferentes grupos de nodos.

Acceda al asistente de configuración del servidor de syslog

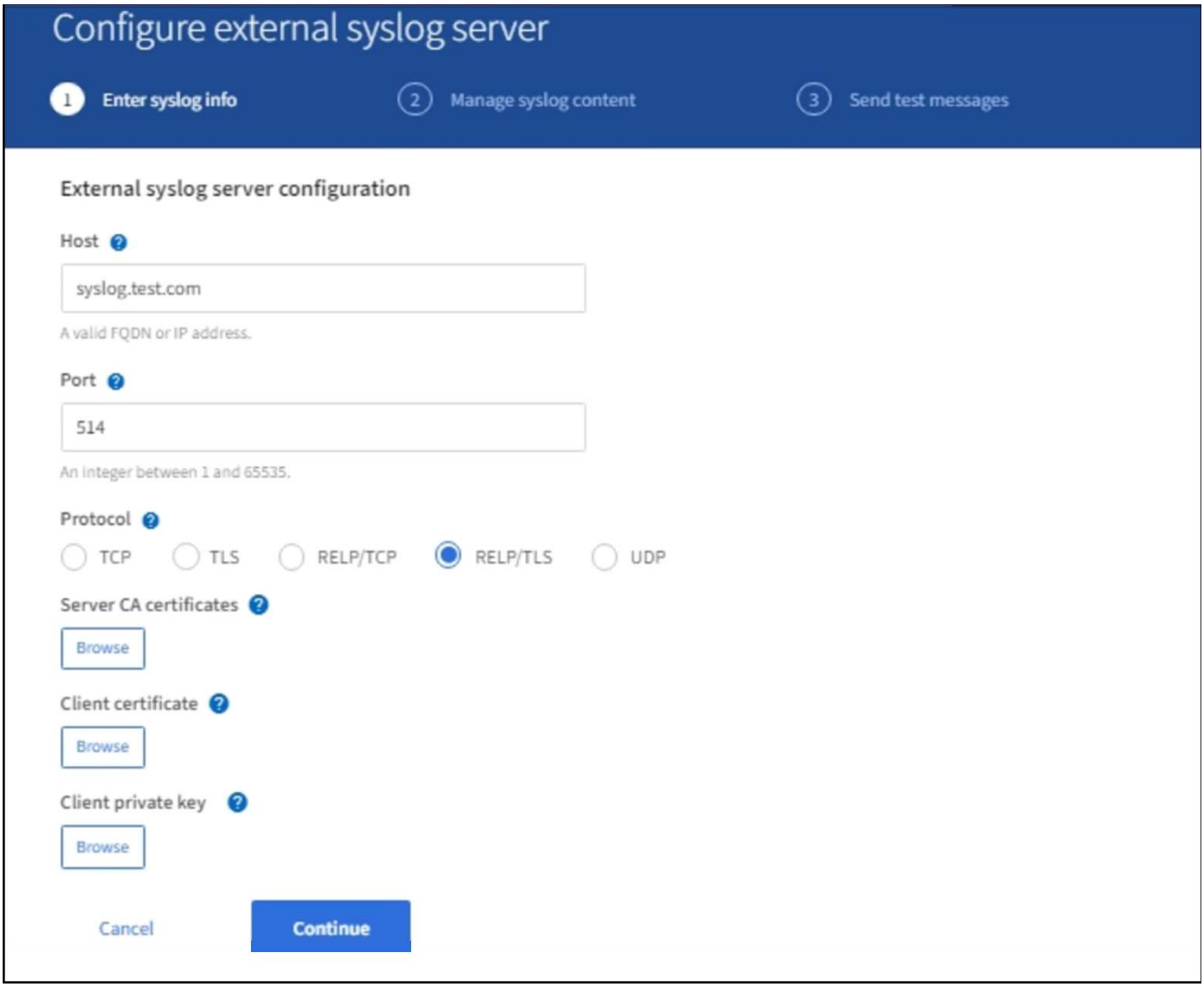
Pasos

1. Seleccione **CONFIGURACIÓN** > **Supervisión** > **servidor de auditoría y syslog**.



2. En la página servidor de auditoría y syslog, seleccione **Configurar servidor de syslog externo**. Si ha configurado previamente un servidor de syslog externo, seleccione **Editar servidor de syslog externo**.

Introduzca la información de syslog



1. Introduzca un nombre de dominio completo válido o una dirección IPv4 o IPv6 para el servidor de syslog externo en el campo **Host**.
2. Introduzca el puerto de destino en el servidor de syslog externo (debe ser un entero entre 1 y 65535). El puerto predeterminado es 514.
3. Seleccione el protocolo utilizado para enviar información de auditoría al servidor de syslog externo.

   Se recomienda 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 Use los certificados de seguridad StorageGRID.

   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.

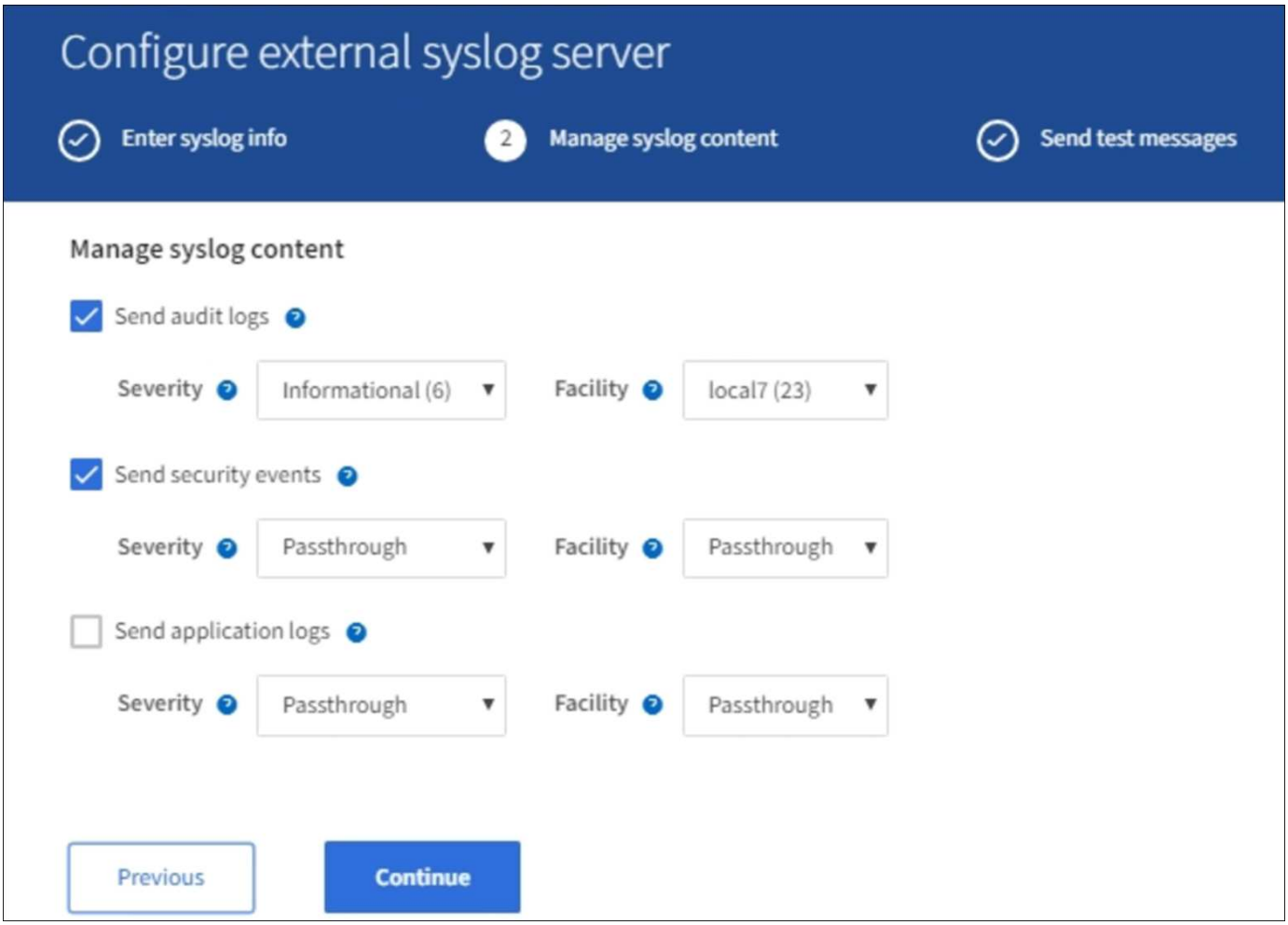
4. Seleccione **continuar**.
5. Si ha seleccionado **TLS** o **RELP/TLS**, cargue los siguientes certificados:
   - **Certificados de CA del servidor**: Uno o más certificados de CA de confianza para verificar el servidor syslog externo (en codificación PEM). Si se omite, se utilizará el certificado de CA de cuadrícula predeterminado. El archivo que cargue aquí puede ser un bundle de CA.
   - **Certificado de cliente**: 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.

     i. Seleccione **Buscar** para el certificado o la clave que desee utilizar.
     ii. Seleccione el archivo de certificado o el archivo de claves.
     iii. 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.
6. Seleccione **continuar**.

Permite gestionar el contenido de syslog



1. Seleccione cada tipo de información de auditoría que desea enviar al servidor de syslog externo.
   - **Enviar registros de auditoría**: Eventos StorageGRID y actividades del sistema
   - **Enviar eventos de seguridad**: Eventos de seguridad como cuando un usuario no autorizado intenta iniciar sesión o un usuario inicia sesión como root
   - **Enviar registros de aplicación**: Archivos de registro útiles para la solución de problemas, incluidos:
     - bycast-err.log
     - bycast.log
     - jaeger.log
     - nms.log (solo nodos del administrador)
     - prometheus.log
     - raft.log
     - hagroups.log
2. Utilice los menús desplegables para seleccionar la gravedad y el servicio (tipo de mensaje) de la categoría de información de auditoría que desea enviar.

   Si selecciona **Paso a través** para severidad e instalación, la información enviada al servidor syslog remoto recibirá la misma gravedad y facilidad que cuando se haya iniciado sesión localmente en el nodo. Establecer las instalaciones y la gravedad pueden ayudarle a agregar los registros de formas personalizables para facilitar el análisis.

Para obtener más información sobre los registros del software StorageGRID, consulte Registros del software StorageGRID.

a. Para **severidad**, seleccione **Paso a través** si desea que cada mensaje enviado al syslog externo tenga el mismo valor de gravedad que en el syslog local.

   Para los registros de auditoría, si selecciona **Paso a través**, la gravedad es 'info'.

   Para eventos de seguridad, si selecciona **Paso a través**, la distribución linux genera los valores de gravedad en los nodos.

   Para los registros de la aplicación, si selecciona **Paso a través**, las gravedades varían entre "info" y "notice", dependiendo de cuál sea el problema. Por ejemplo, la adición de un servidor NTP y la configuración de un grupo ha proporcionan un valor de "información", mientras que la detención intencional del servicio ssm o rsm proporciona un valor de "aviso".

b. Si no desea utilizar el valor de paso a través, seleccione un valor de gravedad entre 0 y 7.

   El valor seleccionado se aplicará a todos los mensajes de este tipo. Se perderá información acerca de las diferentes gravedades cuando elija reemplazar la gravedad con un valor fijo.

Gravedad	Descripción
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

c. Para **Facility**, seleccione **PassThrough** si desea que cada mensaje enviado al syslog externo tenga el mismo valor de instalación que en el syslog local.

   Para los registros de auditoría, si selecciona **PassThrough**, la instalación enviada al servidor syslog externo es 'local7'.

   Para los eventos de seguridad, si selecciona **Paso a través**, los valores de la instalación los genera la distribución linux en los nodos.

   Para los registros de aplicaciones, si selecciona **Paso a través**, los registros de la aplicación enviados al servidor syslog externo tienen los siguientes valores de instalación:

Registro de aplicaciones	Valor de paso a través
bycast.log	usuario o demonio
bycast-err.log	usuario, daemon, local3 o local4
jaeger.log	local2
nms.log	local3
prometheus.log	local4
raft.log	local5
hagroups.log	local6

d. Si no desea utilizar el valor de paso a través, seleccione el valor de la instalación entre 0 y 23.

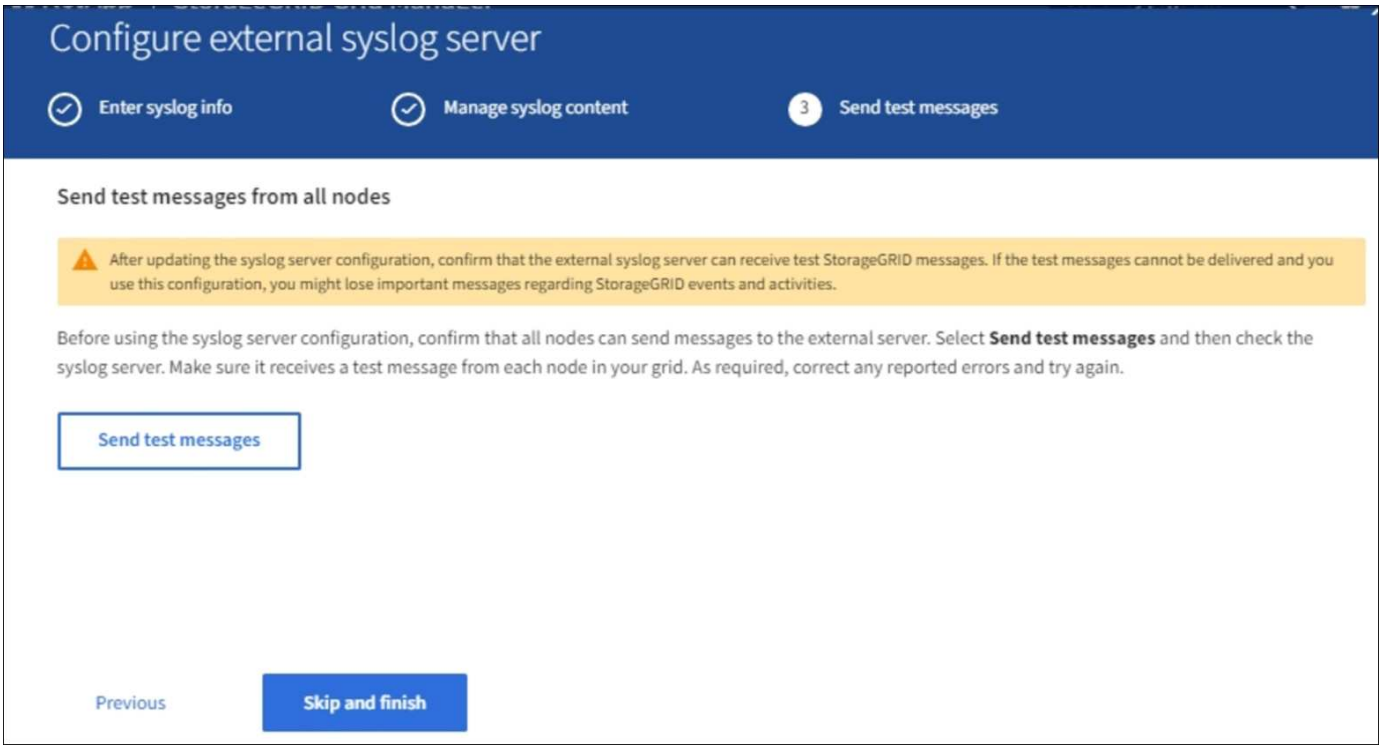
   El valor seleccionado se aplicará a todos los mensajes de este tipo. Se perderá información acerca de las distintas instalaciones cuando elija reemplazar la instalación con un valor fijo.

Centro	Descripción
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 se confirme que el servidor de syslog externo recibió un mensaje de prueba de cada nodo de la cuadrícula y que el mensaje se procesó según lo esperado.

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

   Aparece un banner verde que indica que la configuración se ha guardado correctamente.

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

   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 Solucionar problemas del 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 los demás protocolos.

6. Seleccione **Detener y finalizar**.

   Volverá a la página **Audit and syslog Server**. Aparece un banner verde para notificarle que la configuración del servidor de syslog se ha guardado correctamente.

   > La información de auditoría de StorageGRID no se envía al servidor de syslog externo hasta que se selecciona un destino que incluye el servidor de syslog externo.

Seleccione destinos de información de auditoría

Es posible especificar dónde se envían los registros de eventos de seguridad, los registros de aplicaciones y los registros de mensajes de auditoría.

> Para obtener más información sobre los registros del software StorageGRID, consulte Registros del software StorageGRID.

1. En la página Audit and syslog Server, seleccione el destino para la información de auditoría de las opciones que aparecen:

Opción	Descripción
Predeterminado (nodos de administrador/nodos locales)	Se envían mensajes de auditoría al registro de auditoría (`audit.log`) En el nodo Admin, y los registros de eventos de seguridad y de aplicaciones se almacenan en los nodos en los que se generaron (también denominado "nodo local").
Servidor de syslog externo	La información de auditoría se envía a un 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.
Nodo de administrador y servidor de syslog externo	Se envían mensajes de auditoría al registro de auditoría (`audit.log`) En el nodo Admin, y la información de auditoría se envía al servidor 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.
Solo nodos locales	No se envía información de auditoría a un nodo de administrador ni al servidor de syslog remoto. La información de auditoría solo se guarda en los nodos que la generaron. **Nota**: StorageGRID elimina periódicamente estos registros locales en 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.

La información de auditoría generada en cada nodo local se almacena en `/var/local/log/localaudit.log`

1. Seleccione **Guardar**. A continuación, seleccione Aceptar para aceptar el cambio en el destino del registro.
2. Si ha seleccionado **servidor syslog externo** o **nodos de administración y servidor syslog externo** como destino de la información de auditoría, aparecerá una advertencia adicional. Revise el texto de advertencia.

Debe confirmar que el servidor de syslog externo puede recibir mensajes de StorageGRID de prueba.

1. Confirme que desea cambiar el destino de la información de auditoría seleccionando **Aceptar**.

   Aparece un mensaje de cabecera verde en el que se le notifica que la configuración de auditoría se ha guardado correctamente.

   Los nuevos registros se envían a los destinos seleccionados. Los registros existentes permanecen en su ubicación actual.

Información relacionada

Información general de los mensajes de auditoría

Configurar los mensajes de auditoría y los destinos de registro

Mensajes de auditoría del sistema

Mensajes de auditoría del almacenamiento de objetos

Mensaje de auditoría de gestión

El cliente lee los mensajes de auditoría

Administre StorageGRID

Usar supervisión de SNMP

Si desea supervisar StorageGRID mediante el protocolo simple de gestión de redes (SNMP), debe configurar el agente SNMP que se incluye con StorageGRID.

- Configure el agente SNMP
- Actualice el agente SNMP

Funcionalidades

Cada nodo StorageGRID ejecuta un agente SNMP, o un daemon, que proporciona una base de datos de información de gestión (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.

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** son notificaciones enviadas por el agente SNMP que no requieren el reconocimiento del sistema de administración. 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** es similar a las trampas, pero requieren el reconocimiento del sistema de administración. 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 en los siguientes casos:

- Una alerta predeterminada o personalizada se activa en cualquier nivel de gravedad. Para suprimir las notificaciones SNMP de una alerta, debe configurar un silencio para la alerta. Las notificaciones de alerta se envían mediante el nodo de administrador que esté configurado para que sea el remitente preferido.

  Cada alerta se asigna a uno de los tres tipos de trampa según el nivel de gravedad de la alerta: ActiveMinorAlert, activeMajorAlert y activeCriticalAlert. Para obtener descripciones de las alertas que pueden desencadenar estos retos, consulte Referencia de alertas.

- Ciertas alarmas (sistema heredado) se activan a niveles de gravedad especificados o superiores.

  Las notificaciones SNMP no se envían para cada alarma ni para 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.

Acceda a la MIB

Puede acceder al archivo de definición MIB en la siguiente ubicación en cualquier nodo StorageGRID:

```
/usr/share/snmp/mibs/NETAPP-STORAGEGRID-MIB.txt
```

Información relacionada

- Referencia de alertas
- Referencia de alarmas (sistema heredado)
- Alarmas que generan notificaciones SNMP (sistema heredado)
- Silenciar notificaciones de alerta

Configure el agente SNMP

Puede configurar el agente SNMP de StorageGRID si desea usar un sistema de administración SNMP de terceros para el acceso MIB de solo lectura y las notificaciones.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

Acerca de esta tarea

El agente SNMP de StorageGRID admite las tres versiones del protocolo SNMP. Puede configurar el agente para una o más versiones.

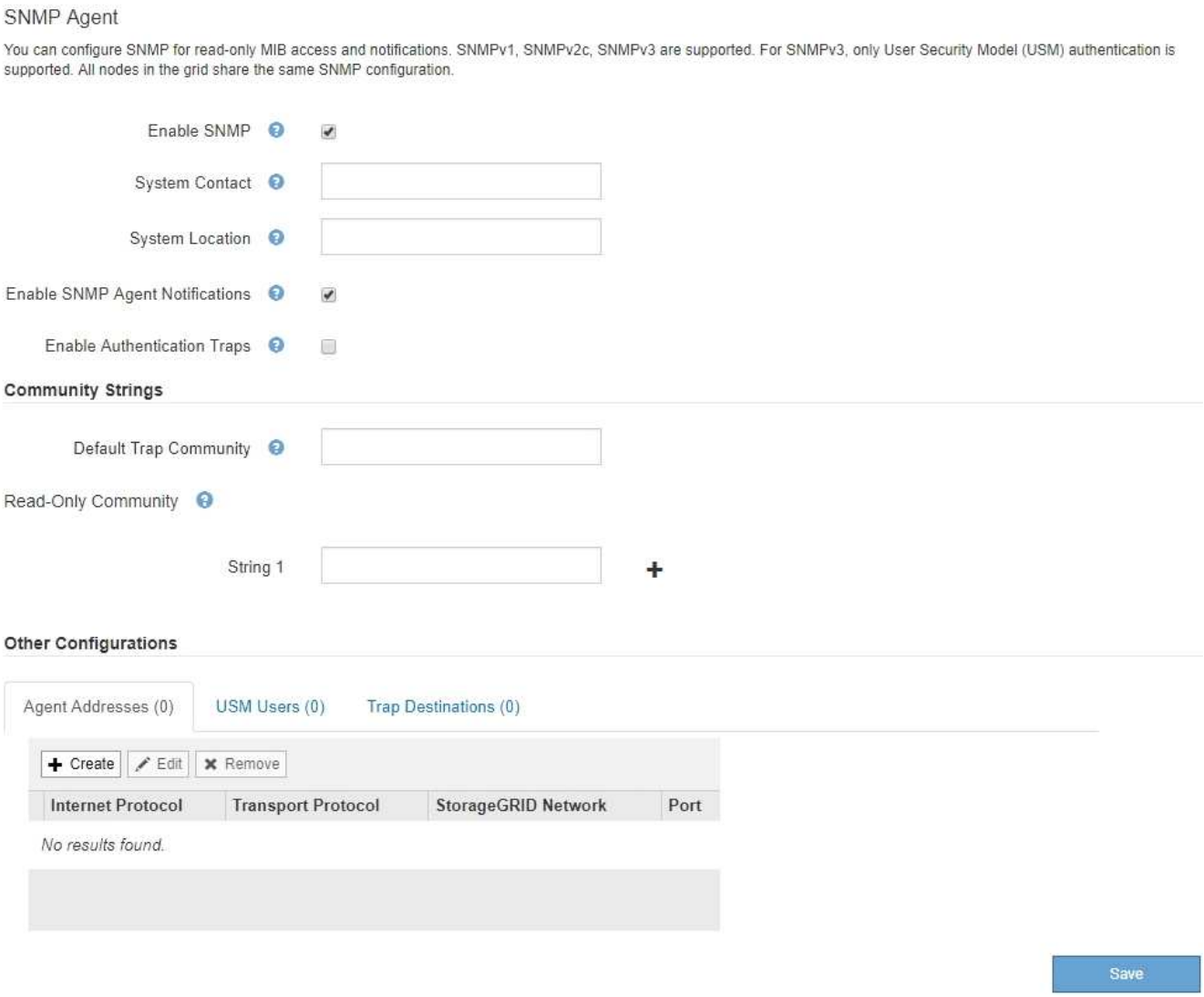
Pasos

1. Seleccione **CONFIGURACIÓN** > **Supervisión** > **Agente SNMP**.

   Aparece la página Agente SNMP.

2. Para activar el agente SNMP en todos los nodos de cuadrícula, active la casilla de verificación **Activar SNMP**.

   Aparecen los campos para configurar un agente SNMP.



3. En el campo **Contacto del sistema**, introduzca el valor que desea que StorageGRID proporcione en los mensajes SNMP para sysContact.

   El Contacto del sistema normalmente es una dirección de correo electrónico. El valor que proporcione se aplicará a todos los nodos del sistema StorageGRID. **Contacto del sistema** puede tener un máximo de 255 caracteres.

4. En el campo **ubicación del sistema**, introduzca el valor que desea que StorageGRID proporcione en los mensajes SNMP para 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. El valor que proporcione se aplicará a todos los nodos del sistema StorageGRID. **Ubicación del sistema** puede tener un máximo de 255 caracteres.

5. Mantenga seleccionada la casilla de verificación **Activar notificaciones de agente SNMP** si desea que el agente SNMP de StorageGRID envíe notificaciones de captura e informe.

   Si esta casilla de verificación no está seleccionada, el agente SNMP admite acceso MIB de sólo lectura, pero no envía ninguna notificación SNMP.

6. Active la casilla de verificación **Activar capturas de autenticación** si desea que el agente SNMP de

StorageGRID envíe una captura de autenticación si recibe un mensaje de protocolo autenticado incorrectamente.

7. Si utiliza SNMPv1 o SNMPv2c, complete la sección Community Strings.

   Los campos de esta sección se utilizan para la autenticación basada en la comunidad en SNMPv1 o SNMPv2c. Estos campos no se aplican a SNMPv3.

   a. En el campo **Default Trap Community**, introduzca opcionalmente la cadena de comunidad predeterminada que desea utilizar para los destinos de captura.

      Según sea necesario, puede proporcionar una cadena de comunidad diferente ("personalizada") cuando usted lo necesite definir un destino de captura específico.

      La comunidad de solapamientos predeterminada puede tener un máximo de 32 caracteres y no puede contener caracteres en espacios en blanco.

   b. Para **Comunidad de sólo lectura**, introduzca una o más cadenas de comunidad para permitir el acceso MIB de sólo lectura en direcciones de agente IPv4 e IPv6. Haga clic en el signo más ➕ para agregar varias cadenas.

      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.

      Cada cadena de comunidad puede tener un máximo de 32 caracteres y no puede contener caracteres en blanco. Se permiten hasta cinco cadenas.

      > ⓘ Para garantizar la seguridad de su sistema StorageGRID, no utilice "'public'" como cadena de la comunidad. Si no introduce una cadena de comunidad, el agente SNMP utiliza el identificador de grid del sistema StorageGRID como la cadena de comunidad.

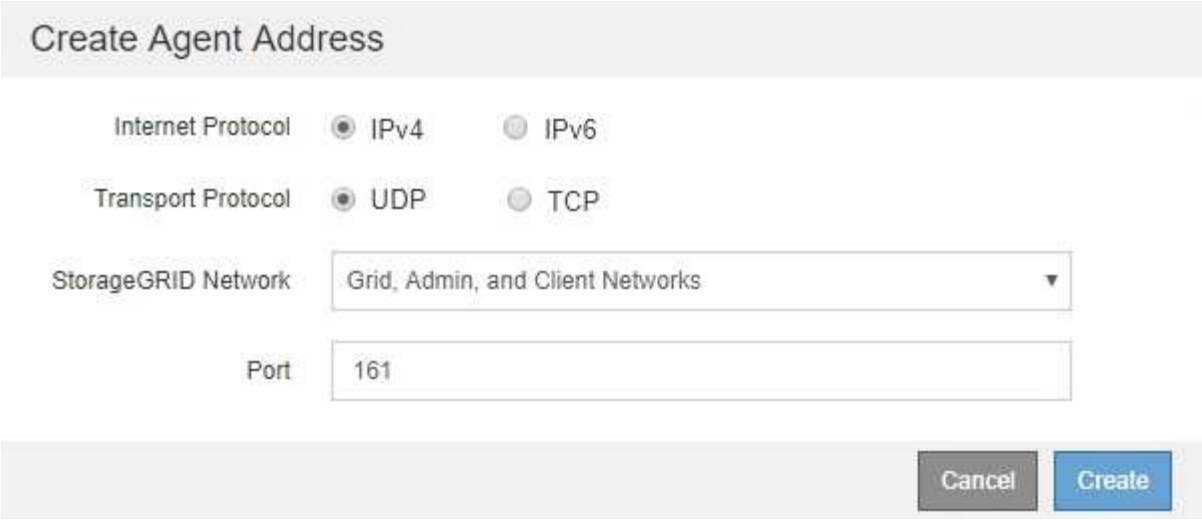
8. Si lo desea, seleccione la ficha direcciones del agente en la sección otras configuraciones.

   Utilice esta pestaña para especificar una o más «'direcciones de escucha'». Éstas son las direcciones StorageGRID en las que el agente SNMP puede recibir consultas. Cada dirección del agente incluye un protocolo de Internet, un protocolo de transporte, una red StorageGRID y, opcionalmente, un puerto.

   Si no configura una dirección de agente, la dirección de escucha predeterminada es el puerto UDP 161 en todas las redes StorageGRID.

   a. Haga clic en **Crear**.

      Aparece el cuadro de diálogo Crear dirección del agente.



b. Para **Internet Protocol**, seleccione si esta dirección utilizará IPv4 o IPv6.

   De forma predeterminada, SNMP utiliza IPv4.

c. Para **Protocolo de transporte**, seleccione si esta dirección utilizará UDP o TCP.

   De forma predeterminada, SNMP utiliza UDP.

d. En el campo **Red StorageGRID**, seleccione en qué red StorageGRID se recibirá la consulta.

   - Redes de grid, administración y cliente: StorageGRID debería escuchar las consultas SNMP en las tres redes.
   - Red Grid
   - Red de administración
   - Red cliente

   > Para garantizar la seguridad de las comunicaciones de cliente con StorageGRID, no debe crear una dirección de agente para la red de cliente.

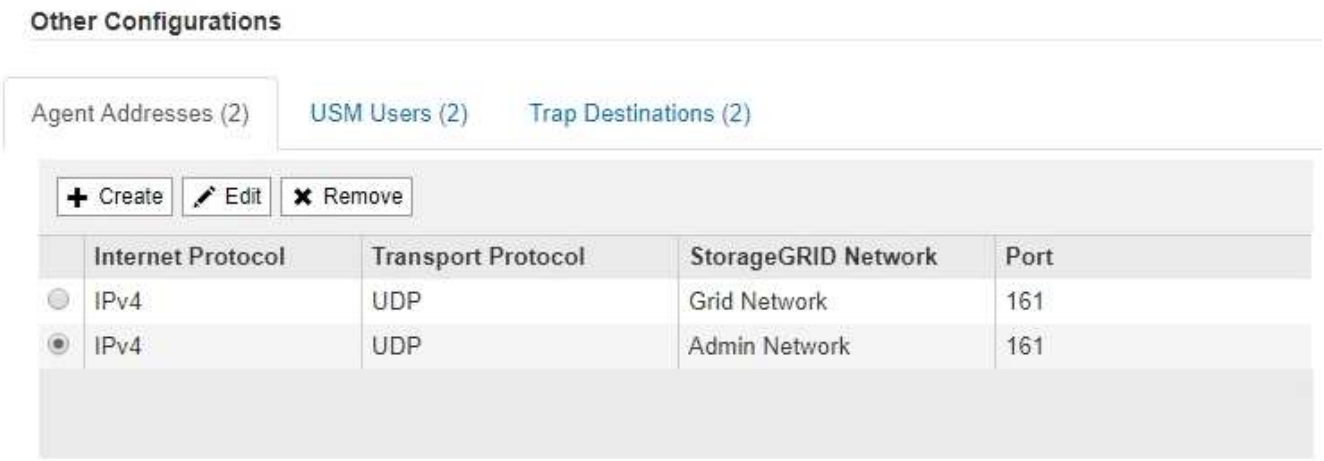
e. En el campo **Puerto**, introduzca opcionalmente el número de puerto en el que debe escuchar el agente SNMP.

   El puerto UDP predeterminado para un agente SNMP es 161, pero puede introducir cualquier número de puerto no utilizado.

   > 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.

f. Haga clic en **Crear**.

   La dirección del agente se crea y se agrega a la tabla.



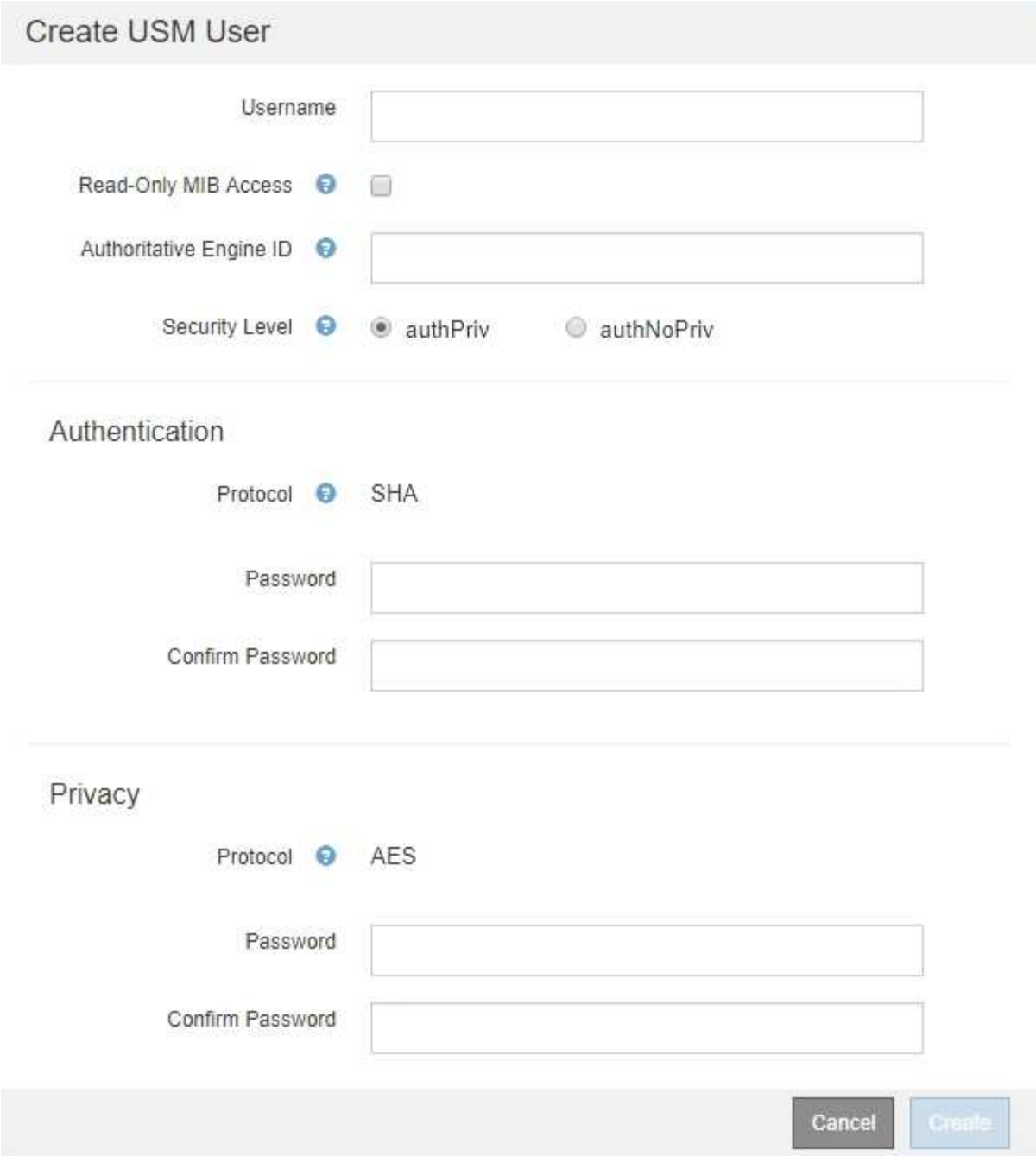
9. Si utiliza SNMPv3, seleccione la pestaña usuarios USM en la sección Other Configurations.

   Use esta pestaña para definir los usuarios USM que están autorizados a consultar el MIB o a recibir capturas e informes.

   > Este paso no se aplica si sólo utiliza SNMPv1 o SNMPv2c.

   a. Haga clic en **Crear**.

      Se muestra el cuadro de diálogo Create USM User.



b. Introduzca un **Nombre de usuario** único para este usuario USM.

   Los nombres de usuario tienen un máximo de 32 caracteres y no pueden contener caracteres en blanco. No se puede cambiar el nombre de usuario una vez creado el usuario.

c. Active la casilla de verificación **acceso MIB de sólo lectura** si este usuario debe tener acceso de sólo lectura a la MIB.

   Si selecciona **acceso MIB de sólo lectura**, el campo **ID de motor autorizado** está desactivado.

   > Los usuarios USM que tengan acceso a MIB de solo lectura no pueden tener ID de motor.

d. Si este usuario se va a utilizar en un destino de informe, introduzca el **ID de motor autorizado** para

este usuario.

> Los destinos de INFORM SNMPv3 deben tener usuarios con ID de motor. El destino de la captura SNMPv3 no puede tener usuarios con ID de motor.

El ID de motor autorizado puede ser de 5 a 32 bytes en hexadecimal.

e. Seleccione un nivel de seguridad para el 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.

f. Introduzca y confirme la contraseña que utilizará este usuario para la autenticación.

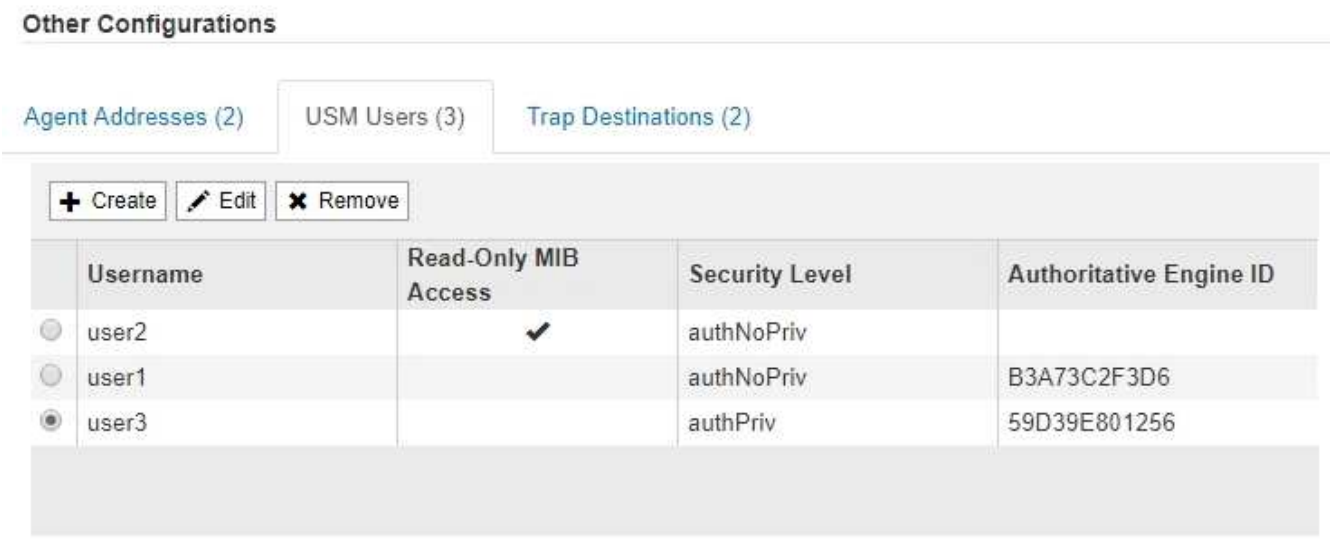
> El único protocolo de autenticación compatible es SHA (HMAC-SHA-96).

g. Si ha seleccionado **authpriv**, introduzca y confirme la contraseña que este usuario utilizará para la privacidad.

> El único protocolo de privacidad compatible es AES.

h. Haga clic en **Crear**.

El usuario USM se crea y se añade a la tabla.

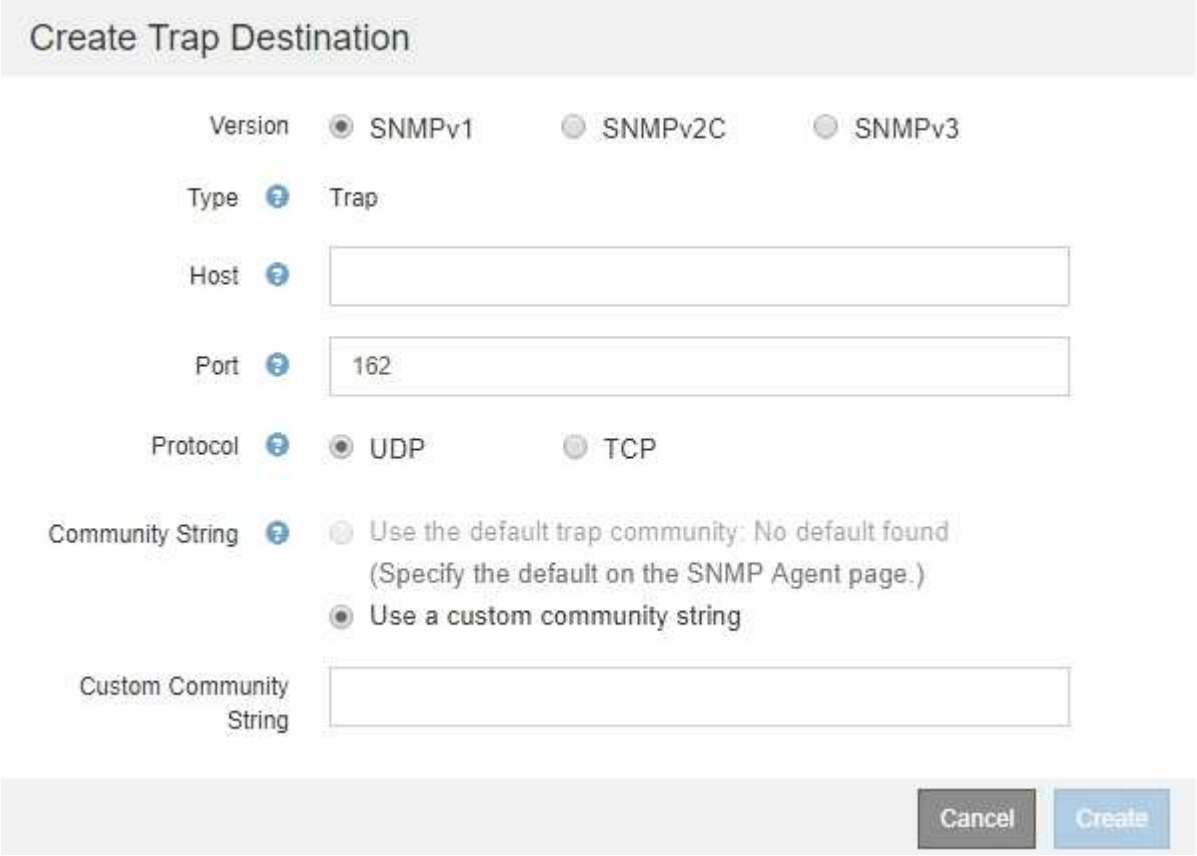


10. en la sección Other Configurations, seleccione la pestaña Trap Destinations.

La pestaña Destinos de captura permite definir uno o varios destinos para las notificaciones de capturas StorageGRID o informar. Al activar el agente SNMP y hacer clic en **Guardar**, StorageGRID comienza a enviar notificaciones a cada destino definido. Las notificaciones se envían cuando se activan alertas y alarmas. También se envían notificaciones estándar para las entidades MIB-II admitidas (por ejemplo, ifdown y coldStart).

a. Haga clic en **Crear**.

Se muestra el cuadro de diálogo Crear destino de captura.



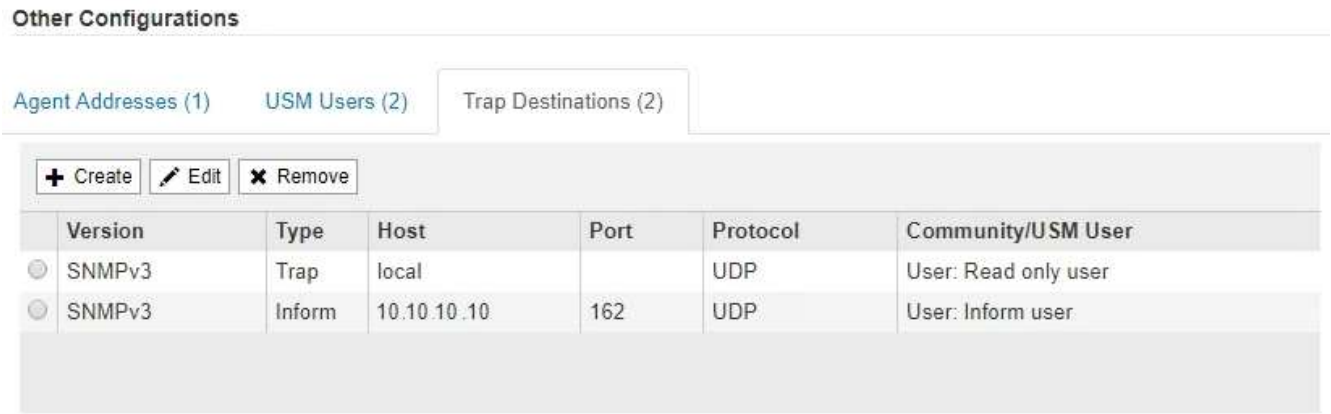
b. En el campo **Versión**, seleccione la versión de SNMP que se utilizará para esta notificación.
c. Complete el formulario en función de la versión seleccionada

Versión	Especifique esta información
SNMPv1	**Nota:** para SNMPv1, el agente SNMP sólo puede enviar capturas. No se admiten los informes. i. En el campo **Host**, introduzca una dirección IPv4 o IPv6 (o FQDN) para recibir la captura. ii. Para **Puerto**, utilice el valor predeterminado (162), a menos que deba utilizar otro valor. (162 es el puerto estándar para las capturas SNMP). iii. Para **Protocolo**, utilice el valor predeterminado (UDP). También admite TCP. (UDP es el protocolo de captura SNMP estándar). iv. Utilice la comunidad de capturas predeterminada, si se especificó una en la página Agente SNMP, 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	i. Seleccione si el destino se utilizará para los solapamientos o para los informes. ii. En el campo **Host**, introduzca una dirección IPv4 o IPv6 (o FQDN) para recibir la captura. iii. Para **Puerto**, utilice el valor predeterminado (162), a menos que deba utilizar otro valor. (162 es el puerto estándar para las capturas SNMP). iv. Para **Protocolo**, utilice el valor predeterminado (UDP). También admite TCP. (UDP es el protocolo de captura SNMP estándar). v. Utilice la comunidad de capturas predeterminada, si se especificó una en la página Agente SNMP, 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.

Versión	Especifique esta información
SNMPv3	i. Seleccione si el destino se utilizará para los solapamientos o para los informes. ii. En el campo **Host**, introduzca una dirección IPv4 o IPv6 (o FQDN) para recibir la captura. iii. Para **Puerto**, utilice el valor predeterminado (162), a menos que deba utilizar otro valor. (162 es el puerto estándar para las capturas SNMP). iv. Para **Protocolo**, utilice el valor predeterminado (UDP). También admite TCP. (UDP es el protocolo de captura SNMP estándar). v. Seleccione el usuario USM que se utilizará 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.

d. Haga clic en **Crear**.

El destino de captura se crea y se añade a la tabla.



11. Cuando haya completado la configuración del agente SNMP, haga clic en **Guardar**

La nueva configuración del agente SNMP se activa.

Información relacionada

Silenciar notificaciones de alerta

Actualice el agente SNMP

Puede que desee deshabilitar las notificaciones SNMP, actualizar cadenas de

comunidad, o añadir o quitar direcciones de agente, usuarios USM y destinos de capturas.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener el permiso acceso raíz.

Acerca de esta tarea

Siempre que actualice Configuración del agente SNMP, Tenga en cuenta que debe hacer clic en **Guardar** en la parte inferior de la página Agente SNMP para confirmar los cambios realizados en cada ficha.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Supervisión** > **Agente SNMP**.

   Aparece la página Agente SNMP.

2. Si desea desactivar el agente SNMP en todos los nodos de cuadrícula, desactive la casilla de verificación **Activar SNMP** y haga clic en **Guardar**.

   El agente SNMP está deshabilitado para todos los nodos de grid. Si después vuelve a habilitar el agente, se conserva cualquier configuración de SNMP anterior.

3. Si lo desea, actualice los valores introducidos para **Contacto del sistema** y **ubicación del sistema**.
4. Opcionalmente, anule la selección de la casilla de verificación **Activar notificaciones de agente SNMP** si ya no desea que el agente SNMP de StorageGRID envíe notificaciones de captura e informe.

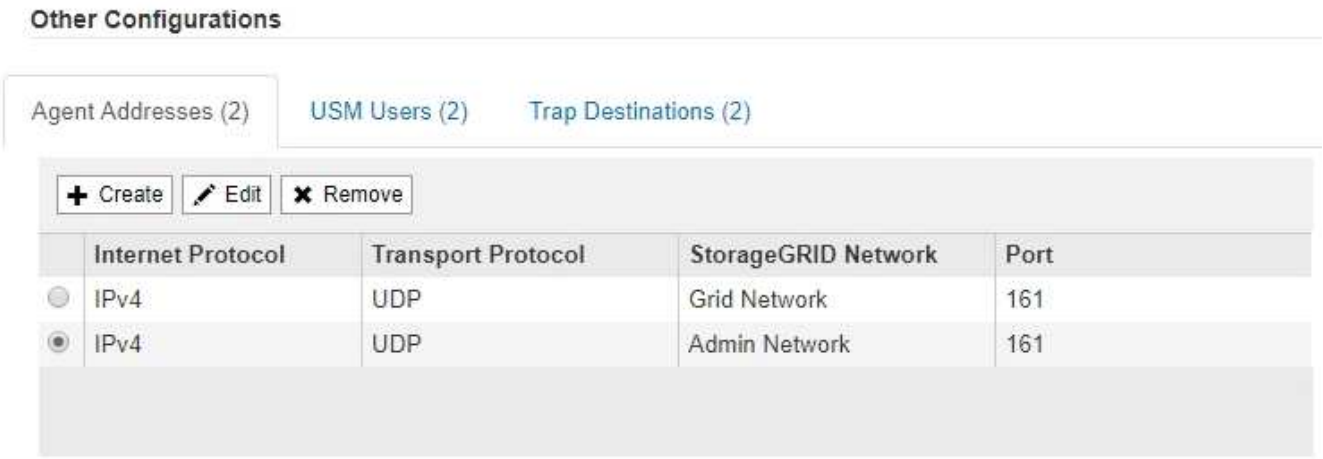
   Cuando esta casilla de verificación está desactivada, el agente SNMP admite acceso MIB de sólo lectura, pero no envía ninguna notificación SNMP.

5. Opcionalmente, anule la selección de la casilla de verificación **Activar capturas de autenticación** si ya no desea que el agente SNMP de StorageGRID envíe una captura de autenticación cuando reciba un mensaje de protocolo autenticado incorrectamente.
6. Si utiliza SNMPv1 o SNMPv2c, puede actualizar opcionalmente la sección Community Strings.

   Los campos de esta sección se utilizan para la autenticación basada en la comunidad en SNMPv1 o SNMPv2c. Estos campos no se aplican a SNMPv3.

   > Si desea quitar la cadena de comunidad predeterminada, primero debe asegurarse de que todos los destinos de capturas utilicen una cadena de comunidad personalizada.

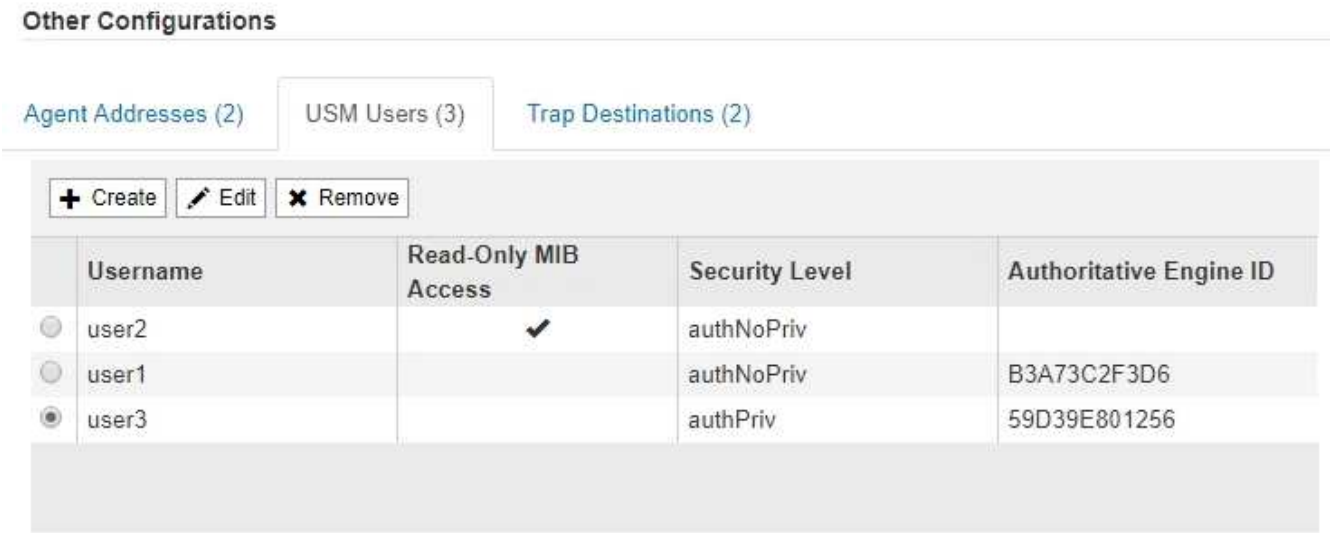
7. Si desea actualizar las direcciones del agente, seleccione la ficha direcciones del agente en la sección otras configuraciones.



Utilice esta pestaña para especificar una o más «'direcciones de escucha'». Éstas son las direcciones StorageGRID en las que el agente SNMP puede recibir consultas. Cada dirección de agente incluye un protocolo de Internet, un protocolo de transporte, una red StorageGRID y un puerto.

a. Para agregar una dirección de agente, haga clic en **Crear**. A continuación, consulte el paso correspondiente a las direcciones del agente en las instrucciones para configurar el agente SNMP.
b. Para editar una dirección de agente, seleccione el botón de opción de la dirección y haga clic en **Editar**. A continuación, consulte el paso correspondiente a las direcciones del agente en las instrucciones para configurar el agente SNMP.
c. Para eliminar una dirección de agente, seleccione el botón de opción de la dirección y haga clic en **Quitar**. A continuación, haga clic en **Aceptar** para confirmar que desea eliminar esta dirección.
d. Para confirmar los cambios, haga clic en **Guardar** en la parte inferior de la página Agente SNMP.

8. Si desea actualizar usuarios de USM, seleccione la pestaña usuarios de USM en la sección Other Configurations.



Use esta pestaña para definir los usuarios USM que están autorizados a consultar el MIB o a recibir capturas e informes.

a. Para añadir un usuario USM, haga clic en **Crear**. A continuación, consulte el paso para los usuarios de USM en las instrucciones para configurar el agente de SNMP.
b. Para editar un usuario USM, seleccione el botón de opción del usuario y haga clic en **Editar**. A

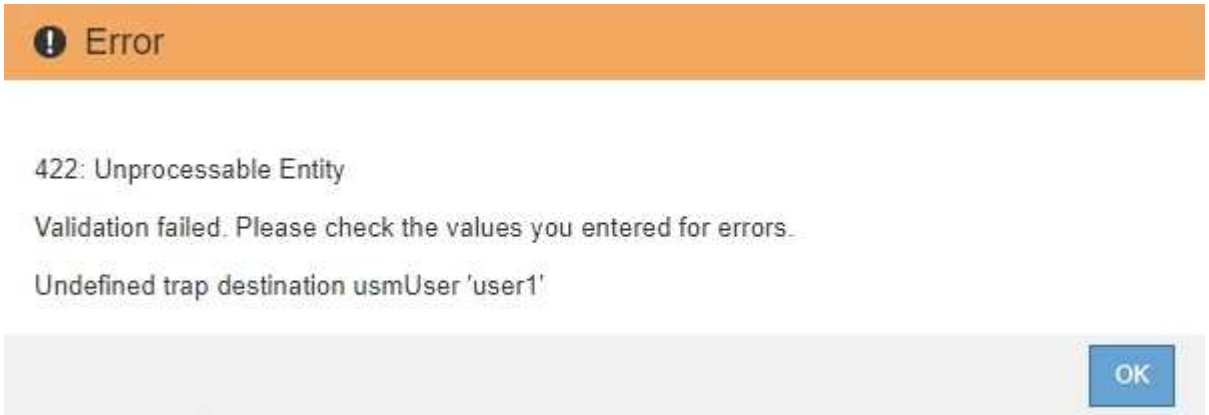
continuación, consulte el paso para los usuarios de USM en las instrucciones para configurar el agente de SNMP.

El nombre de usuario de un usuario USM existente no se puede cambiar. Si necesita cambiar un nombre de usuario, debe eliminar el usuario y crear uno nuevo.

> Si agrega o quita un identificador de motor autorizado de un usuario y ese usuario está seleccionado actualmente para un destino, debe editar o quitar el destino, como se describe en el paso Destino de capturas SNMP. De lo contrario, se produce un error de validación al guardar la configuración del agente SNMP.

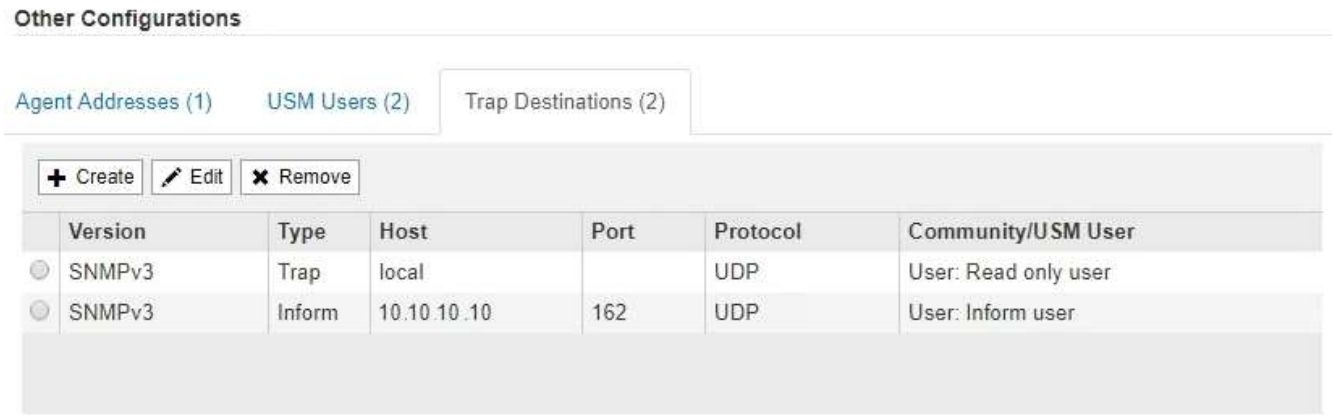
c. Para eliminar un usuario USM, seleccione el botón de opción del usuario y haga clic en **Quitar**. A continuación, haga clic en **Aceptar** para confirmar que desea eliminar este usuario.

> Si el usuario que quitó está actualmente seleccionado para un destino de captura, debe editar o quitar el destino, como se describe en el paso Destino de capturas SNMP. De lo contrario, se produce un error de validación al guardar la configuración del agente SNMP.



a. Para confirmar los cambios, haga clic en **Guardar** en la parte inferior de la página Agente SNMP.

9. Si desea actualizar los destinos de capturas, seleccione la pestaña Destinos de captura en la sección otras configuraciones.



La pestaña Destinos de captura permite definir uno o varios destinos para las notificaciones de capturas StorageGRID o informar. Al activar el agente SNMP y hacer clic en **Guardar**, StorageGRID comienza a enviar notificaciones a cada destino definido. Las notificaciones se envían cuando se activan alertas y alarmas. También se envían notificaciones estándar para las entidades MIB-II admitidas (por ejemplo,

ifdown y coldStart).

a. Para agregar un destino de captura, haga clic en **Crear**. A continuación, consulte el paso para los destinos de capturas en las instrucciones para configurar el agente SNMP.
b. Para editar un destino de captura, seleccione el botón de opción del usuario y haga clic en **Editar**. A continuación, consulte el paso para los destinos de capturas en las instrucciones para configurar el agente SNMP.
c. Para eliminar un destino de captura, seleccione el botón de opción del destino y haga clic en **Quitar**. A continuación, haga clic en **Aceptar** para confirmar que desea eliminar este destino.
d. Para confirmar los cambios, haga clic en **Guardar** en la parte inferior de la página Agente SNMP.

10. Cuando haya actualizado la configuración del agente SNMP, haga clic en **Guardar**.

Recopilación de datos de StorageGRID adicionales

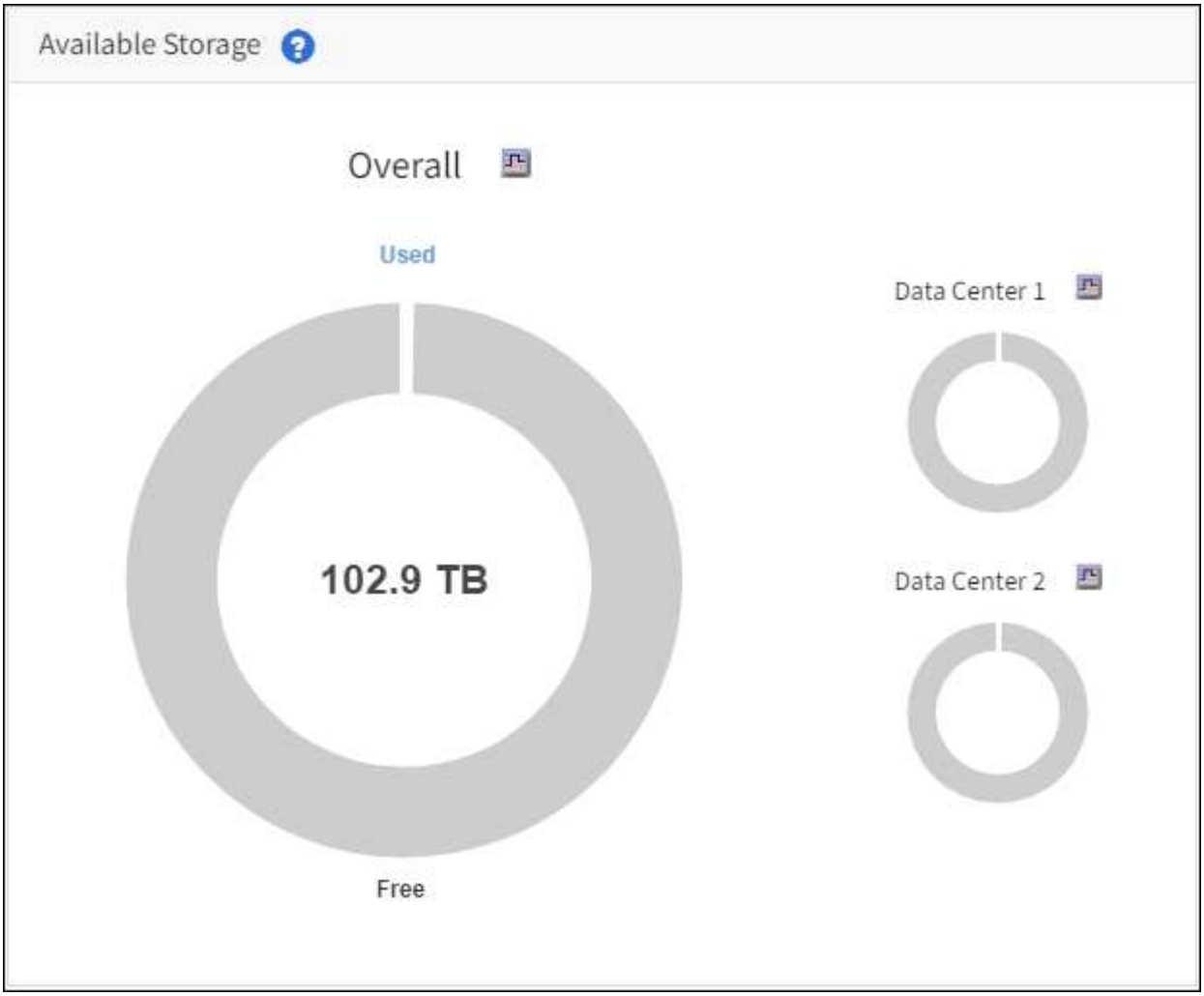
Utilice gráficos y gráficos

Puede utilizar gráficos e informes para supervisar el estado del sistema StorageGRID y solucionar problemas. Los tipos de gráficos e informes disponibles en Grid Manager incluyen gráficos de anillos (sólo en el Panel), gráficos e informes de texto.

Tipos de gráficos

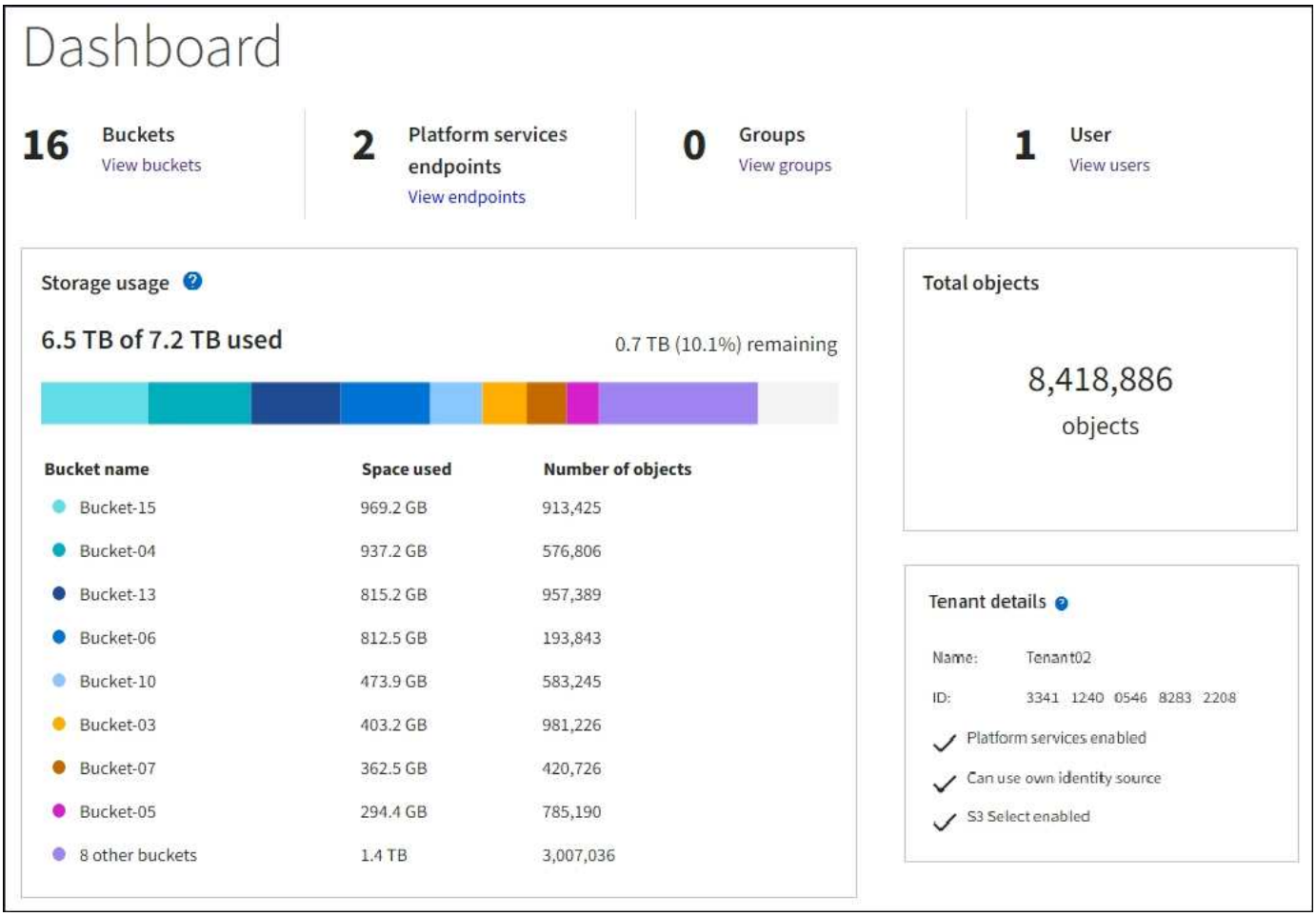
Los gráficos y los gráficos resumen los valores de métricas y atributos de StorageGRID específicos.

El Panel de Grid Manager incluye gráficos de anillos para resumir el almacenamiento disponible para la cuadrícula y cada sitio.



El panel de uso del almacenamiento de la consola de tenant Manager muestra lo siguiente:

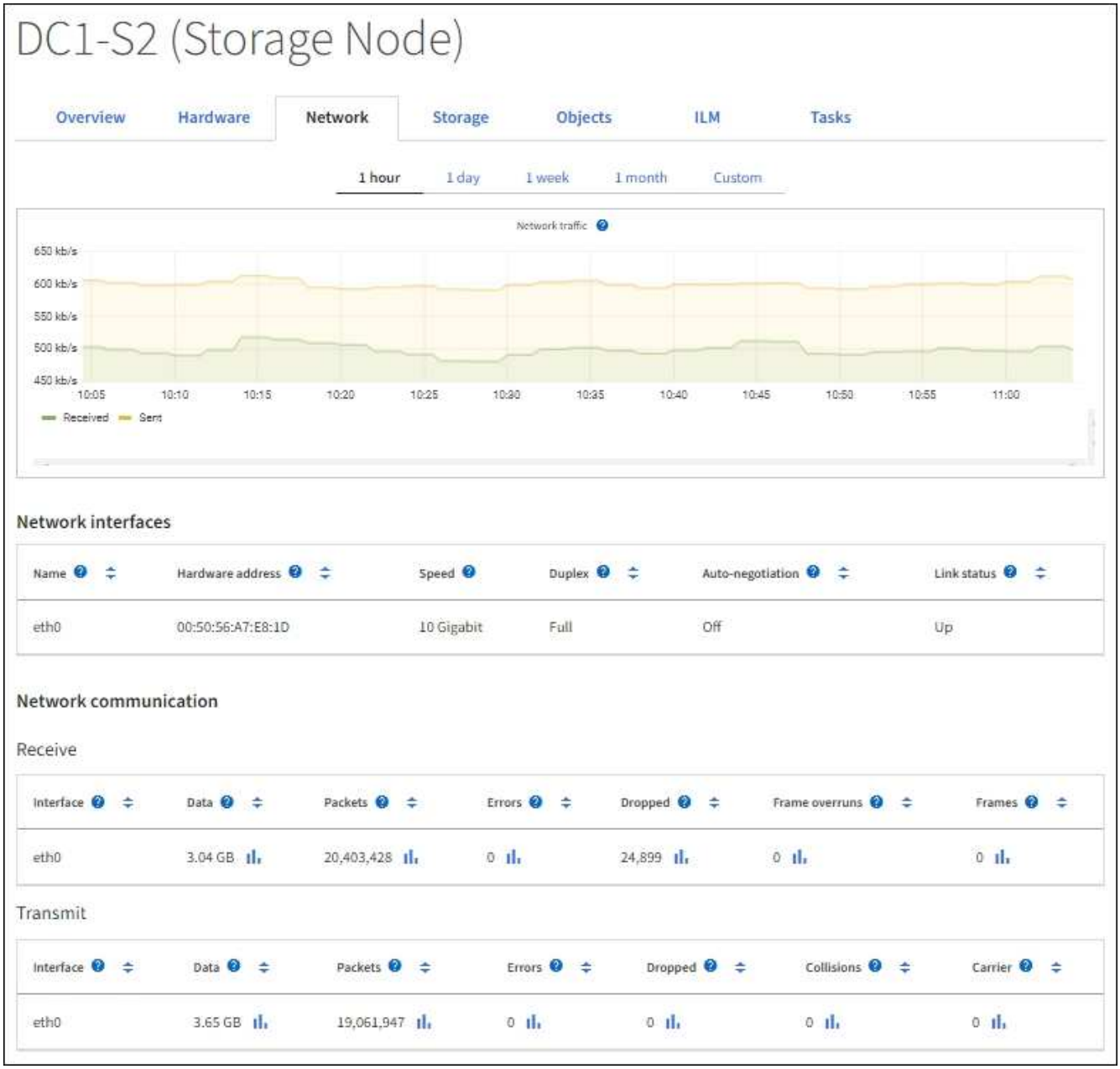
- Una lista de los bloques más grandes (S3) o los contenedores (Swift) para el inquilino
- Un gráfico de barras que representa los tamaños relativos de los cubos o contenedores más grandes
- La cantidad total de espacio utilizado y, si se establece una cuota, la cantidad y el porcentaje de espacio restante



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**.

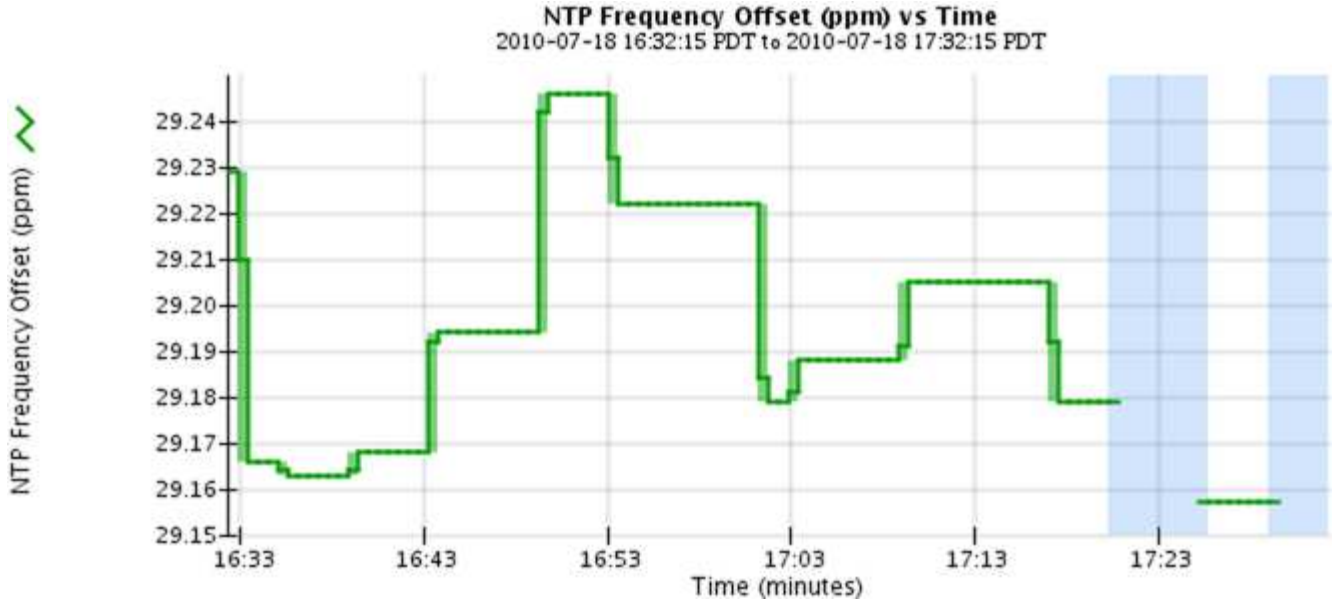
Existen cuatro tipos de gráficos:

- * 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.

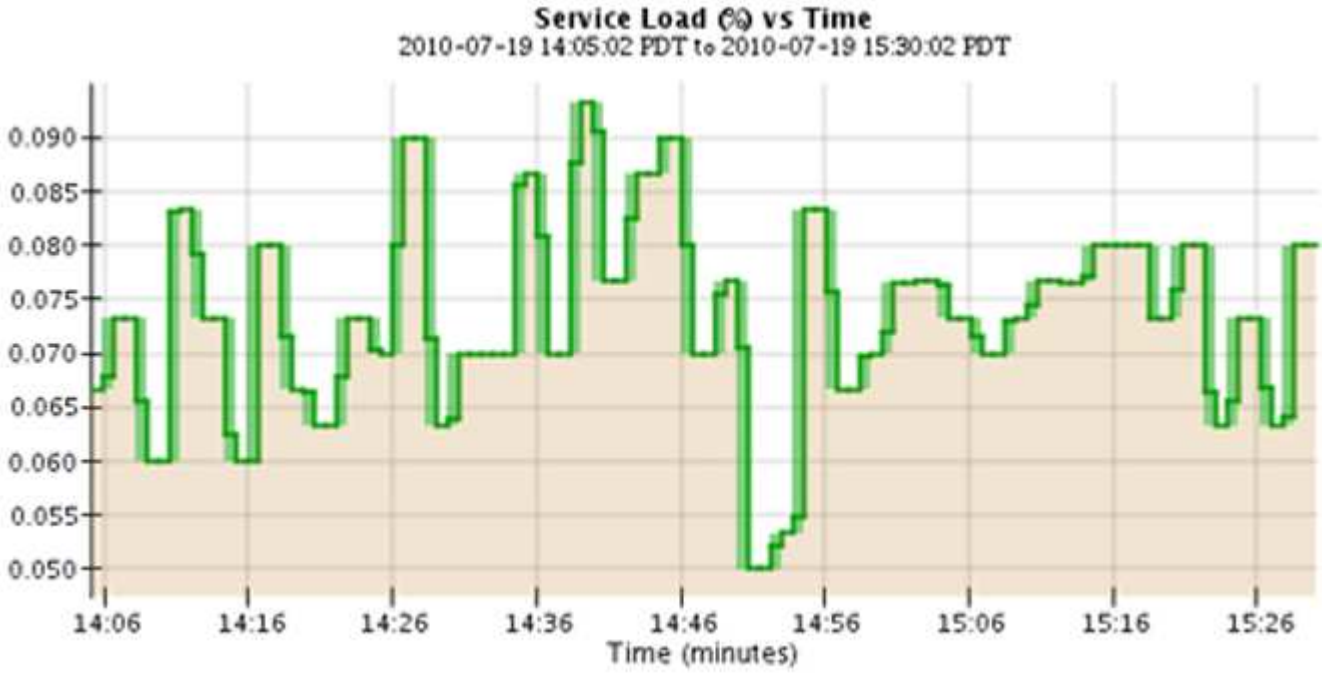


Los gráficos Grafana también se incluyen en los paneles preconstruidos disponibles en la página **SUPPORT** > **Tools** > **Metrics**.

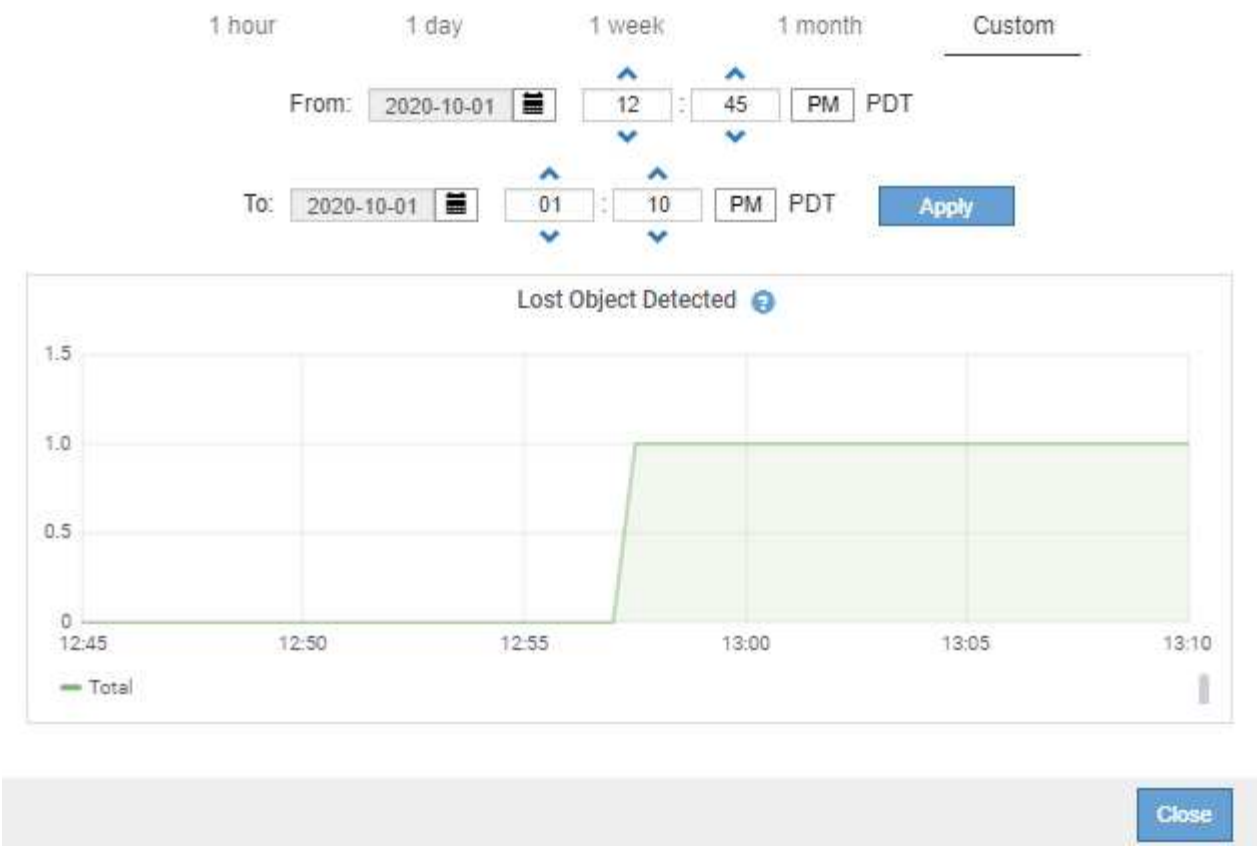
- **Gráficos de líneas**: Disponible en la página Nodes y en la página **SUPPORT** > **Tools** > **Topología de cuadrícula** (seleccione el icono de gráfico Después de un valor de datos), los gráficos de líneas se utilizan para trazar los valores de los atributos StorageGRID que tienen un valor de unidad (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.



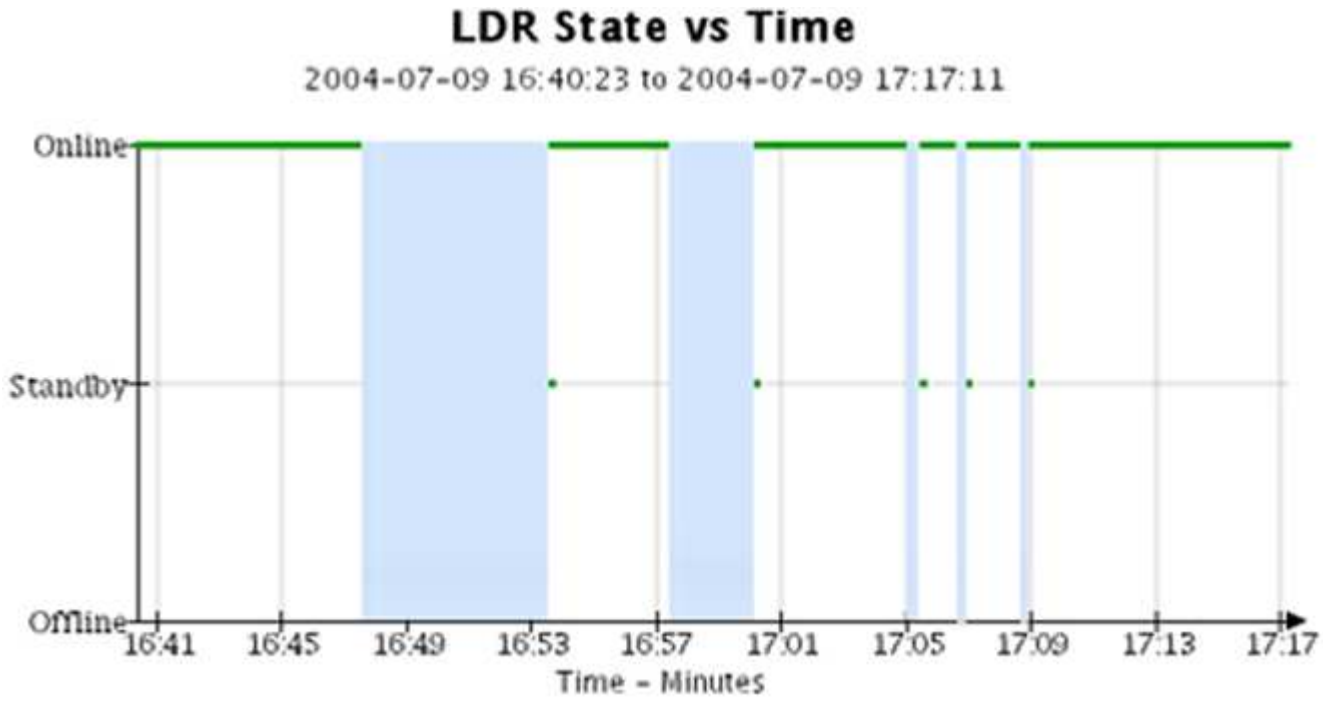
- **Gráficos de área**: Disponible en la página Nodes y en la página **SUPPORT** > **Tools** > **Grid topolog** (seleccione el icono del gráfico) después de un valor de datos), los gráficos de área se utilizan para trazar cantidades de atributos volumétricos, como recuentos de objetos o valores de carga 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

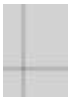
Vea la página Nodes

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.

Muestra	Significado
	Los valores de atributo reportados se trazan utilizando líneas verdes oscuras.
	El sombreado verde claro alrededor de las líneas verdes oscuras indica que los valores reales de ese intervalo de tiempo varían y han sido "'binados'" 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.

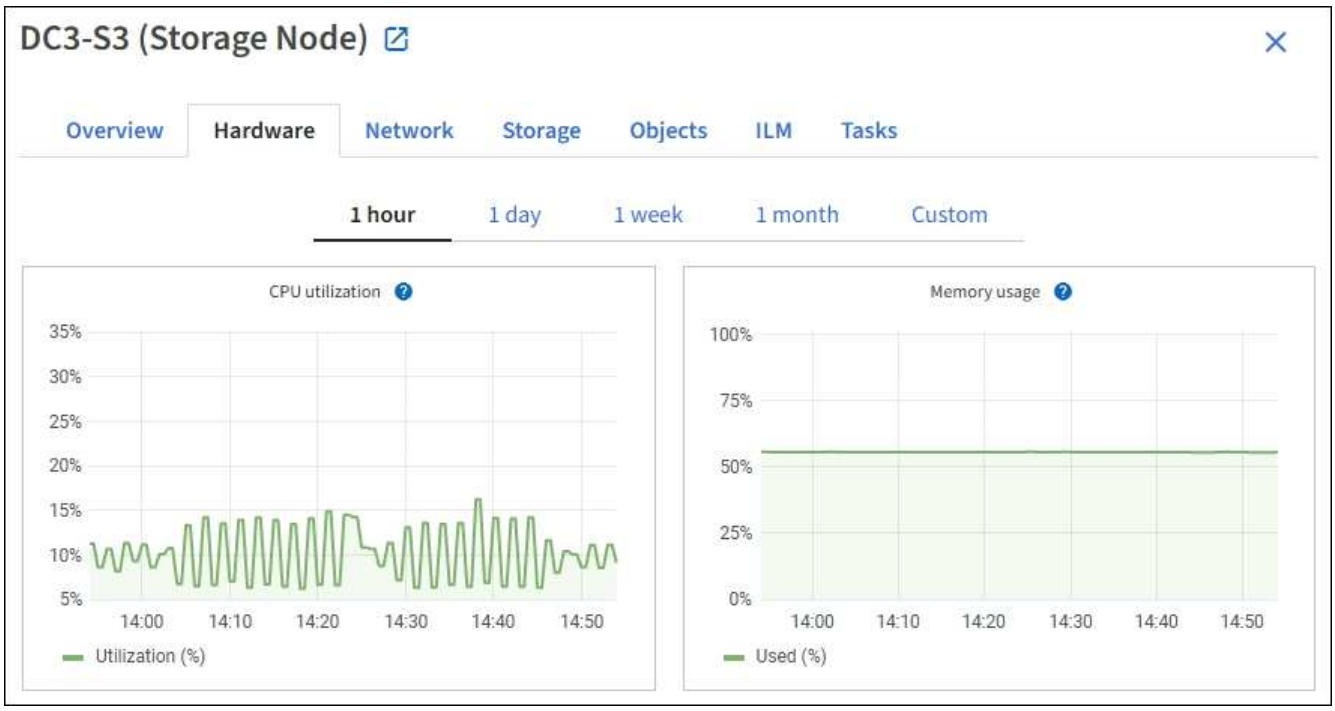
Lo que necesitará

Debe iniciar sesión en Grid Manager mediante un navegador web compatible.

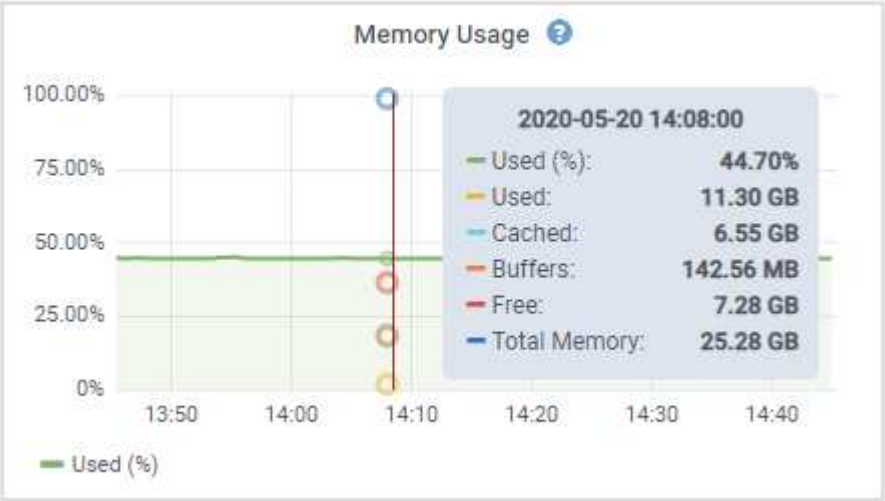
Pasos

1. Seleccione **NODES**. 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. De manera opcional, pase el cursor sobre el gráfico para ver valores más detallados de un momento específico.

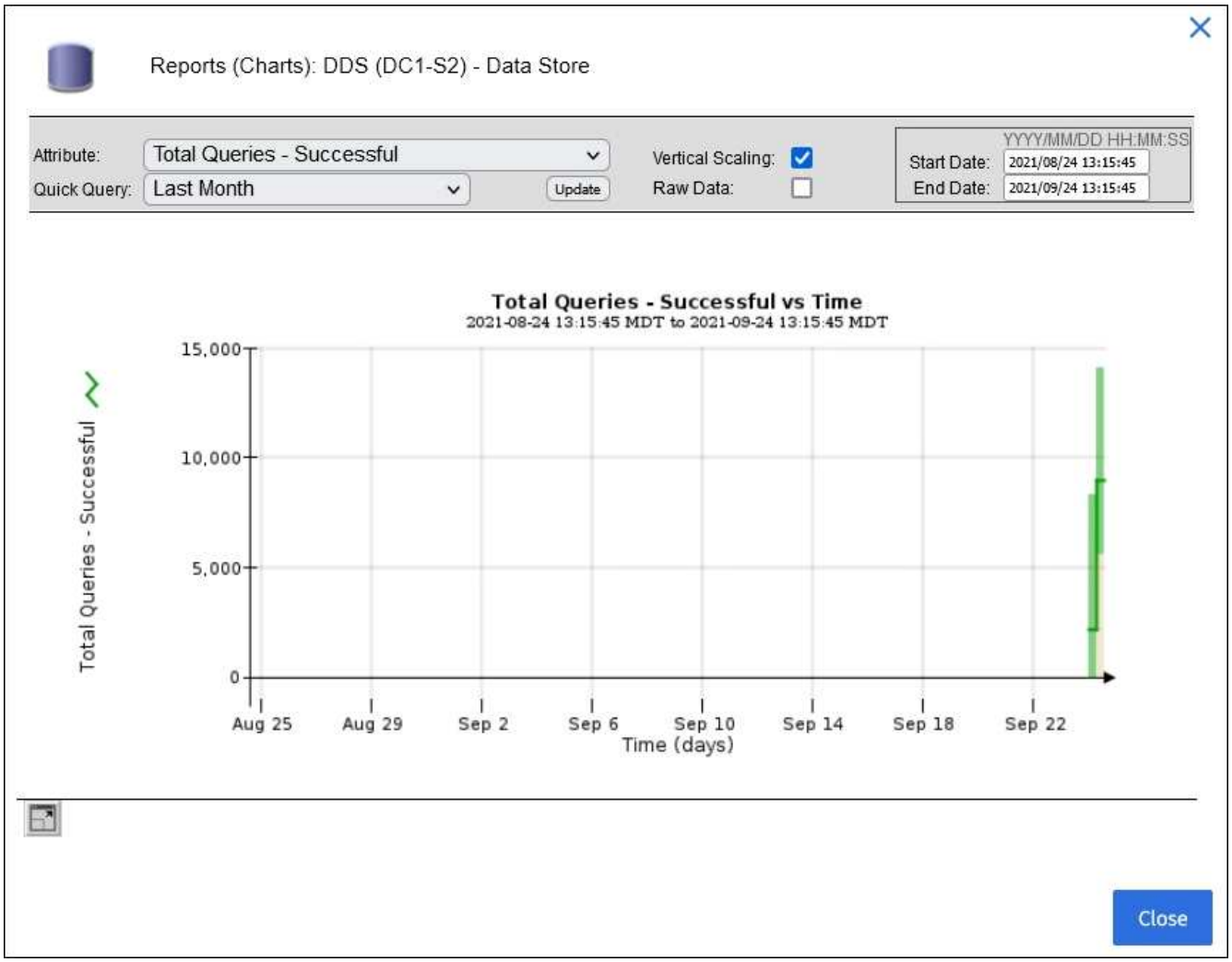


4. Según sea necesario, a menudo puede mostrar un gráfico para un atributo o métrica específicos. En la tabla de la página Nodes, seleccione el icono del gráfico a la derecha del nombre del atributo.

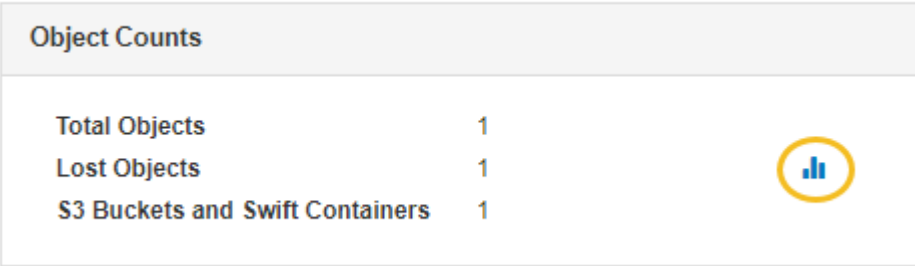
Los gráficos no están disponibles para todas las métricas y atributos.

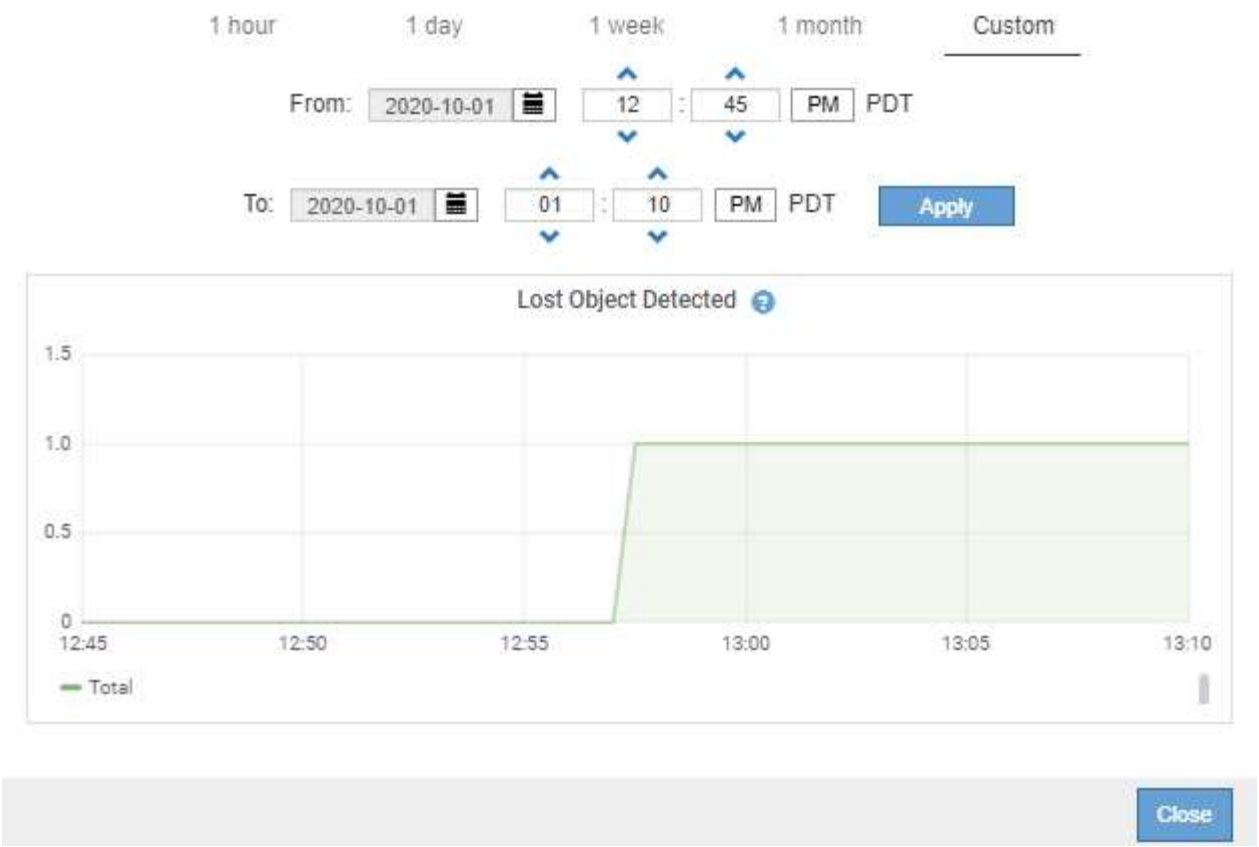
Ejemplo 1: En la ficha objetos de un nodo de almacenamiento, puede seleccionar el icono del gráfico Para ver el número total de consultas correctas del almacén de metadatos para el nodo de almacenamiento.

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

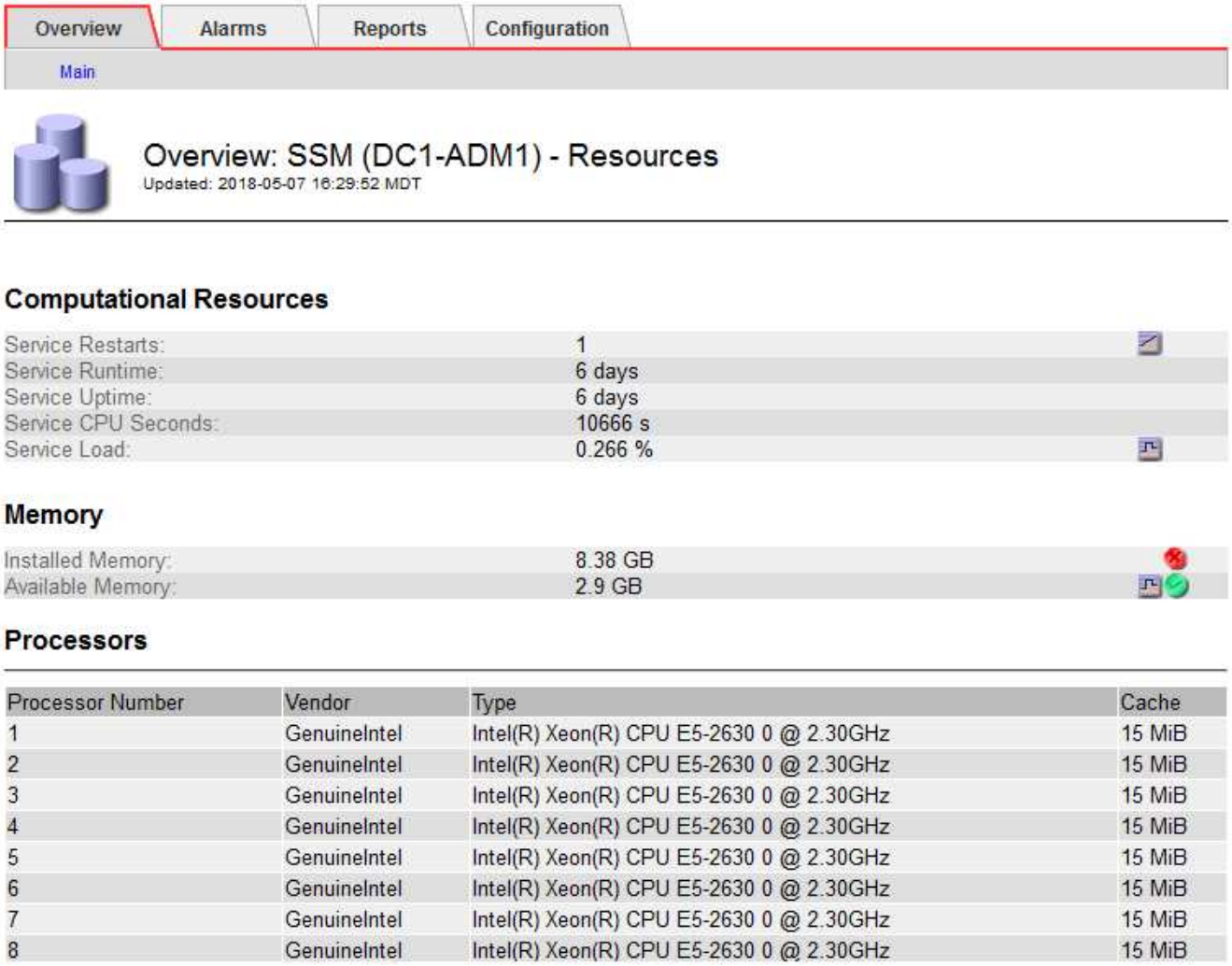


Ejemplo 2: En la ficha objetos de un nodo de almacenamiento, puede seleccionar el icono del gráfico Para ver el gráfico Grafana del número de objetos perdidos detectados con el tiempo.





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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener 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 el inicio del eje y a cero, desactive la casilla de verificación **escala vertical**.
5. Para mostrar valores con precisión completa, active la casilla de verificación **datos sin procesar** o

redondear valores a un máximo de tres posiciones decimales (por ejemplo, para los atributos informados 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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener 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 decimales (por ejemplo, para los atributos notificados como porcentajes), anule la selección de la casilla de verificación **datos brutos** .
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

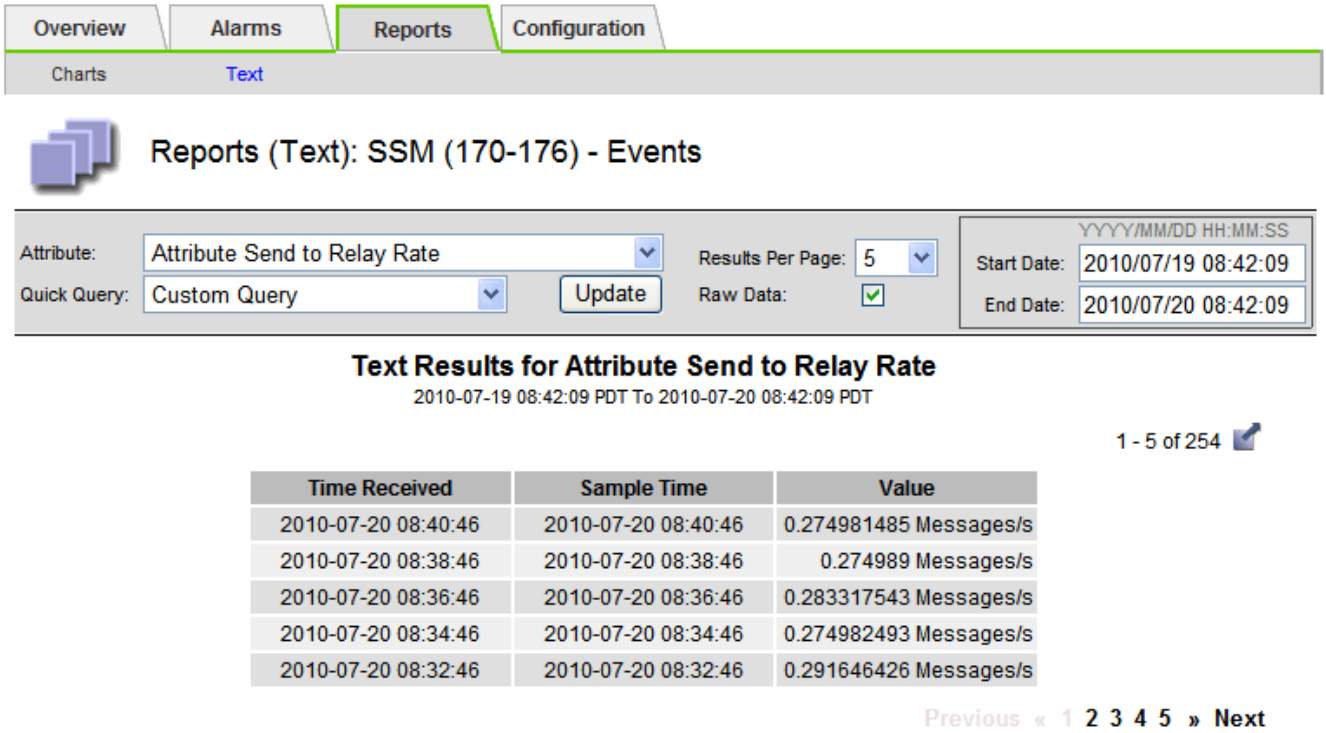
Los informes de texto exportados abren una nueva pestaña del navegador, que permite seleccionar y copiar los datos.

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: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
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 con regularidad y registre los resultados,

para que pueda identificar tendencias que puedan 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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener los permisos 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 dañado no identificado** se activa si el sistema detecta un objeto dañado 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.

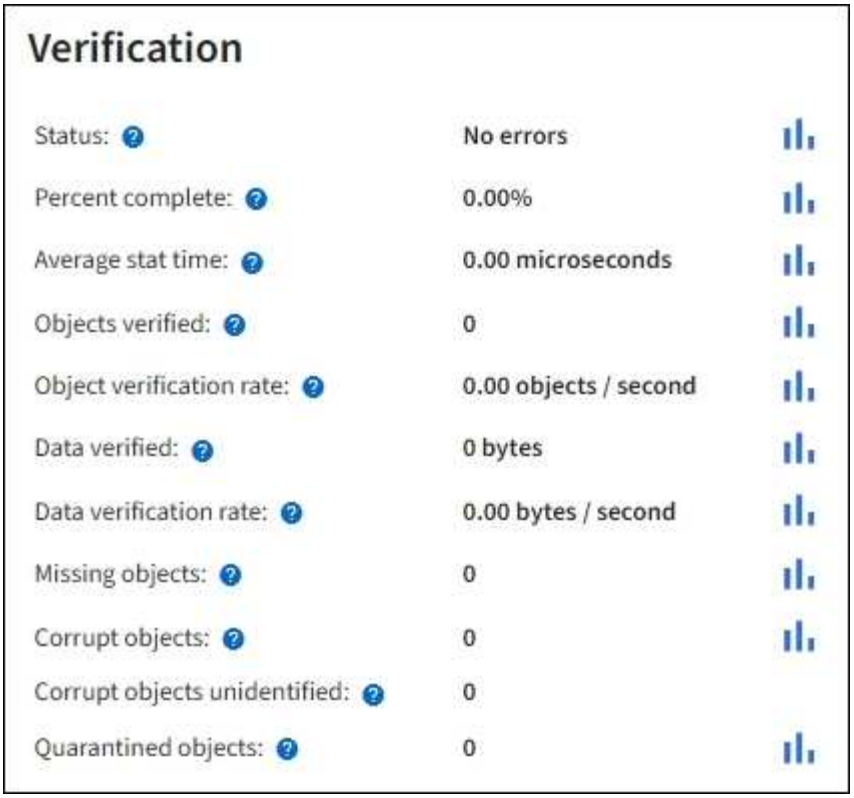
Pasos

1. Revise los resultados de las verificaciones de fondo:

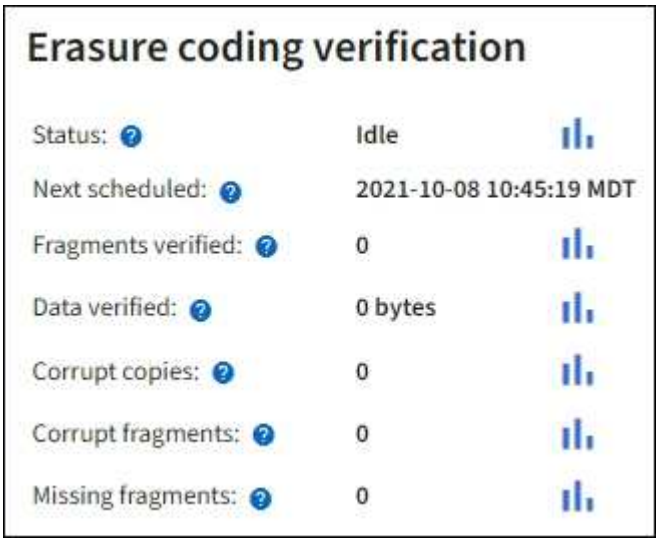
   a. Seleccione **NODES** > ***Storage Node*** > **Objects**.

   b. Compruebe los resultados de verificación:

      - Para comprobar la verificación de datos de objetos replicados, observe los atributos de la sección verificación.

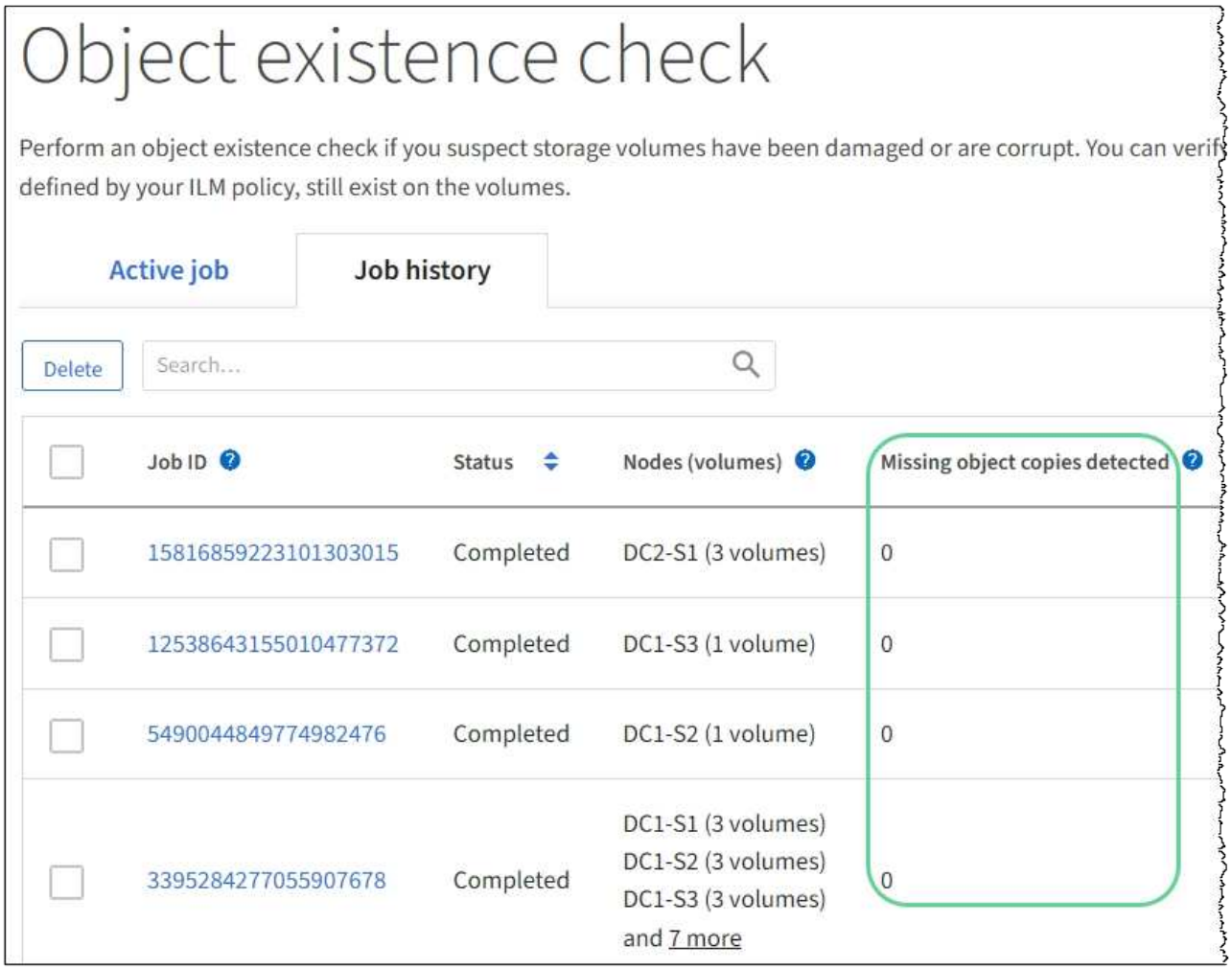


- Para comprobar la verificación de fragmentos codificados por borrado, seleccione ***Storage Node*** > **ILM** y observe los atributos de la sección verificación de códigos de borrado.



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 da como resultado que falten 100 o más copias de objetos y el Los objetos perdieron la alerta se ha activado, 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 acerca de 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**.

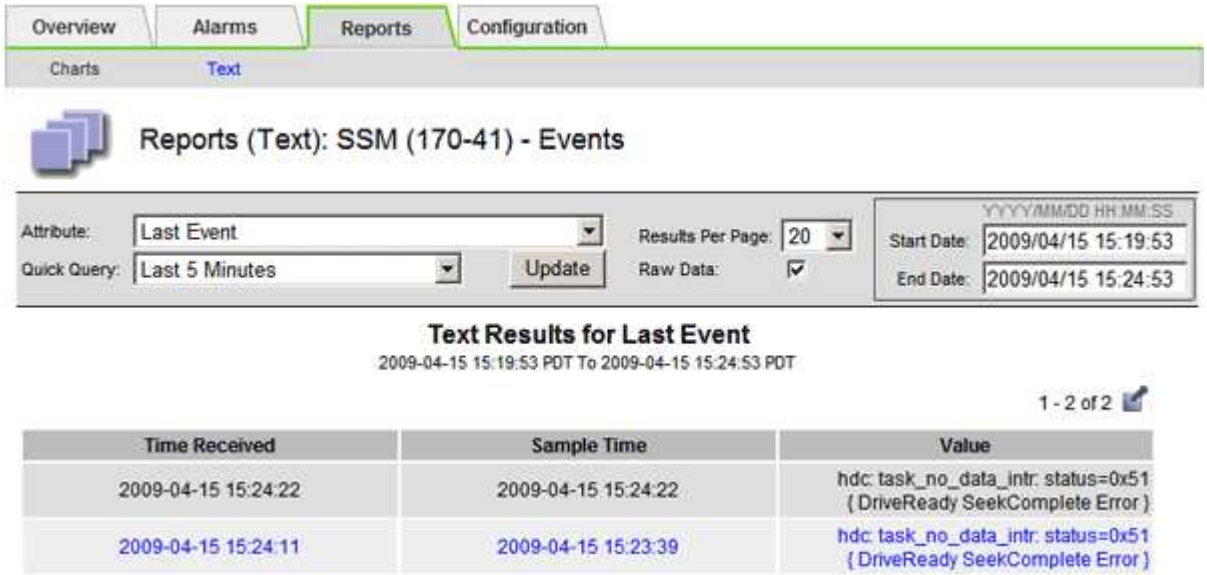
c. Seleccione **texto**.

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.

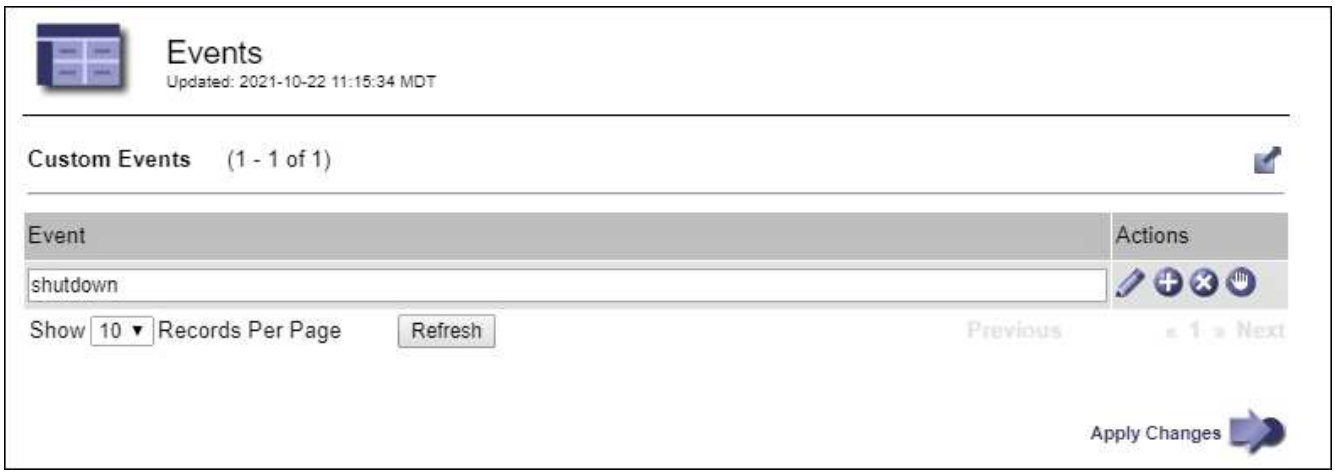
- Después de crear un evento personalizado, se supervisa cada incidencia de él.
- Para crear un evento personalizado basado en palabras clave de `/var/local/log/messages` los registros de dichos archivos deben ser:
  - Generado por el núcleo
  - Generado por daemon o programa de usuario en el nivel de 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

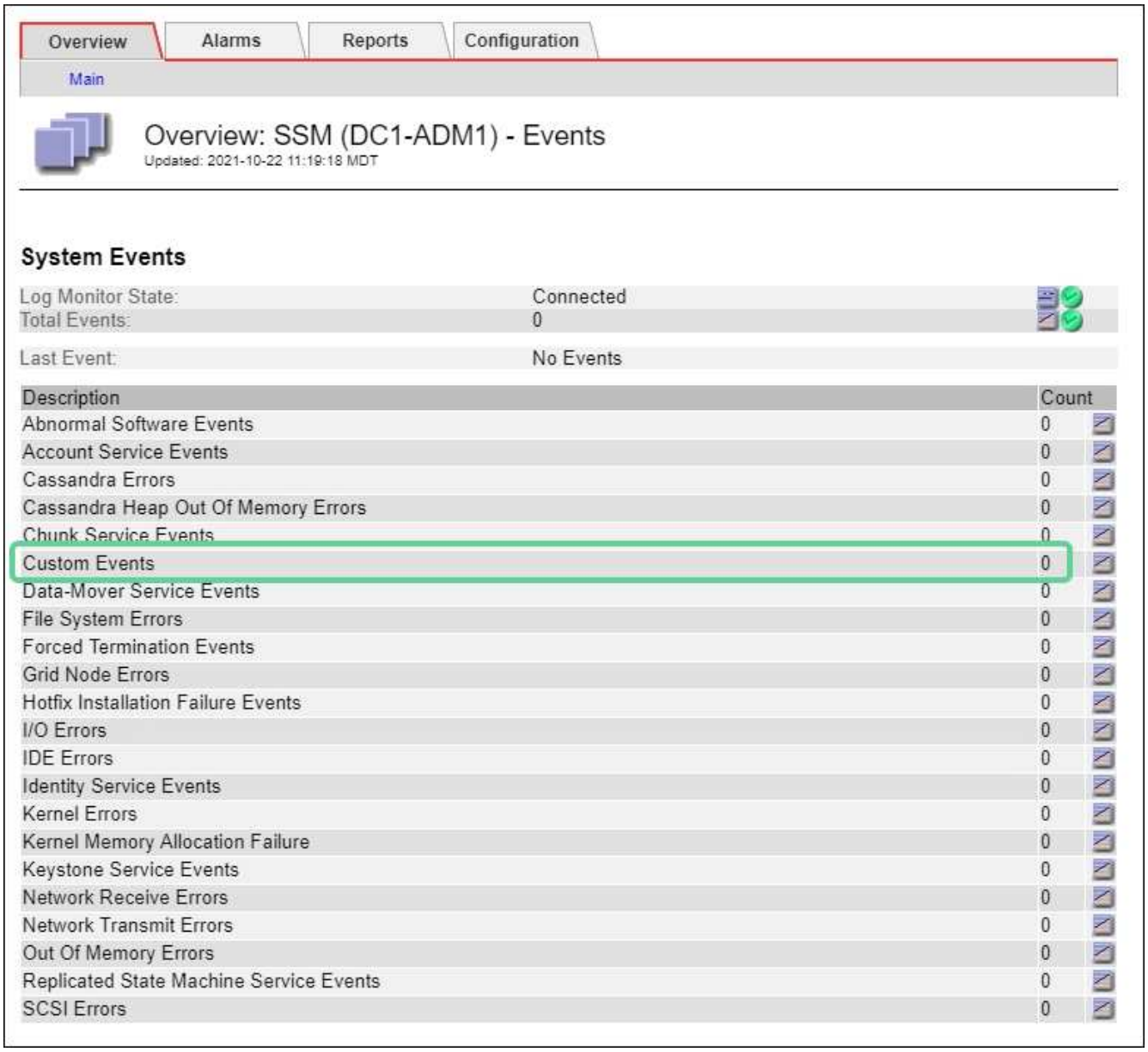
1. Seleccione **SUPPORT** > **Alarms (Legacy)** > **Eventos personalizados**.

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.



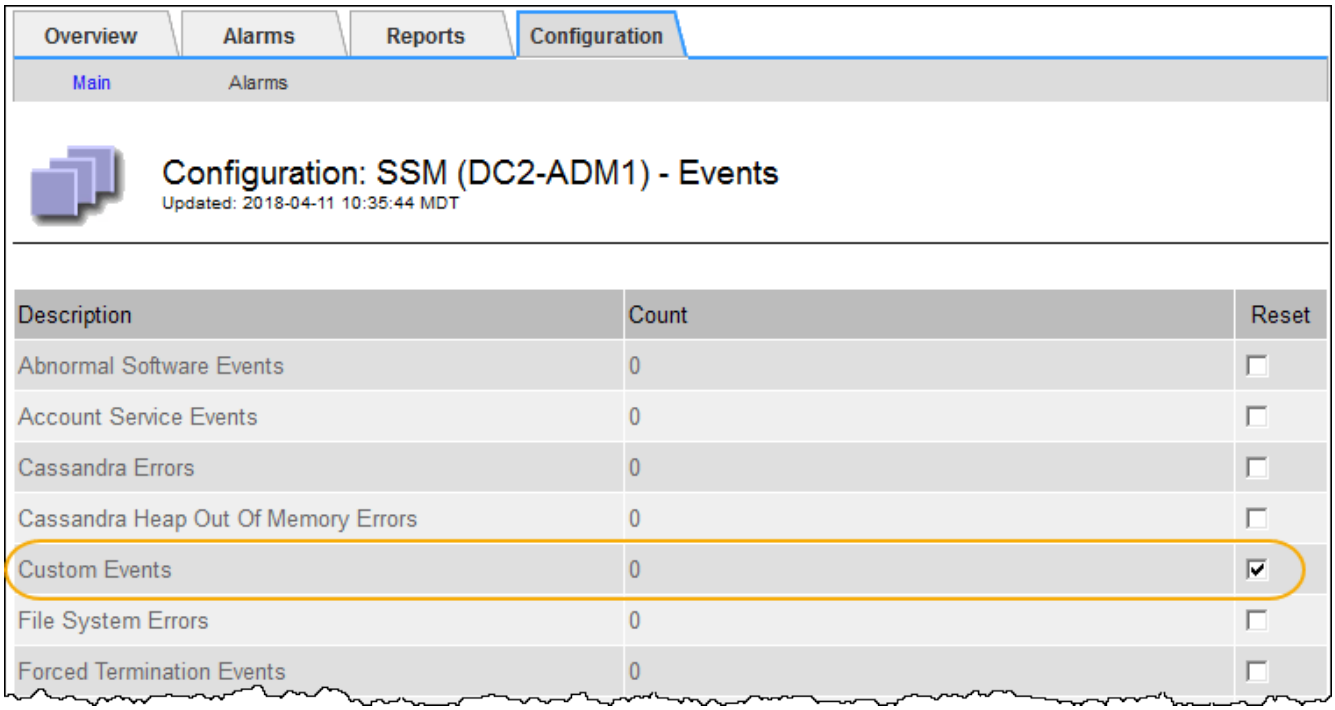
Restablece el número de eventos personalizados a cero

Si desea restablecer el contador solo para eventos personalizados, debe usar la página Grid Topology del menú de soporte.

Acerca de esta tarea

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.

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***grid node*** > **SSM** > **Eventos** > **Configuración** > **Principal**.
3. Seleccione la casilla de verificación **Restablecer** 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, es posible configurar el acceso de clientes al recurso compartido de auditoría para NFS y CIFS (CIFS está obsoleto). 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 que se encuentran disponibles para analizar los mensajes de auditoría, consulte las instrucciones para los mensajes de auditoría. Para obtener más información sobre cómo configurar el acceso de cliente de auditoría, consulte las instrucciones para administrar StorageGRID.

Información relacionada

Revisar los registros de auditoría

Administre StorageGRID

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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener permisos de acceso específicos.
- Debe tener la clave de acceso de aprovisionamiento.

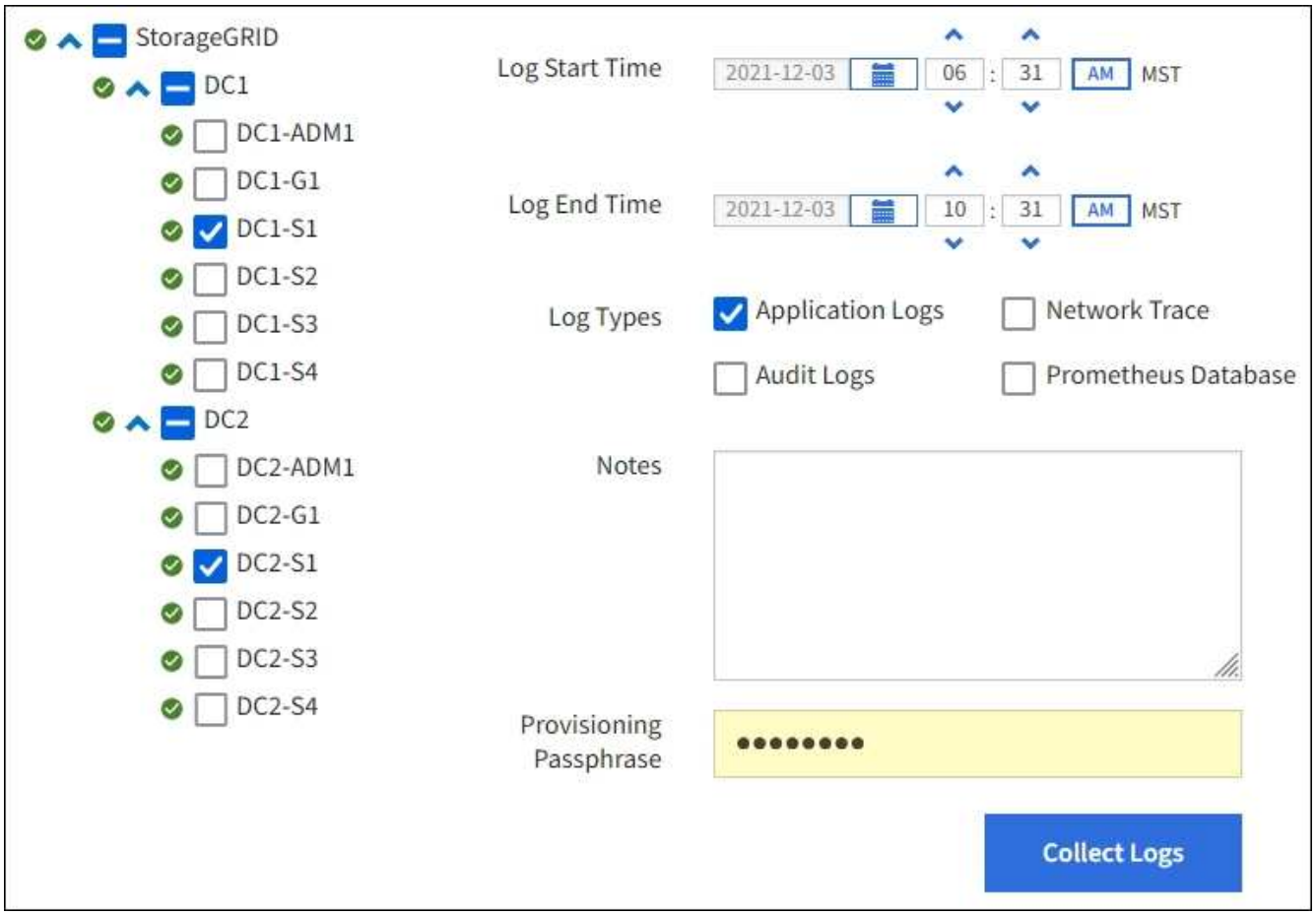
Acerca de esta tarea

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 mensaje de AutoSupport

Con el fin de ayudar al soporte técnico a solucionar problemas con su sistema StorageGRID, puede activar manualmente el envío de un mensaje de AutoSupport.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener el permiso acceso raíz u otra configuración de cuadrícula.

Pasos

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

   Aparece la página AutoSupport con la ficha **Configuración** seleccionada.

2. Seleccione **Enviar AutoSupport desencadenado por el usuario**.

   StorageGRID intenta enviar un mensaje de AutoSupport al soporte técnico. Si el intento se realiza correctamente, se actualizan los valores **resultado más reciente** y **tiempo más reciente** de la ficha **resultados**. Si hay algún problema, el valor del **resultado más reciente** se actualiza a "error" y StorageGRID no intenta volver a enviar el mensaje AutoSupport.

Después de enviar un mensaje AutoSupport activado por el usuario, actualice la página AutoSupport en el explorador después de 1 minuto para acceder a los resultados más recientes.

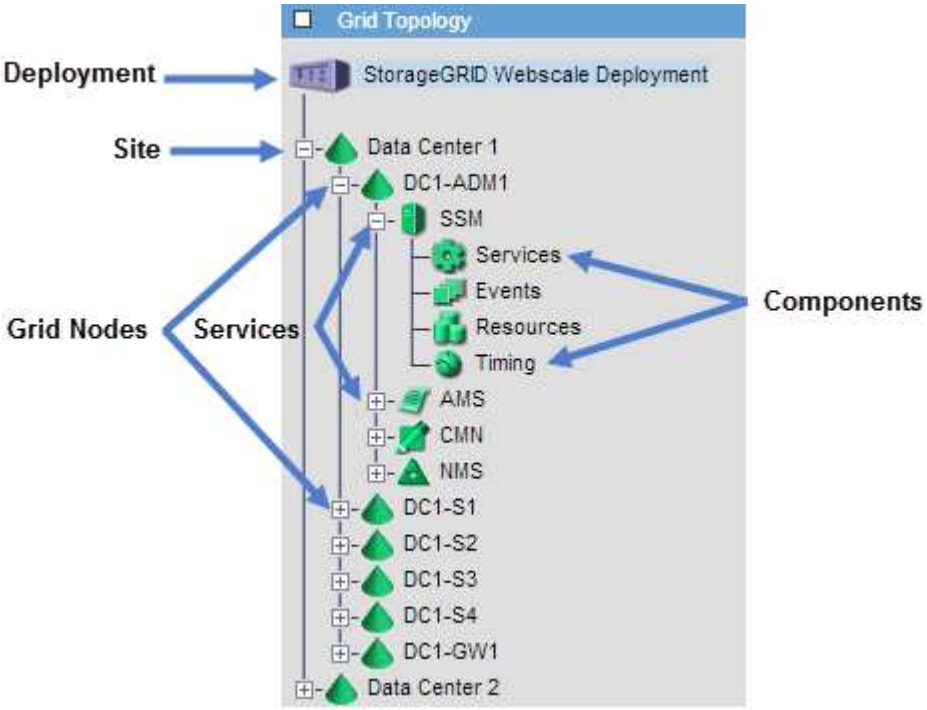
Información relacionada

Configurar los ajustes del servidor de correo electrónico para las alarmas (sistema heredado)

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.

Revisar las métricas de soporte

Al solucionar problemas, puede trabajar con el soporte técnico para revisar métricas y gráficos detallados para su sistema StorageGRID.

Lo que necesitará

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

Acerca de esta tarea

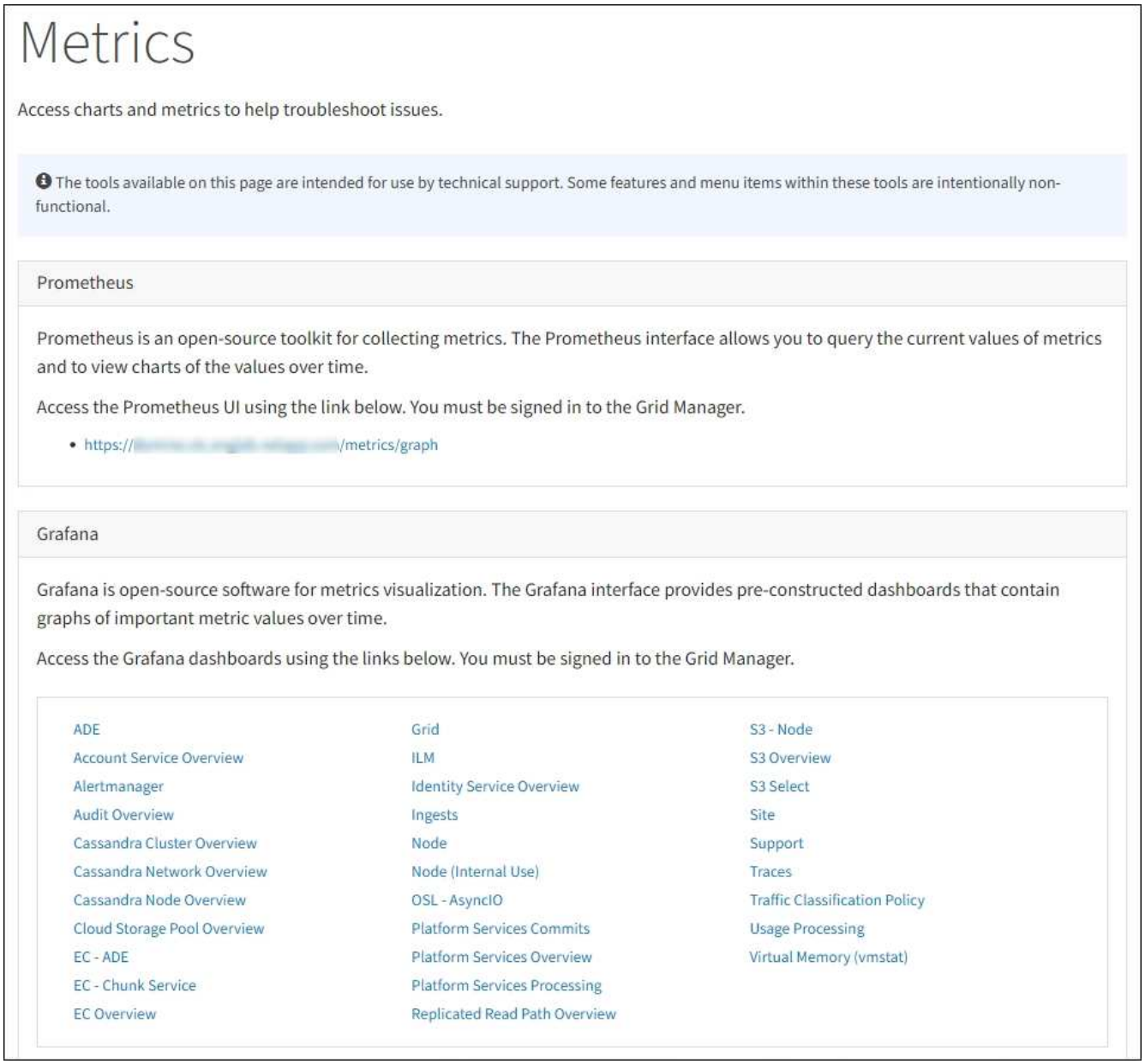
La página Metrics le permite acceder a las interfaces de usuario Prometheus y Grafana. Prometheus es un software de código abierto para recopilar métricas. Grafana es un software de código abierto para la visualización de métricas.

> 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

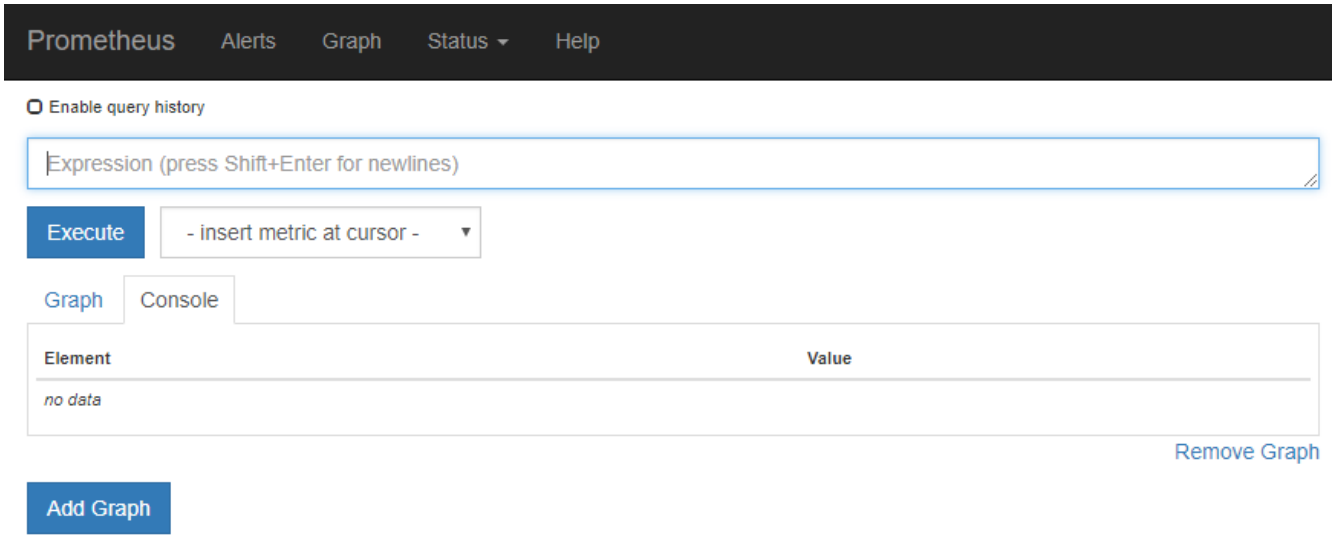
1. Según lo indicado por el soporte técnico, seleccione **ASISTENCIA** > **Herramientas** > **métricas**.

   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

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene 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.

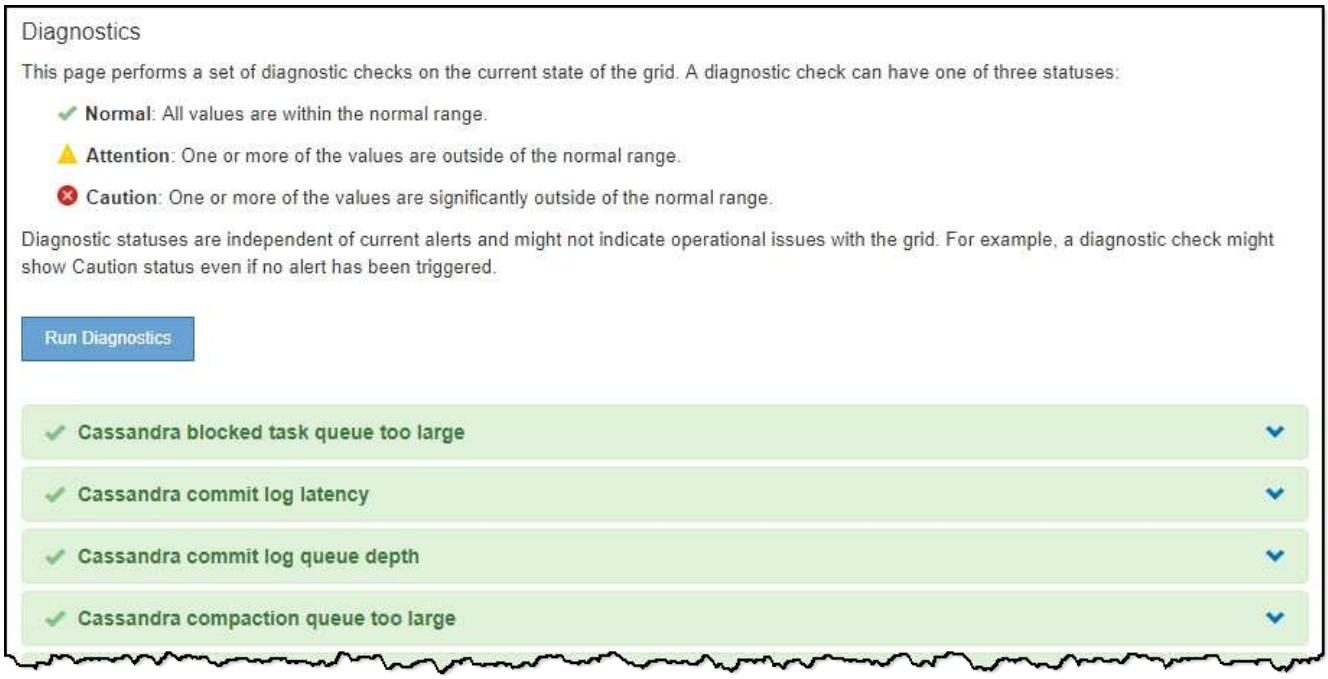
Los Estados de diagnóstico son independientes de las alertas actuales y podrían no indicar problemas operativos con la cuadrícula. Por ejemplo, una comprobación de diagnóstico puede mostrar el estado Precaución aunque no se haya activado ninguna alerta.

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.

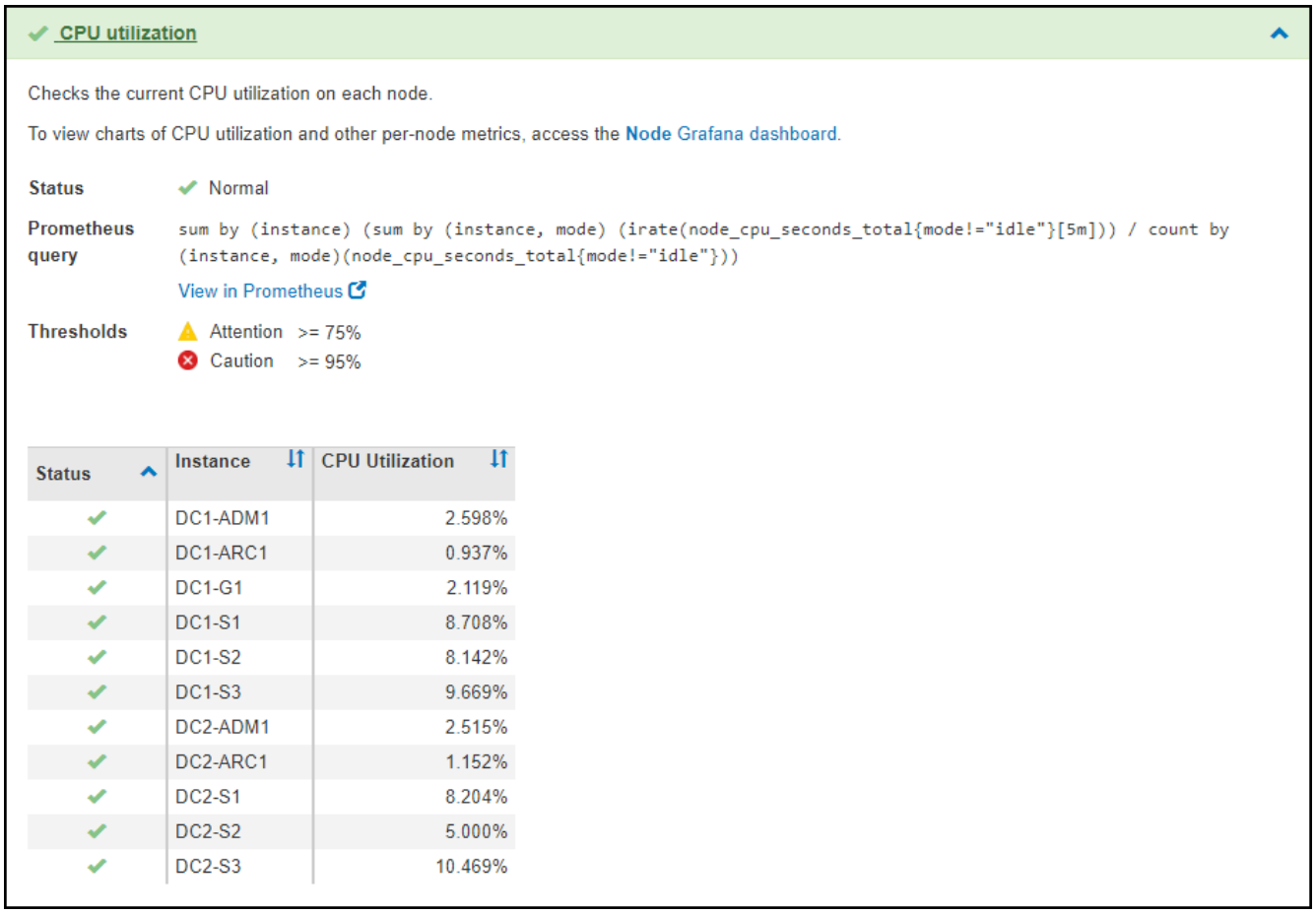
   Aparecen detalles sobre el diagnóstico y sus resultados actuales. Se enumeran los siguientes detalles:

   - **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 es posible 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.



Status	Instance	CPU Utilization
✔	DC1-ADM1	2.598%
✔	DC1-ARC1	0.937%
✔	DC1-G1	2.119%
✔	DC1-S1	8.708%
✔	DC1-S2	8.142%
✔	DC1-S3	9.669%
✔	DC2-ADM1	2.515%
✔	DC2-ARC1	1.152%
✔	DC2-S1	8.204%
✔	DC2-S2	5.000%
✔	DC2-S3	10.469%

3. **Opcional**: Para ver los gráficos Grafana relacionados con este diagnóstico, haga clic en el enlace **Grafana Dashboard**.

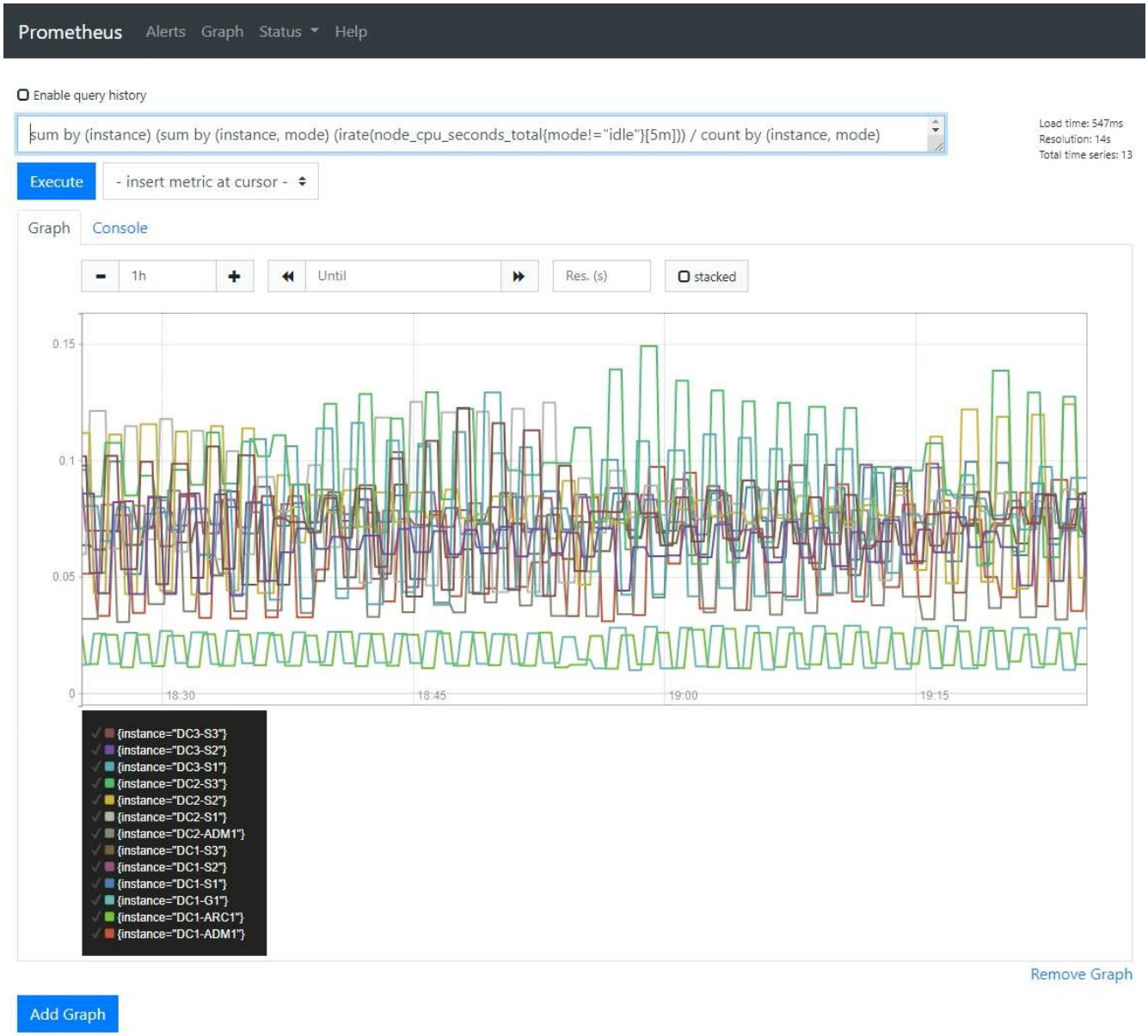
   Este enlace no se muestra para todos los diagnósticos.

   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 métricas que no se muestran en una página existente del Administrador de grid, o si desea crear paneles personalizados para StorageGRID, puede utilizar la API de administración 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, seleccione el icono de ayuda y seleccione **Documentación de API** > **métricas**.

metrics Operations on metrics

GET	/grid/metric-labels/{label}/values	Lists the values for a metric label
GET	/grid/metric-names	Lists all available metric names
GET	/grid/metric-query	Performs an instant metric query at a single point in time
GET	/grid/metric-query-range	Performs a metric query over a range of time

Los detalles de cómo implementar una aplicación de supervisión personalizada están fuera del alcance de esta documentación.

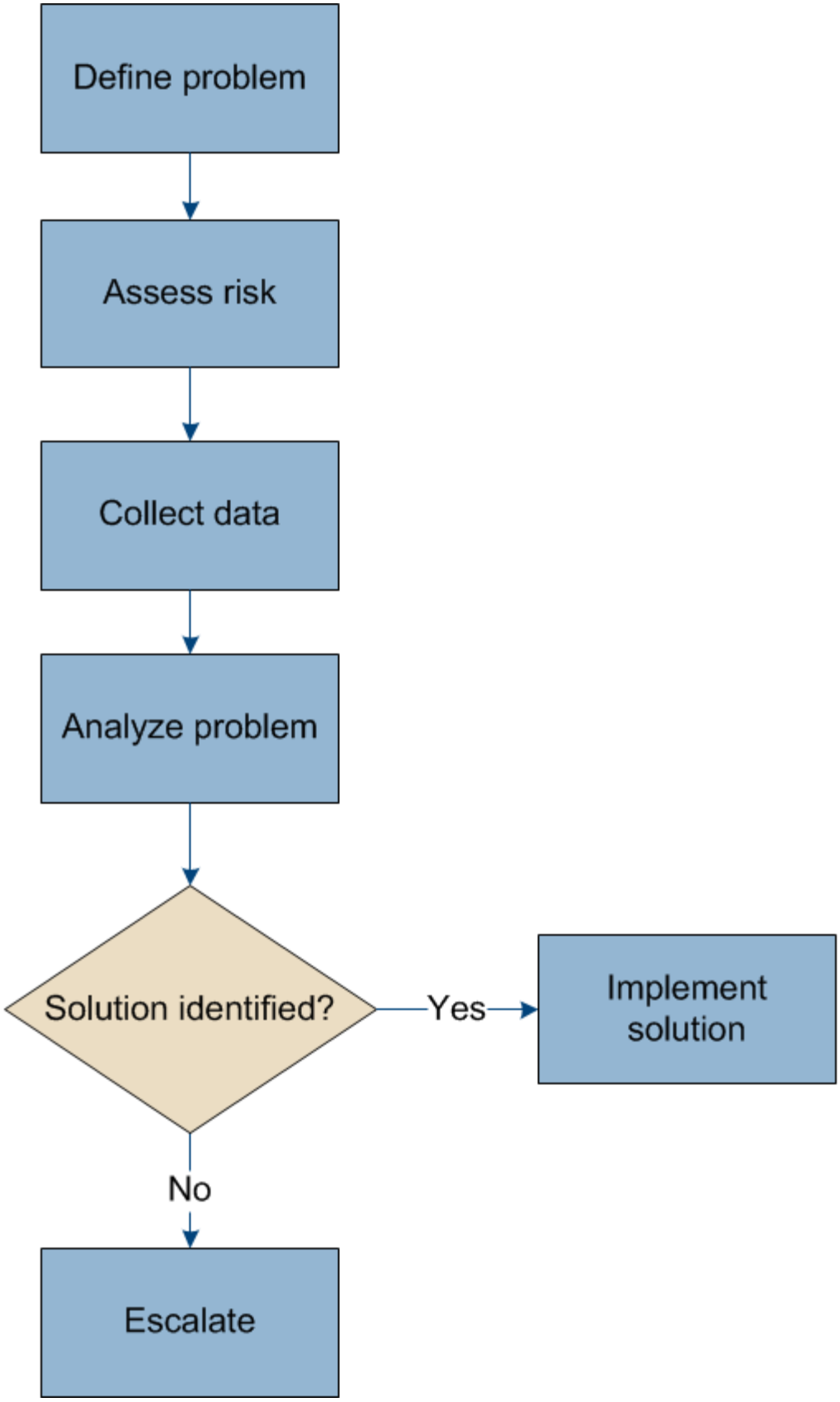
Solucionar los problemas de un sistema StorageGRID

Solucionar los problemas de un sistema StorageGRID

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

Descripción general de la determinación de problemas

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



Defina el problema

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

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

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

Evalúe el riesgo y el impacto sobre el sistema

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

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

Pregunta	Ejemplo de respuesta
¿El sistema StorageGRID puede procesar contenido?	No
¿Las aplicaciones cliente pueden recuperar contenido?	Algunos objetos se pueden recuperar y otros no.
¿Los datos están en riesgo?	No
¿Se ve gravemente afectada la capacidad para llevar a cabo operaciones empresariales?	Sí, porque las aplicaciones cliente no pueden almacenar objetos en el sistema StorageGRID y los datos no pueden recuperarse de forma 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 este archivo dat	Instrucciones
Crear una línea de tiempo de los cambios recientes	Los cambios realizados en el sistema StorageGRID, su configuración o su entorno pueden provocar nuevos comportamientos.	• Crear una línea de tiempo de cambios recientes
Revise las alertas y alarmas	Las alertas y alarmas pueden ayudarle a determinar rápidamente la causa raíz de un problema, proporcionando pistas importantes sobre los problemas subyacentes que podrían estar causando. Revise la lista de alertas y alarmas actuales para ver si StorageGRID ha identificado la causa raíz de un problema. Revise las alertas y alarmas activadas en el pasado para obtener información adicional.	• Ver las alertas actuales • Ver alarmas heredadas • Ver alertas resueltas • Revisar las alarmas históricas y la frecuencia de las alarmas (sistema heredado)
Supervisar eventos	Entre los eventos se incluye cualquier evento de error del sistema o fallo de un nodo, incluidos errores como errores de red. Supervisar eventos para obtener más información acerca de problemas o para ayudar en la solución de problemas.	• 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

Tipo de datos que se van a recoger	Por qué recoger este archivo dat	Instrucciones
Revisar los mensajes de auditoría	Revise los mensajes de auditoría para seguir las operaciones de StorageGRID con detalle. Los detalles de los mensajes de auditoría pueden ser útiles para solucionar muchos tipos de problemas, incluidos problemas de rendimiento.	• Revisar los mensajes de auditoría
Comprobar la ubicación de objetos y la integridad del almacenamiento	Si tiene problemas de almacenamiento, compruebe que los objetos se encuentren en la ubicación que espera. Compruebe la integridad de los datos de objetos en un nodo de almacenamiento.	• Supervise las operaciones de verificación de objetos • Confirme las ubicaciones de los datos del objeto • Verifique la integridad del objeto
Recopile datos para el soporte técnico	Es posible que el soporte técnico le solicite recopilar datos o revisar información específica para ayudar a resolver problemas.	• Recopilar archivos de registro y datos del sistema • Active manualmente un mensaje de 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?

[[Establish_líneas base]]establezca líneas base

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

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

Propiedad	Valor	Cómo obtener
Tasa de operaciones de S3/Swift	Operaciones por segundo	Vaya a Panel en Grid Manager. En la sección Protocol Operations, consulte los valores para la tasa de S3 y la tasa de Swift. Para ver las tasas y recuentos de procesamiento y recuperación de un sitio o nodo específico, seleccione **NODES** > ***site o Storage Node*** > **objetos**. Pase el cursor sobre el gráfico ingesta y recuperación de S3 o Swift.
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. Pase el cursor sobre el gráfico para calcular un valor de línea de base para **tasa de evaluación** para su sistema.
Tasa de análisis de ILM	Objetos por segundo	Seleccione **NODES** > ***grid*** > **ILM**. En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Pase el cursor sobre el gráfico para calcular un valor de línea de base para **tasa de exploración** para su sistema.

Propiedad	Valor	Cómo obtener
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. Pase el cursor por encima del gráfico para calcular un valor de línea de base para **objetos en cola (desde operaciones de cliente)** para su sistema.
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 codificados de borrado? ¿Garantiza ILM la redundancia de sitios? ¿Las reglas de ILM usan los comportamientos de ingesta estrictos, equilibrados o dobles?
	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

✔	Elemento	Notas
	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

En función del problema, es posible que desee confirmar dónde se almacenan los datos del objeto. Por ejemplo, puede que desee verificar que la política de ILM esté funcionando como se espera y que los datos de objetos se almacenen donde estaba previsto.

Lo que necesitará

- Debe tener un identificador de objeto, que puede ser uno de los siguientes:
  - **UUID**: Identificador único universal del objeto. Introduzca el UUID en toda la mayúscula.
  - **CBID**: Identificador único del objeto dentro de StorageGRID . Es posible obtener el CBID de un objeto del registro de auditoría. Introduzca el CBID en todas las mayúsculas.
  - **Bloque de S3 y clave de objeto**: Cuando un objeto se ingiere a través de la interfaz S3, la aplicación cliente utiliza una combinación de bucket y clave de objeto para almacenar e identificar el objeto.
  - **Nombre de objeto y contenedor Swift**: Cuando un objeto se ingiere a través de la interfaz Swift, la aplicación cliente utiliza una combinación de nombre de objeto y contenedor para almacenar e identificar el objeto.

Pasos

1. Seleccione **ILM** > **Búsqueda de metadatos de objetos**.
2. Escriba el identificador del objeto en el campo **Identificador**.

   Es posible introducir un UUID, CBID, bucket/object-key de S3 o nombre de objeto/contenedor de Swift.

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

4. 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 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",
```


Información relacionada

Gestión de objetos con ILM

Use S3

Use Swift

Errores del almacén de objetos (volumen de almacenamiento)

El almacenamiento subyacente en un nodo de almacenamiento se divide en almacenes de objetos. 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

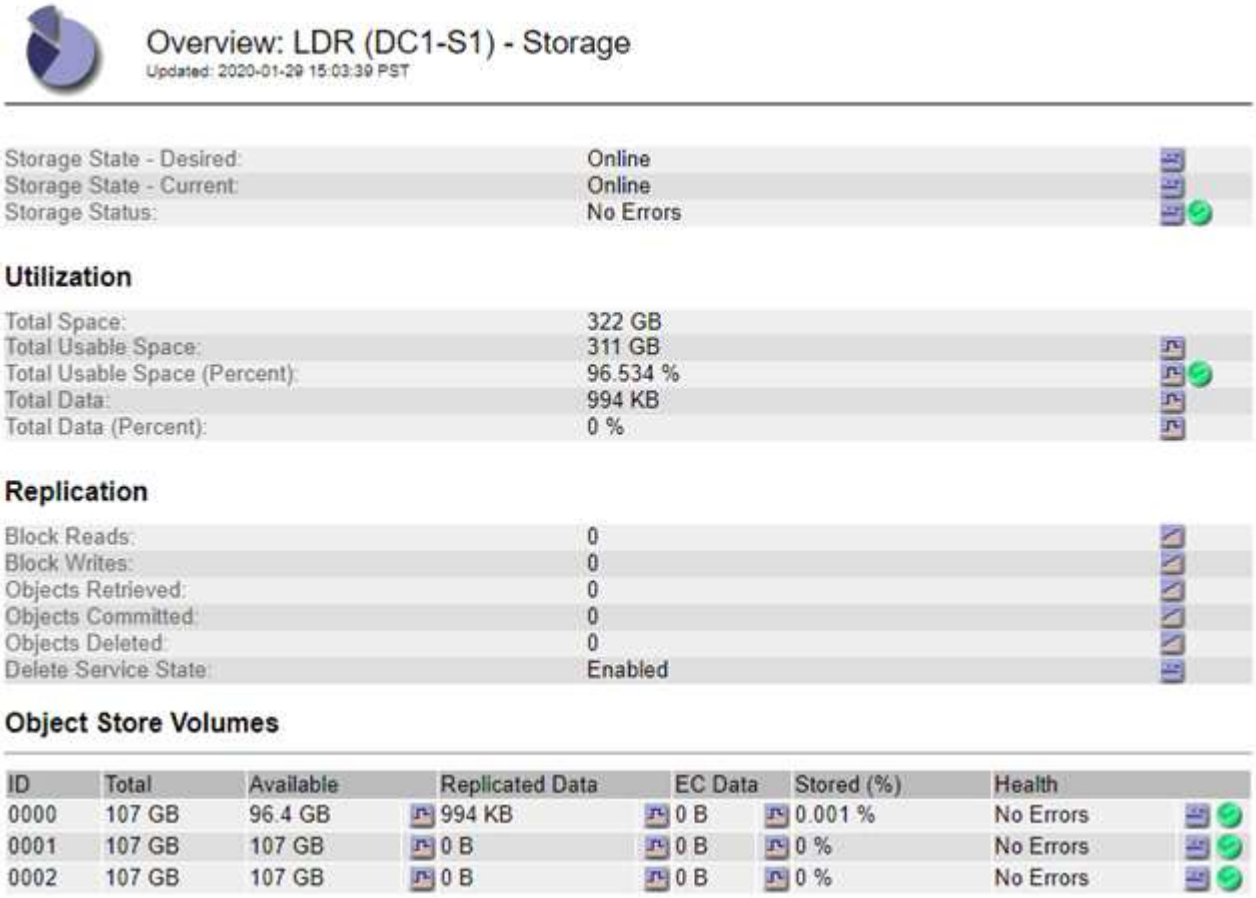
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	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 sobre 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 ficha **Configuración** y colocar el nodo de almacenamiento en un estado de sólo lectura-para que el sistema StorageGRID pueda utilizarlo para la recuperación de datos mientras se prepara para una recuperación completa del servidor.

Información relacionada

Recuperación y mantenimiento

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 coloca una copia nueva sin daños para satisfacer la política activa de ILM. Es posible que la nueva copia no se coloque en el nodo de almacenamiento que se utilizó para la copia original.

  > Los datos de objetos dañados se ponen en cuarentena en lugar de eliminarse del sistema, de modo que aún se puede acceder a ellos. Para obtener más información sobre el acceso a los datos de objetos en cuarentena, póngase en contacto con el soporte técnico.

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

  El proceso de verificación en segundo plano comprueba los objetos solo en los nodos de almacenamiento. No comprueba los objetos en los nodos de archivado ni en un pool de almacenamiento en cloud. Los objetos deben tener una antigüedad superior a cuatro días para poder optar a la verificación en segundo plano.

La verificación en segundo plano se ejecuta a una velocidad continua diseñada para no interferir con las actividades normales del sistema. No se puede detener la verificación en segundo plano. Sin embargo, puede aumentar la tasa de verificación en segundo plano para verificar más rápidamente el contenido de un nodo de almacenamiento si sospecha que existe un problema.

Alertas y alarmas (heredadas) relacionadas con la verificación en segundo plano

Si el sistema detecta un objeto dañado que no puede corregir automáticamente (debido a que el daño impide que el objeto se identifique), se activa la alerta **objeto dañado no identificado**.

Si la verificación en segundo plano no puede reemplazar a 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.

Lo que necesitará

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

Acerca de esta tarea

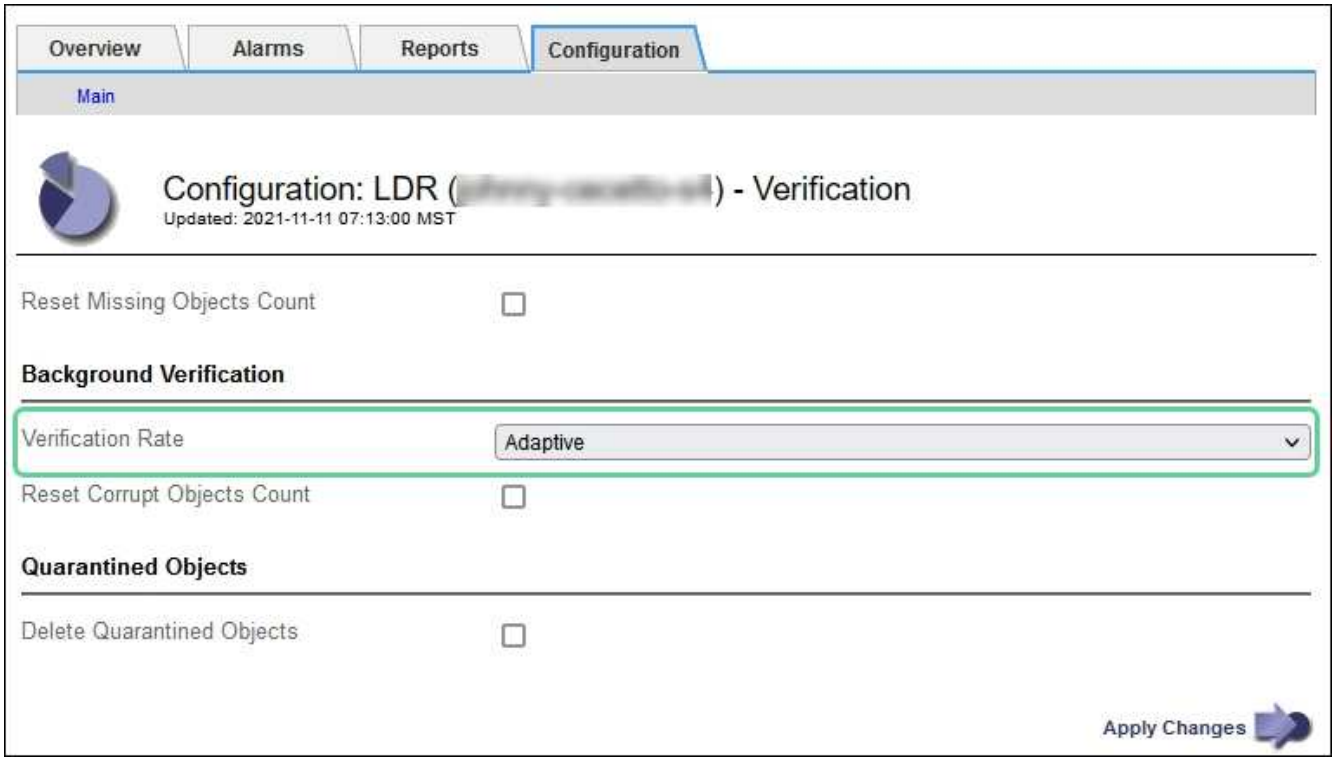
Es posible cambiar la tasa de verificación para la verificación en segundo plano en un nodo de almacenamiento:

- 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 puede realizarse en cualquier punto del sistema StorageGRID que satisfaga la política de ILM activa.
- Si no se puede extraer el identificador de objeto (porque ha estado dañado), se incrementa la métrica **objetos corruptos no identificados** y se activa la alerta **objeto dañado no identificado**.

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

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 coloca una copia nueva para satisfacer la política de ILM activa del sistema. Es posible que esta nueva copia no se coloque en la misma ubicación en la que se 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 con 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 debe seleccionar el control de coherencia para el trabajo.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el 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 la existencia de objetos puede tardar días o semanas en completarse, según la cantidad de objetos de la cuadrícula, los nodos y volúmenes de almacenamiento seleccionados y el control de coherencia seleccionado. 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, active 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, active la casilla de verificación **volumen de almacenamiento** en el encabezado de columna.

6. Seleccione **continuar**.
7. Seleccione el control de coherencia del trabajo.

   El control de consistencia determina cuántas copias de metadatos de objetos se usan para la comprobación de la existencia de objetos.

   - * 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 el control de 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 en pausa, pero no puede reanudar un trabajo que ha 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 el mensaje «Servicio no disponible» o «error interno del servidor». Después de un minuto, actualice la página para continuar supervisando el trabajo.

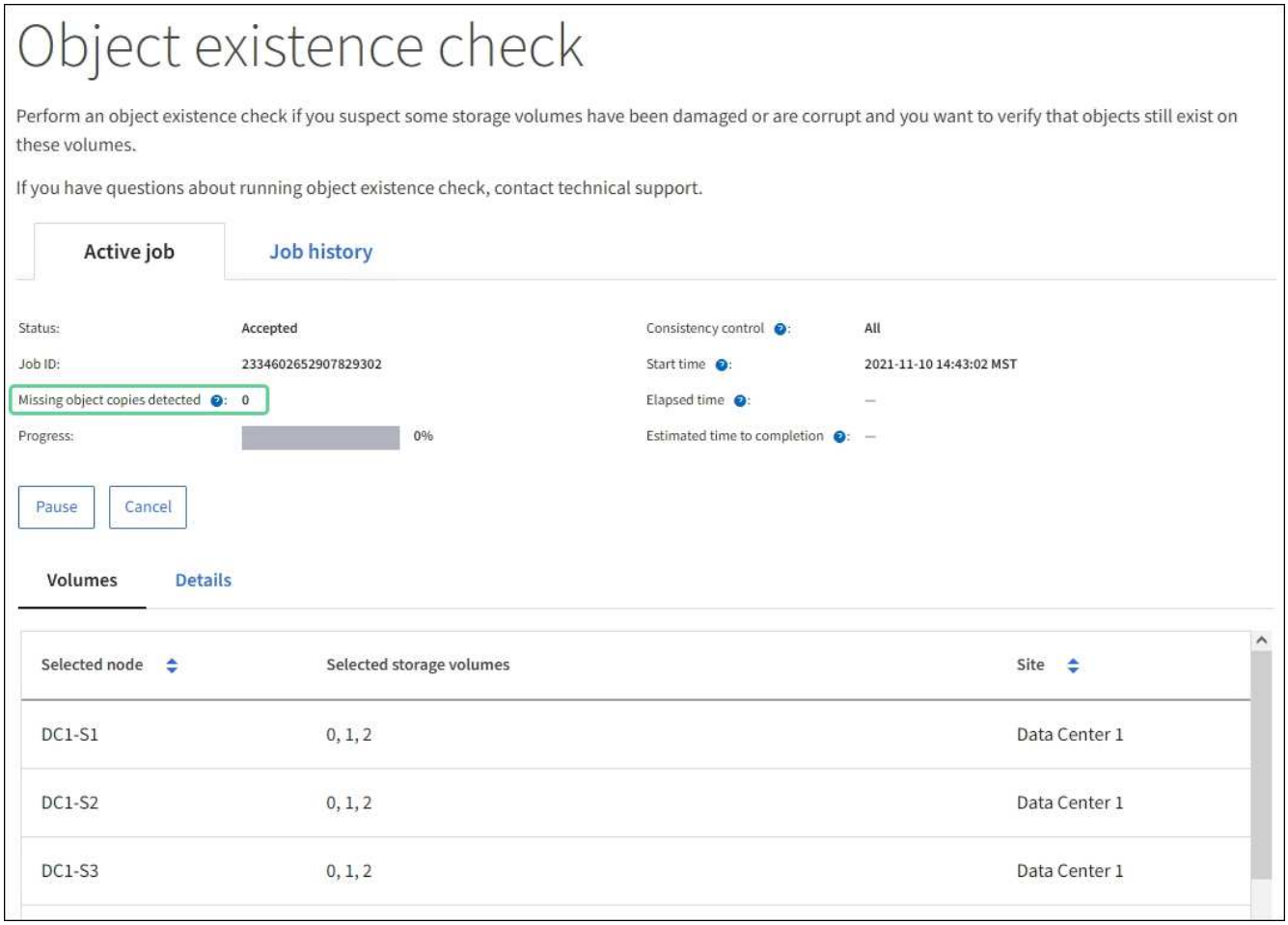
     Según sea necesario, puede salir de la página de comprobación existencia de objetos y volver para continuar supervisando el trabajo.

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.



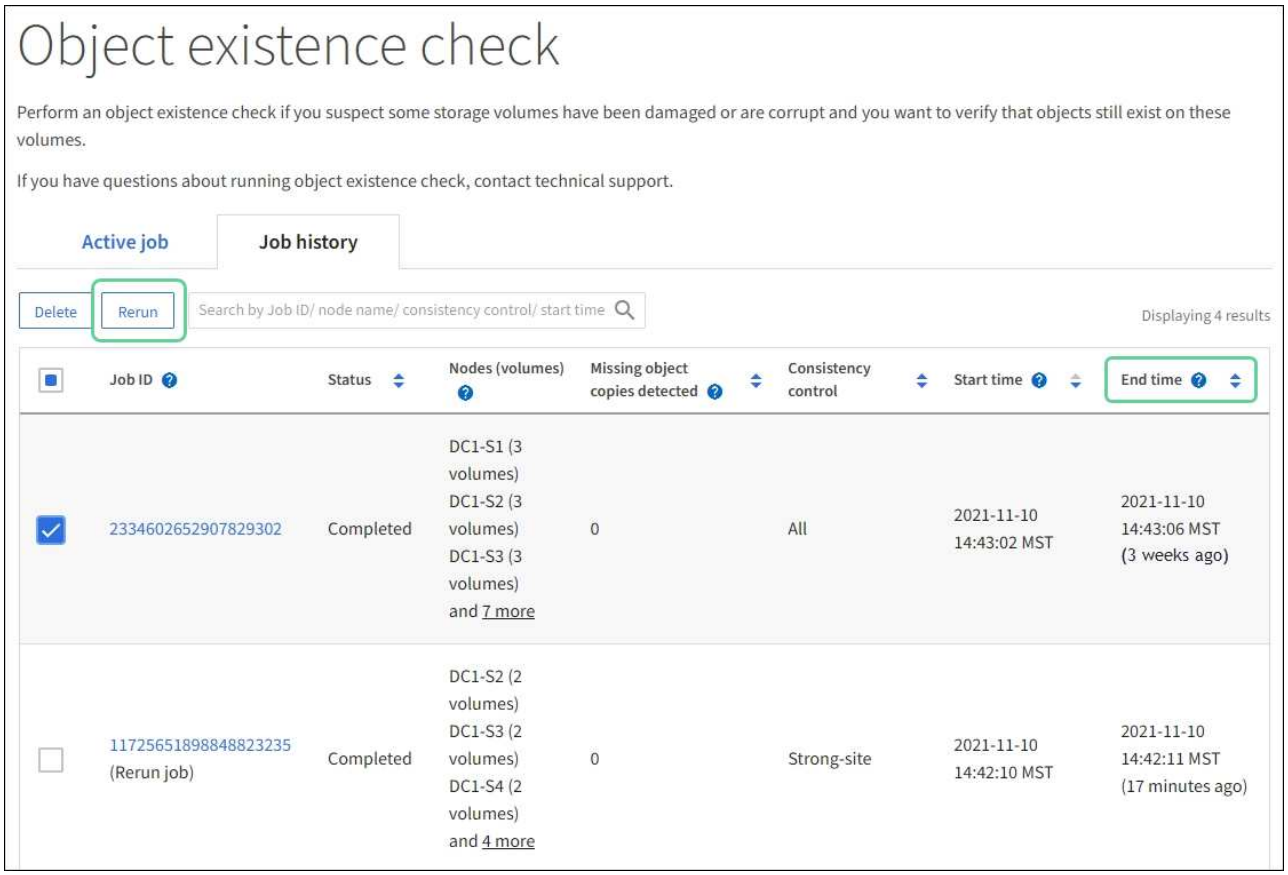
11. Una vez completado el trabajo, realice las acciones necesarias adicionales:
    - Si las copias de objeto que faltan detectadas son cero, no se encontraron problemas. No se requiere ninguna acción.
    - Si las copias de objetos que faltan detectadas son superiores a cero y la alerta **objetos perdidos** 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 ha seleccionado el control de coherencia de sitio seguro o global para el trabajo, 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 de cada trabajo que desee volver a ejecutar y, a continuación, seleccione **Rerun**.



d. En el asistente Rerun Jobs, revise los nodos y volúmenes seleccionados y el control de coherencia.
e. Cuando esté listo para volver a ejecutar los trabajos, seleccione **Rerun**.

Aparece la ficha Trabajo activo. Todos los trabajos seleccionados se vuelven a ejecutar como un trabajo en un control de coherencia de un sitio seguro. 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.

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:

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

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.

Información relacionada

Investigar los objetos perdidos

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.

Lo que necesitará

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

Acerca de esta tarea

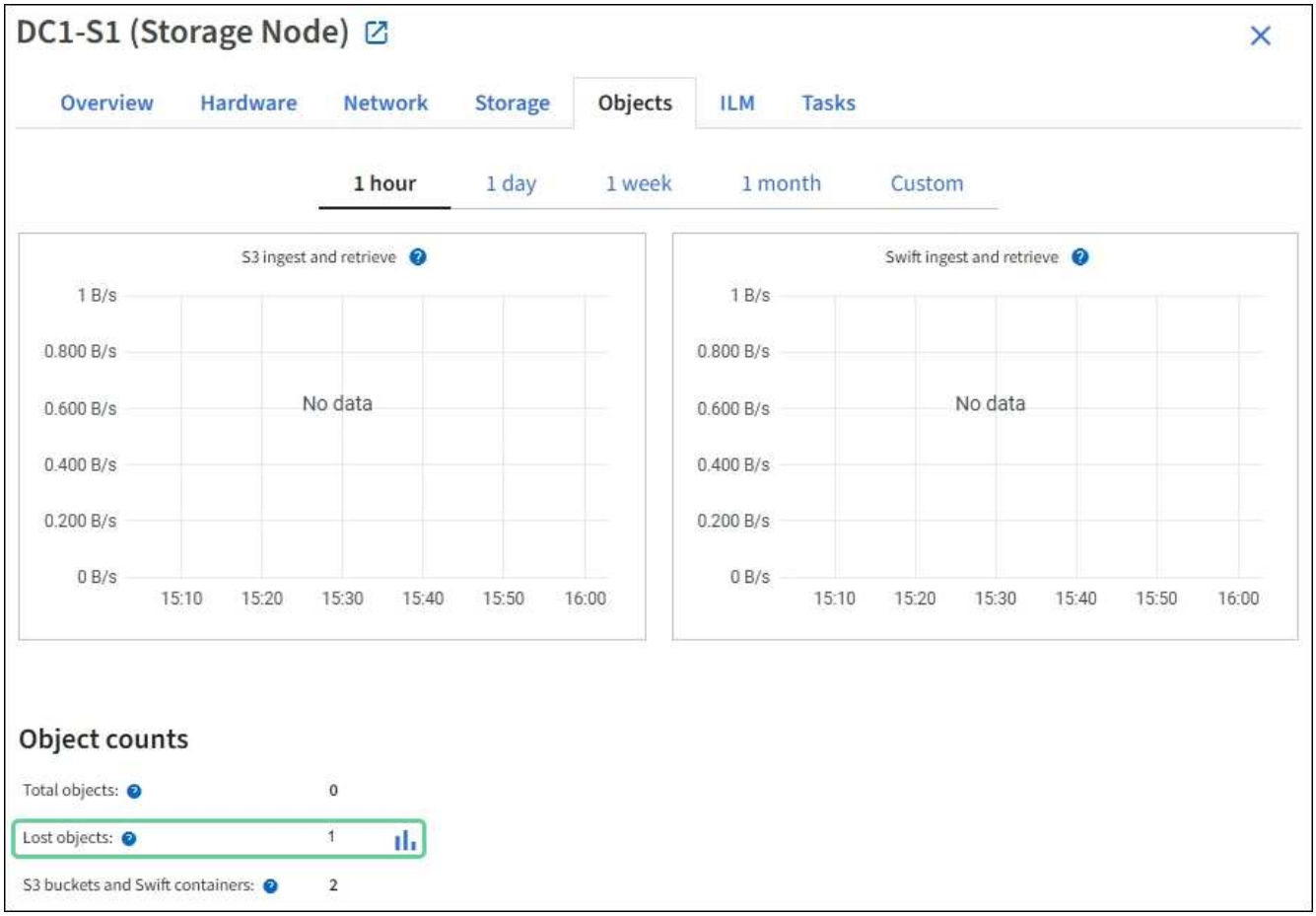
La alerta * objetos perdidos* indica que StorageGRID cree que no hay copias de un objeto en la cuadrícula. Es posible que los datos se hayan perdido de forma permanente.

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. Seleccione **NODES**.
2. Seleccione ***Storage Node*** > **Objects**.
3. Revise el número de objetos perdidos que se muestra en la tabla recuentos de objetos.

   Este número indica el número total de objetos que este nodo de cuadrícula detecta como no recibidos de todo el sistema StorageGRID. El valor es la suma de los contadores de objetos perdidos del componente almacén de datos dentro de los servicios LDR y DDS.



4. Desde un nodo de administración, acceda al registro de auditoría para determinar el identificador único (UUID) del objeto que activó la alerta **objetos perdidos**:
   a. Inicie sesión en el nodo de grid:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo. Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.
   b. Cambie al directorio donde se encuentran los registros de auditoría. Introduzca: `cd /var/local/audit/export/`
   c. Utilice grep para extraer los mensajes de auditoría de objetos perdidos (OLST). Introduzca: `grep OLST audit_file_name`

d. Observe el valor de UUID incluido en el mensaje.

```
>Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Utilice la `ObjectByUUID` Comando para encontrar el objeto mediante su identificador (UUID) y, a continuación, determinar si los datos están en riesgo.

   a. Telnet a localhost 1402 para acceder a la consola LDR.

   b. Introduzca: `/proc/OBRP/ObjectByUUID UUID_value`

      En este primer ejemplo, el objeto con `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` tiene dos ubicaciones en la lista.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
```

```
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```


En el segundo ejemplo, el objeto con `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` no tiene ninguna ubicación en la lista.

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}
```

a. Revise el resultado de /proc/OBRP/ObjectByUUID y realice la acción correspondiente:

Metadatos	Conclusión
No se ha encontrado ningún objeto ("ERROR":"")	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. Es decir, ¿se ha emitido un comando *repair-data* en cualquier nodo de almacenamiento y la recuperación sigue en curso? Consulte la información acerca de restaurar datos de objeto en un volumen de almacenamiento.

Información relacionada

Revisar los registros de auditoría

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.

Lo que necesitará

- Debe tener el UUID de cualquier objeto perdido, tal como se identifica en "'investigar objetos perdidos".
- Debe tener la `Passwords.txt` archivo.

Acerca de esta tarea

Puede seguir este procedimiento para buscar copias replicadas del objeto perdido en otra parte de la cuadrícula. En la mayoría de los casos, el objeto perdido no se encuentra. Sin embargo, en algunos casos, es posible que pueda encontrar y restaurar un objeto replicado perdido si realiza una acción rápida.

Póngase en contacto con el soporte técnico para obtener ayuda con este procedimiento.

Pasos

1. En un nodo de administrador, busque los registros de auditoría para las posibles ubicaciones de objetos:
   a. Inicie sesión en el nodo de grid:
      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
      ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
      iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo. Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.
   b. Cambie al directorio donde se encuentran los registros de auditoría: `cd /var/local/audit/export/`
   c. Utilice grep para extraer los mensajes de auditoría asociados con el objeto potencialmente perdido y enviarlos a un archivo de salida. Introduzca: `grep uuid-valueaudit_file_name > output_file_name`

      Por ejemplo:

      ```
      Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
      messages_about_lost_object.txt
      ```

   d. Utilice grep para extraer los mensajes de auditoría de ubicación perdida (LLST) de este archivo de salida. Introduzca: `grep LLST output_file_name`

      Por ejemplo:

      ```
      Admin: # grep LLST messages_about_lost_objects.txt
      ```

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

      ```
      [AUDT:\[NOID\(UI32\):12448208\][CBIL(UI64):0x38186FE53E3C49A5]
      [UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
      [PCLD\(CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
      [TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):
      1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
      SM]
      [ATID(UI64):7086871083190743409]]
      ```

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

      Si está presente, el valor de PCLD es la ruta completa del disco a la copia del objeto replicado que falta. El valor DE NOID es el ID de nodo de la LDR, donde se puede encontrar una copia del objeto.

Si encuentra una ubicación de objeto, es posible que pueda restaurar el objeto.

f. Busque el nodo de almacenamiento para este ID de nodo LDR.

El ID de nodo se puede usar de dos formas de encontrar el nodo de almacenamiento:

- En Grid Manager, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***Data Center*** > ***Storage Node*** > **LDR**. El ID del nodo LDR se encuentra en la tabla Información del nodo. Revise la información de cada nodo de almacenamiento hasta que encuentre el que aloja esta LDR.
- Descargue y descomprima el paquete de recuperación para el grid. Hay un directorio *\docs* en DICHO paquete. Si abre el archivo index.html, el Resumen de servidores muestra todos los ID de nodo para todos los nodos de cuadrícula.

2. Determine si el objeto existe en el nodo de almacenamiento que se indica en el mensaje de auditoría:

a. Inicie sesión en el nodo de grid:

i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

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

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

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

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

1. Determine si existe la ruta del archivo para el objeto.

Para la ruta de acceso del archivo del objeto, utilice el valor de PCLD del mensaje de auditoría LLST.

Por ejemplo, introduzca:

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

Nota: Siempre encierre la ruta del archivo de objeto entre comillas simples en comandos para escapar de cualquier carácter especial.

- Si no se encuentra la ruta de objeto, se pierde el objeto y no se puede restaurar con este procedimiento. Póngase en contacto con el soporte técnico.
- Si se encuentra la ruta del objeto, continúe con el paso Restaure el objeto en StorageGRID. Puede intentar restaurar el objeto encontrado de nuevo en StorageGRID.

a. Si se encuentra la ruta del objeto, intente restaurar el objeto en StorageGRID:

i. 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'`

ii. Telnet a localhost 1402 para acceder a la consola LDR. Introduzca: `telnet 0 1402`

iii. Introduzca: `cd /proc/STOR`

iv. Introduzca: `Object_Found 'file_path_of_object'`

Por ejemplo, introduzca:

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

Emitir el `Object\_Found` command notifica a la cuadrícula la ubicación del objeto. También activa la política de ILM activa, con la que se realizan copias adicionales según se especifique en la política.

Nota: Si el nodo de almacenamiento donde encontró el objeto está sin conexión, puede copiar el objeto en cualquier nodo de almacenamiento que esté en línea. Coloque el objeto en cualquier directorio /var/local/rangedb del nodo de almacenamiento en línea. A continuación, emita el `Object\_Found` comando que usa esa ruta de acceso al objeto.

- Si el objeto no se puede restaurar, el `Object\_Found` error del comando. Póngase en contacto con el soporte técnico.
- Si el objeto se restauró correctamente en StorageGRID, aparece un mensaje de éxito. Por ejemplo:

```
ade 12448208: /proc/STOR > Object_Found
'/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
```

Continúe con el paso Compruebe que se han creado nuevas ubicaciones

v. 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"
        }
    ]
}
```


1. Cierre la sesión en la consola LDR. Introduzca: `exit`

a. 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.

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 `#`.
3. Cambie al directorio donde se encuentran los registros de auditoría: `cd /var/local/audit/export/`
4. 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
```

5. Utilice grep para extraer los mensajes de auditoría Object Rules MET (ORLM) de este archivo de salida. Introduzca: `grep ORLM output_file_name`

   Por ejemplo:

```
Admin: # grep ORLM messages_about_restored_object.txt
```

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

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

6. 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. . Restablezca el recuento de objetos perdidos en el Gestor de grid.

Información relacionada

Investigar los objetos perdidos

Restablecer el número de objetos perdidos y faltantes

Revisar los registros de auditoría

Restablecer el número de objetos perdidos y faltantes

Después de investigar el sistema StorageGRID y comprobar que todos los objetos perdidos registrados se pierden permanentemente o que se trata de una alarma falsa, puede restablecer el valor del atributo objetos perdidos a cero.

Lo que necesitará

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

Acerca de esta tarea

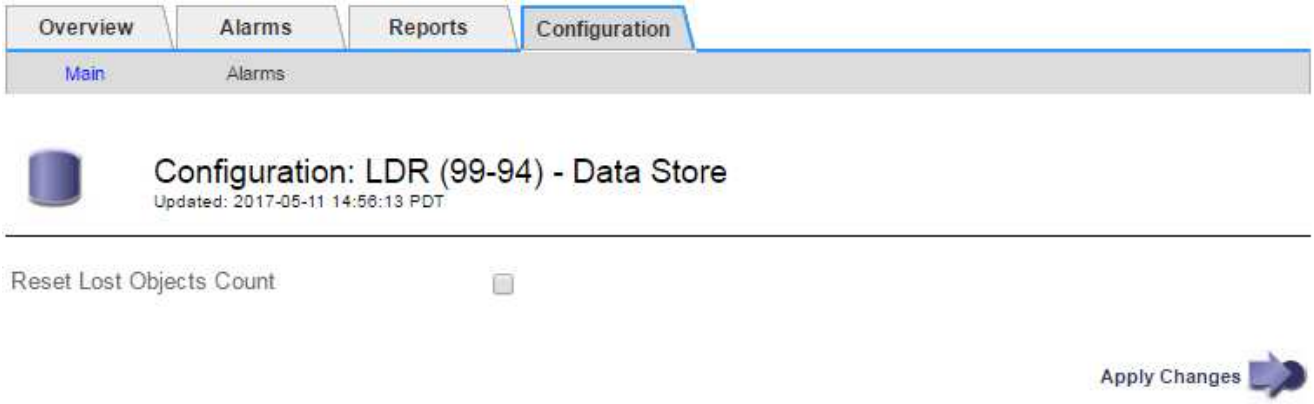
Puede restablecer el contador objetos perdidos desde cualquiera de las siguientes páginas:

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

Estas instrucciones muestran cómo 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.

Lo que necesitará

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

Acerca de esta tarea

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

De forma predeterminada, se activa una alerta principal cuando esta condición se evalúa como TRUE:

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

En esta condición:

- `storagegrid_storage_utilization_data_bytes` Es una estimación del tamaño total de los datos de objetos codificados de replicación y borrado para un nodo de almacenamiento.
- `storagegrid_storage_utilization_usable_space_bytes` Es la cantidad total de espacio de almacenamiento de objetos que queda para un nodo de almacenamiento.

Si se activa una alerta de **almacenamiento de datos de objeto bajo** importante o menor, debe realizar un

procedimiento de expansión Lo antes posible..

Pasos

1. Seleccione **ALERTS** > **Current**.

   Aparece la página Alertas.

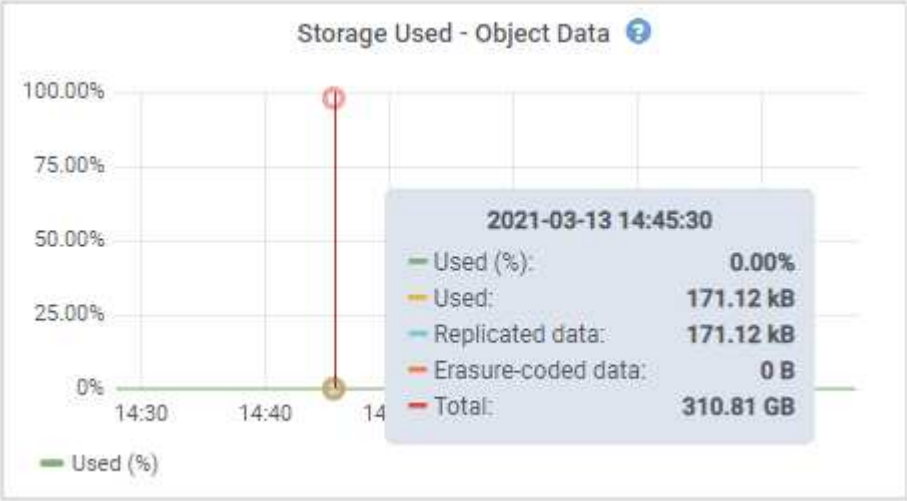
2. En la tabla de alertas, expanda el grupo de alertas **almacenamiento de datos de objeto bajo**, si es necesario, y seleccione la alerta que desea ver.

   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. Pase el cursor sobre el gráfico almacenamiento utilizado - datos de objeto.

   Se muestran los siguientes valores:

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



6. Seleccione los controles de tiempo encima del gráfico para ver el uso del almacenamiento en diferentes periodos de tiempo.

   Si se mira el uso del almacenamiento a lo largo del tiempo, puede comprender cuánto almacenamiento se

utilizó antes y después de que se activó la alerta, y puede ayudar a calcular cuánto tiempo podría tardar en llenarse el espacio restante del nodo.

7. Lo antes posible., realice un procedimiento de ampliación para añadir capacidad de almacenamiento.

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

   > Para gestionar un nodo de almacenamiento completo, consulte las instrucciones para administrar StorageGRID.

Información relacionada

Solucione los problemas de la alarma de estado de almacenamiento (SST)

Amplíe su grid

Administre StorageGRID

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, las marcas de agua de solo lectura y de lectura y escritura optimizadas se aplican automáticamente a todos los volúmenes de almacenamiento, a menos que se establezca lo siguiente:

- 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.

Lo que necesitará

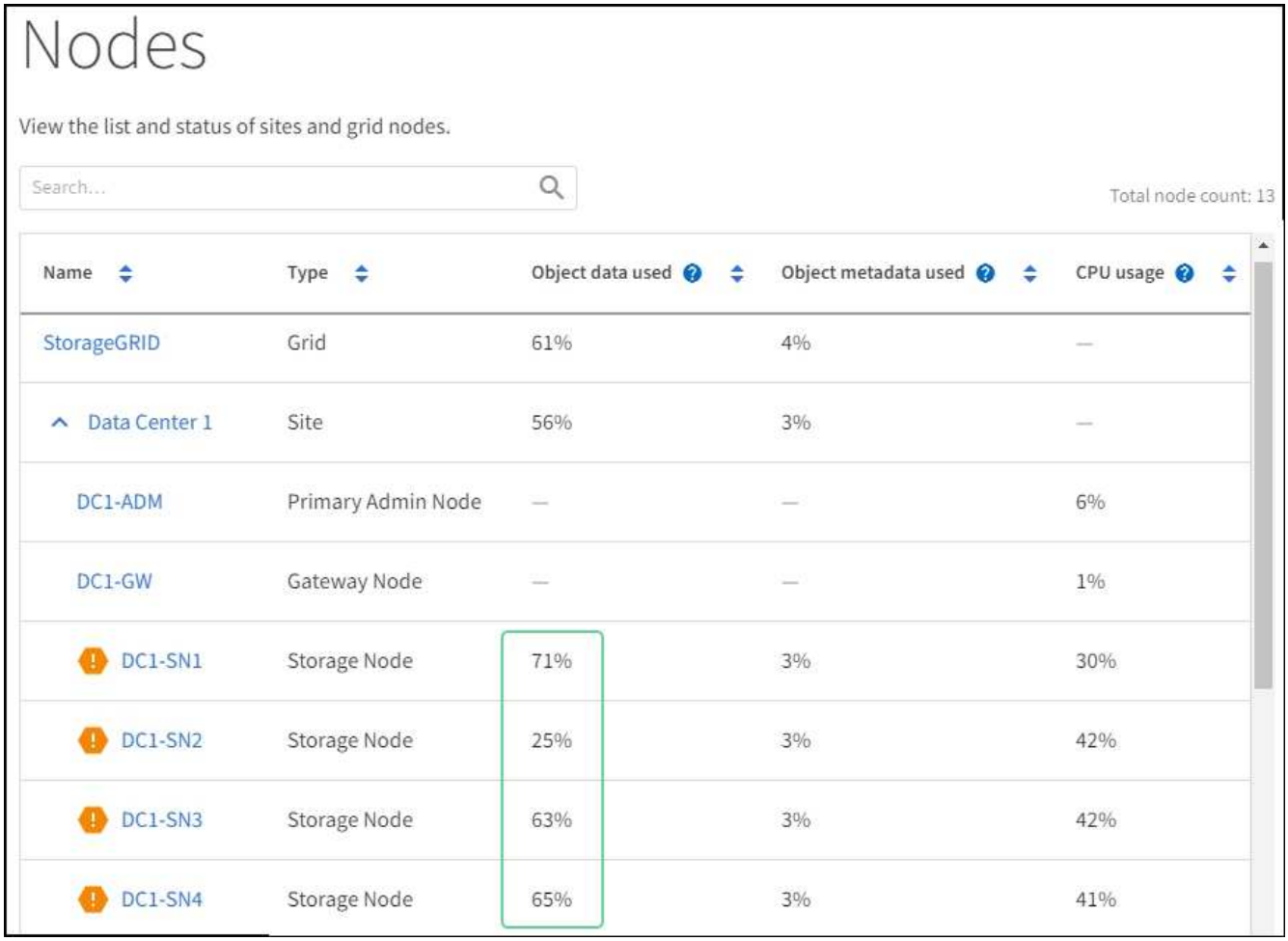
- Ha completado la actualización a StorageGRID 11.6.
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso acceso raíz.

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

1. Seleccione **NODES**.
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. 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.

> Hay algunas excepciones a esta regla general. Por ejemplo, si las reglas de ILM utilizan un comportamiento de procesamiento estricto o si los pools de almacenamiento específicos están cerca de su totalidad, primero debe realizar los pasos de Vea las marcas de agua de almacenamiento optimizadas y.. Determine si puede utilizar marcas de agua optimizadas.

5. Si uno más nodos de almacenamiento se encuentra cerca del completo, realice los pasos en Vea las marcas de agua de almacenamiento optimizadas y.. Determine si puede utilizar marcas de agua optimizadas.

Vea las 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.

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

Determine si puede utilizar marcas de agua optimizadas

1. Seleccione **NODES**.
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.

   En caso contrario, amplíe su grid Lo antes posible.. Añada volúmenes de almacenamiento a 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**.

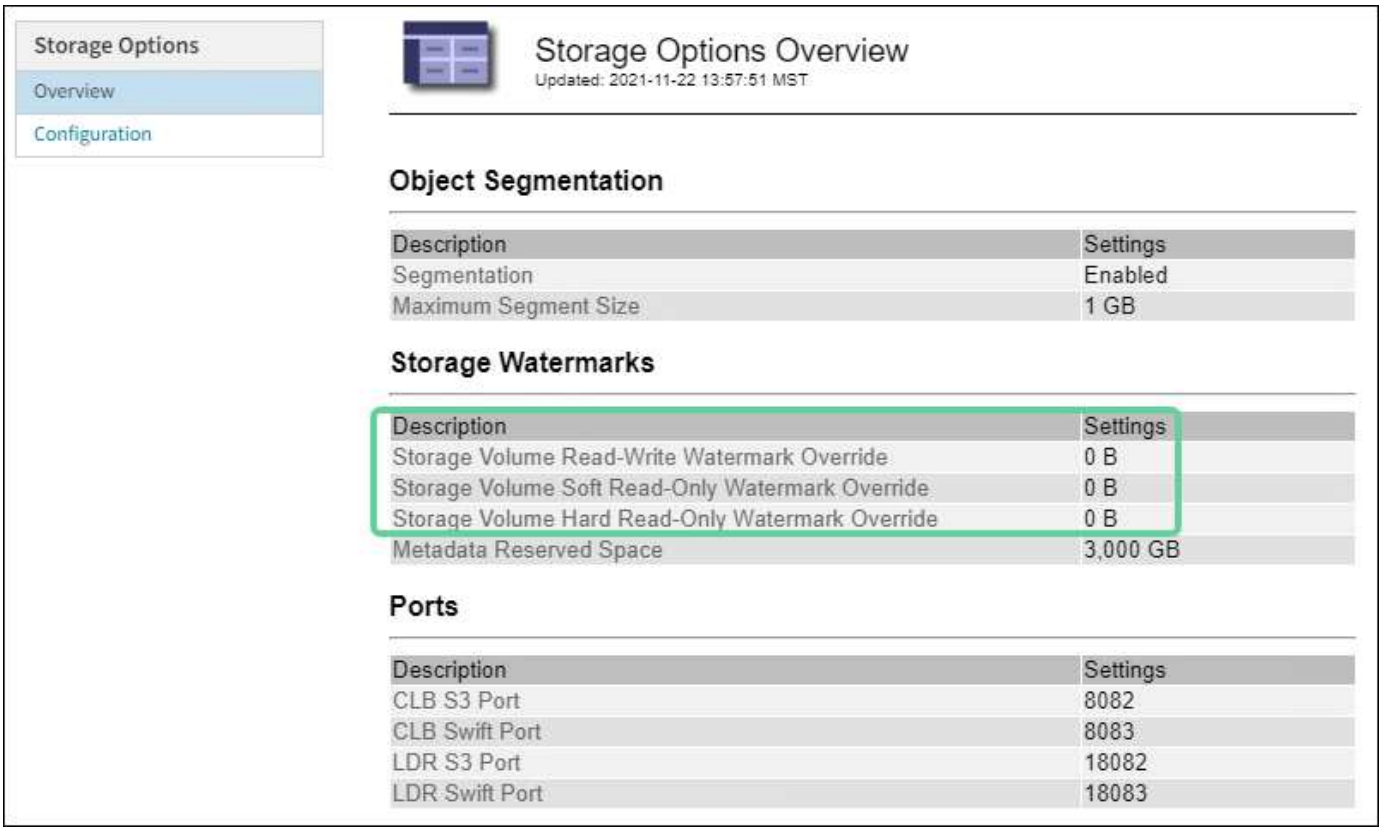
> Los mismos valores de Marca de agua personalizados se aplican a cada volumen de almacenamiento de cada nodo de almacenamiento. Si se utilizan valores más pequeños de lo recomendado para las marcas de agua del volumen de almacenamiento, es posible que algunos volúmenes de almacenamiento se vuelvan inaccesibles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

Utilice marcas de agua optimizadas

1. Vaya a **CONFIGURACIÓN** > **sistema** > **Opciones de almacenamiento**.
2. Seleccione **Configuración** en el menú Opciones de almacenamiento.
3. Cambie las tres anulaciones de Marca de agua a 0.
4. Seleccione **aplicar cambios**.

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.

Lo que necesitará

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

Acerca de esta tarea

La alarma SSTS (Estado de almacenamiento) se activa en el nivel de aviso cuando la cantidad de espacio libre en cada volumen de un nodo de almacenamiento cae por debajo del valor de la Marca de agua de sólo lectura suave del volumen de almacenamiento (**CONFIGURACIÓN** > **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.

Overview | Alarms | Reports | Configuration
Main | History

Alarms: LDR (DC1-S3-101-195) - Storage
Updated: 2019-10-09 12:52:43 MDT

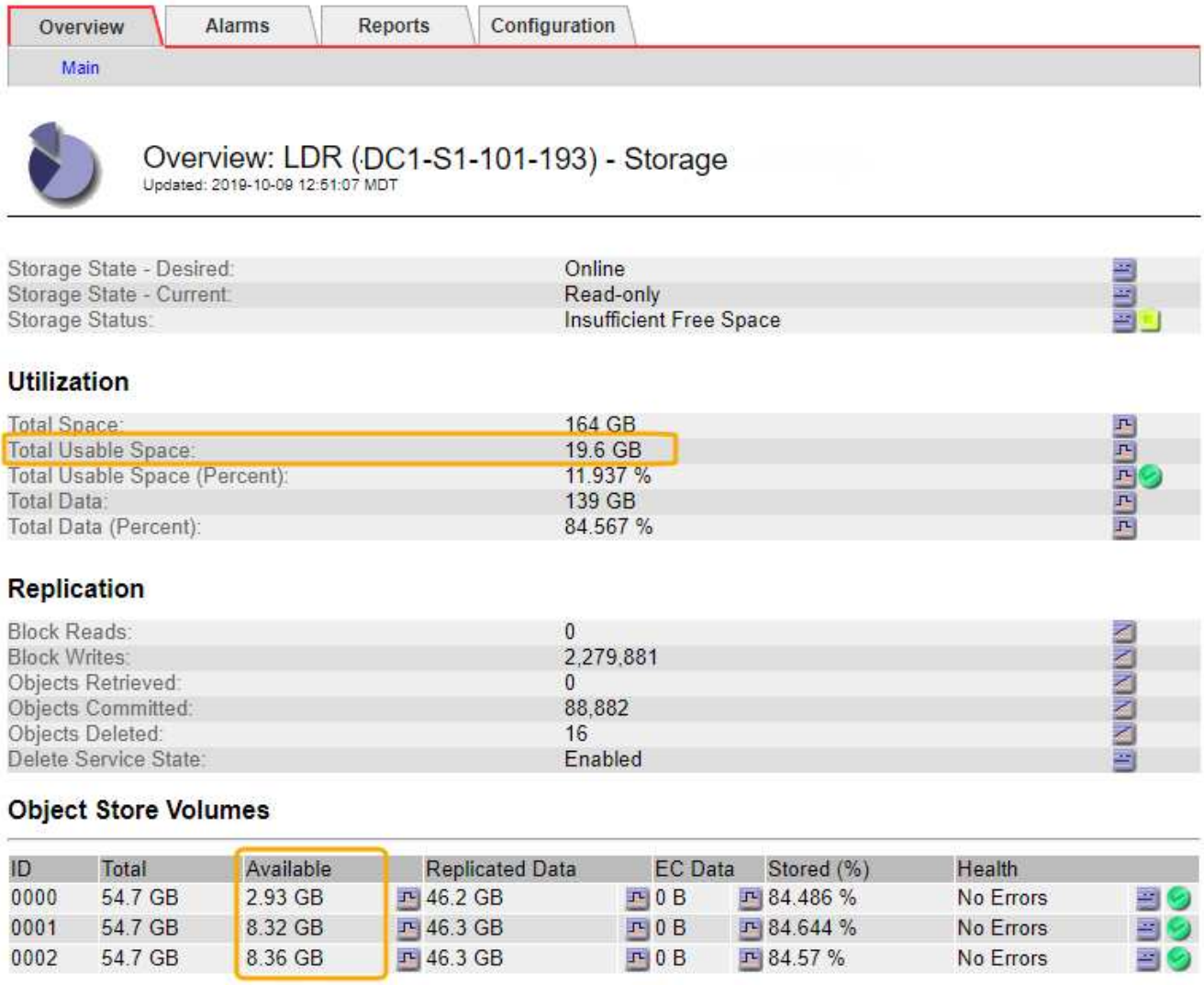
Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Notice	SSTS (Storage Status)	Insufficient Free Space	2019-10-09 12:42:51 MDT	Insufficient Free Space	Insufficient Free Space		
Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT	7.95 %	7.95 %		
Normal	SHLH (Health)						

Apply Changes

   En este ejemplo, se han activado las alarmas SSTS (Estado del almacenamiento) y SAVP (espacio útil total (porcentaje)) en el nivel de aviso.

Normalmente, tanto LA alarma SSTS como la alarma SAVP se activan aproximadamente al mismo tiempo; sin embargo, si ambas alarmas se activan depende del valor de la Marca de agua en GB y del valor de la alarma SAVP en porcentaje.

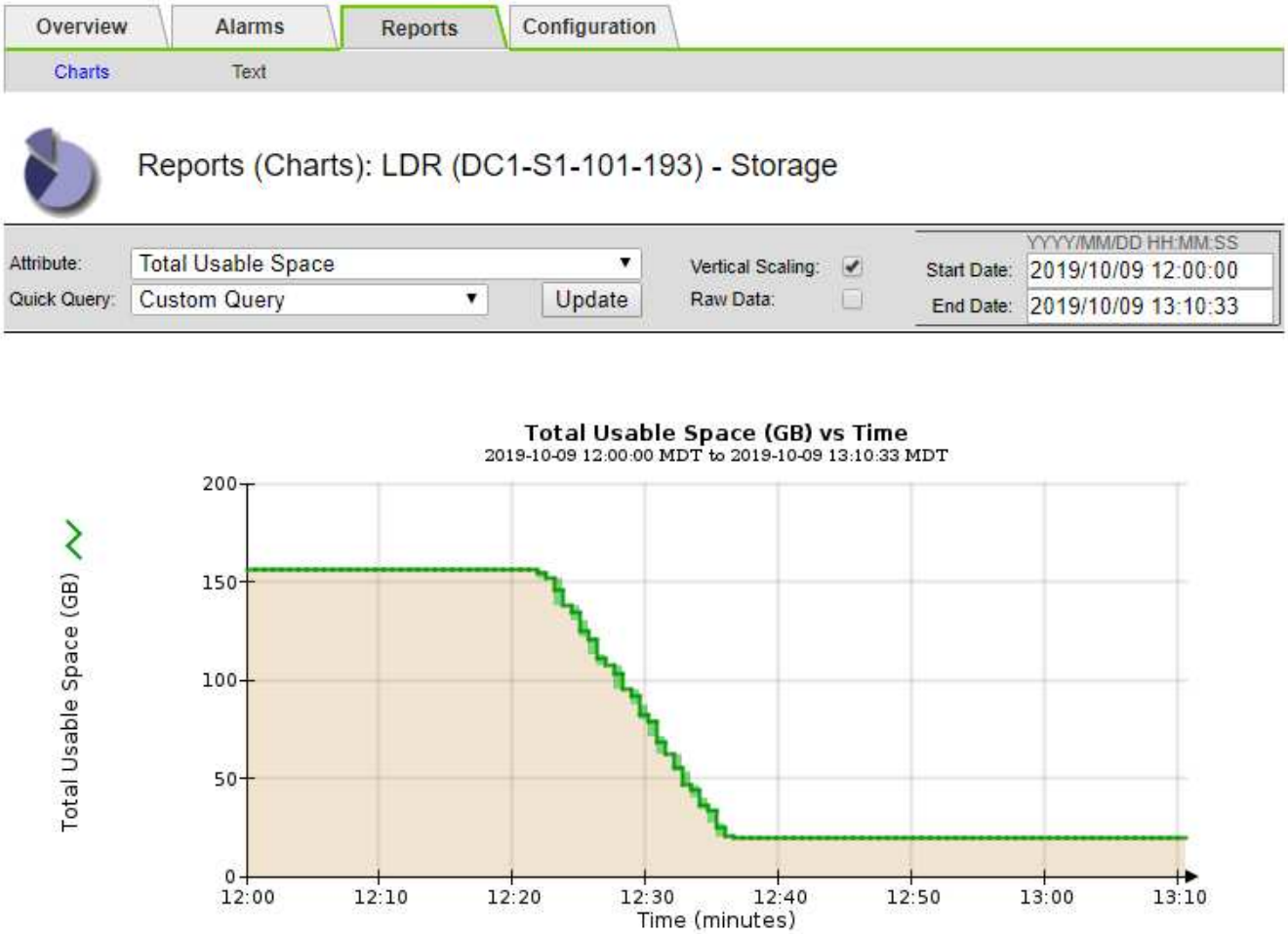
3. Para determinar cuánto espacio útil está realmente disponible, seleccione **LDR** > **almacenamiento** > **Descripción general** y busque el atributo espacio útil total (STS).



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.

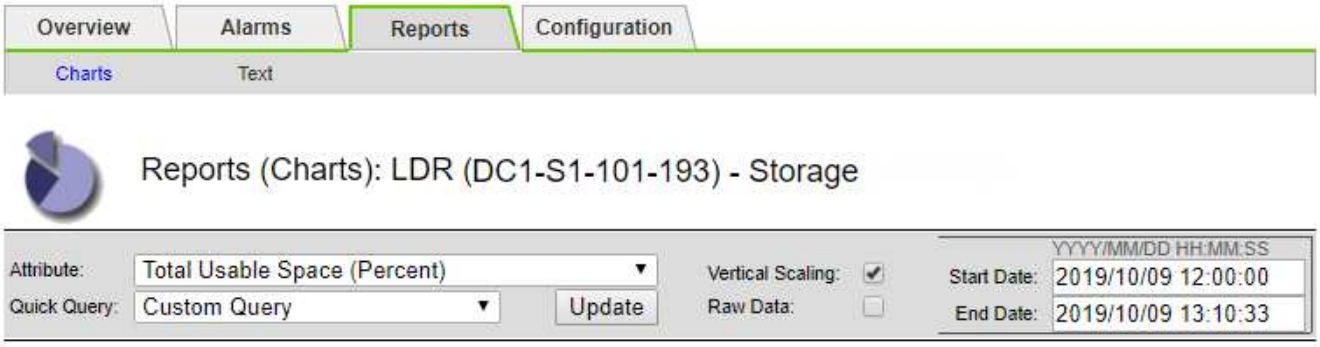
4. Para comprender cómo se ha utilizado el almacenamiento a lo largo del tiempo, seleccione la ficha **Informes** y Trace el espacio útil total en las últimas horas.

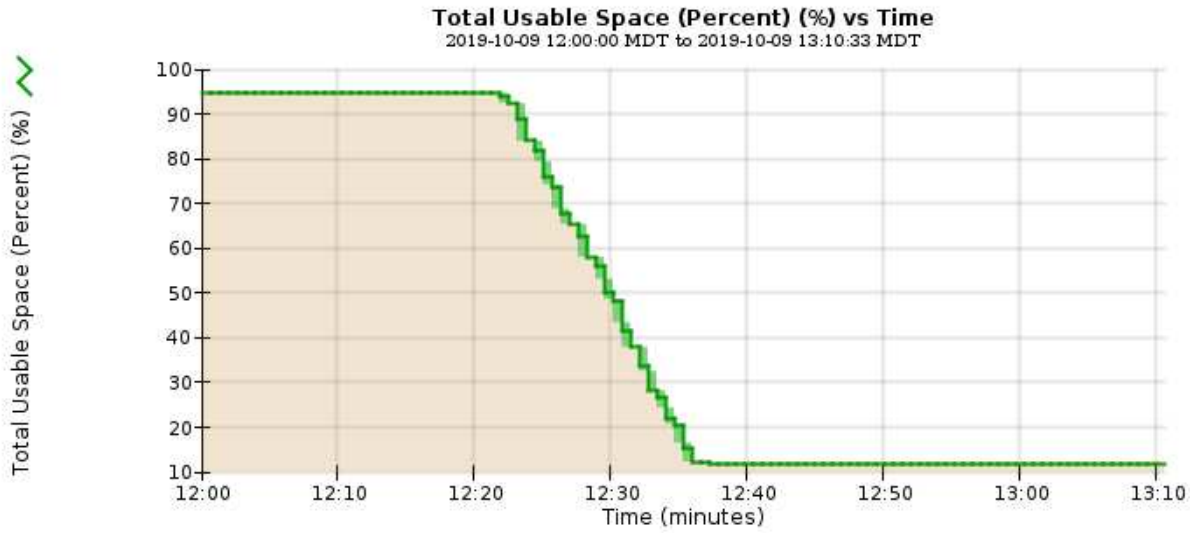
   En este ejemplo, el espacio útil total cayó de aproximadamente 155 GB a 12:00 a 20 GB a 12:35, lo que corresponde al tiempo en que se activó la alarma DE SST.



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. Cuando sea necesario, añada capacidad de almacenamiento mediante Ampliar el sistema StorageGRID.

   Para obtener procedimientos acerca de cómo gestionar un nodo de almacenamiento completo, consulte Instrucciones para administrar StorageGRID.

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

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

Acerca de esta tarea

Por ejemplo, la carga de varias partes de S3 puede realizarse correctamente aunque no se pueda enviar el mensaje de notificación o replicación asociado al extremo configurado. O bien, puede no producirse un error en el mensaje de la replicación de CloudMirror si los metadatos son demasiado largos.

La alarma SMTT contiene un mensaje de último evento que dice: `Failed to publish notifications for bucket-name object key` para el último objeto cuya notificación falló.

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 información adicional acerca de la solución de problemas de los servicios de la plataforma, consulte Instrucciones para administrar StorageGRID. 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.

Solucione los problemas de la alerta de almacenamiento de metadatos bajos

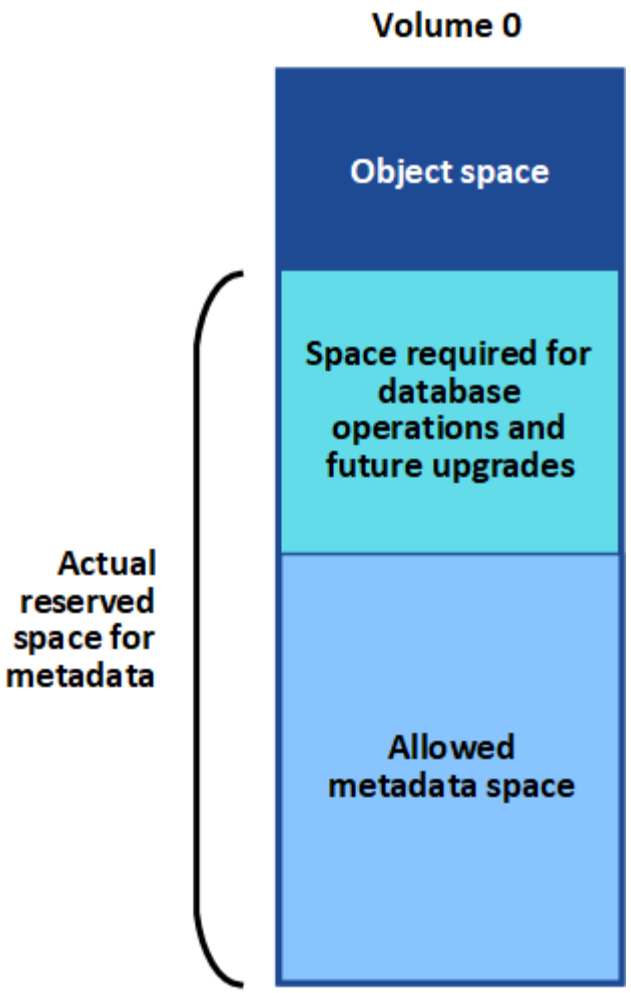
Si se activa la alerta **almacenamiento de metadatos bajo**, debe agregar nuevos nodos de almacenamiento.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un 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 los objetos consumen más del 100% del espacio permitido para los metadatos, las operaciones de base de datos no se pueden ejecutar de forma eficiente y se producirán errores.

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

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

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

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

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

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

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

Pasos

1. Seleccione **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**.

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

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

Lo que necesitará

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

Acerca de esta tarea

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

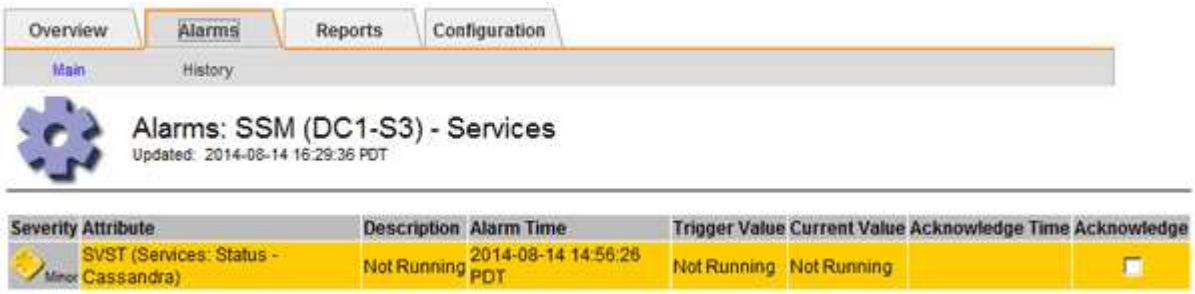
Puede hacerlo ejecutar diagnóstico para obtener información adicional sobre el estado actual de la cuadrícula.

> 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 continúe con los pasos a continuación.

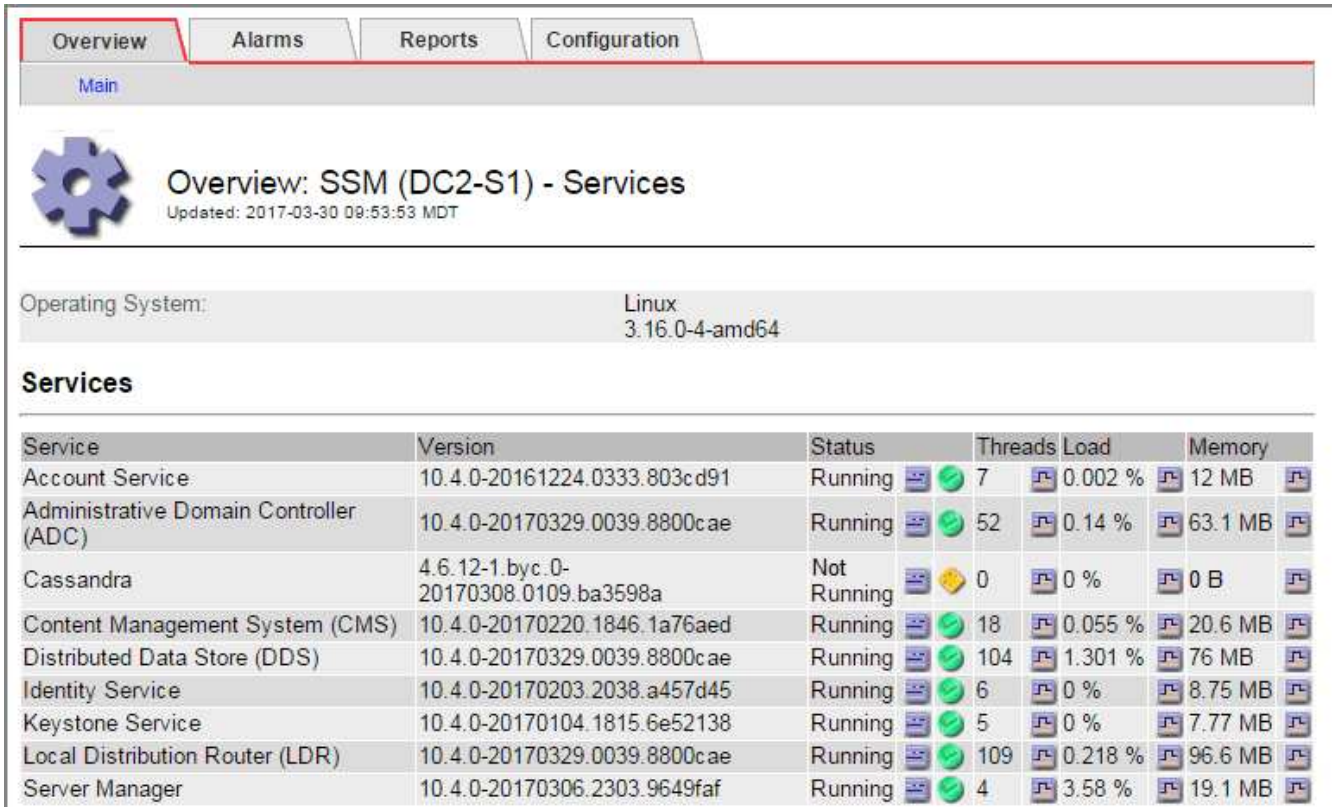
Pasos

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.



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

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.

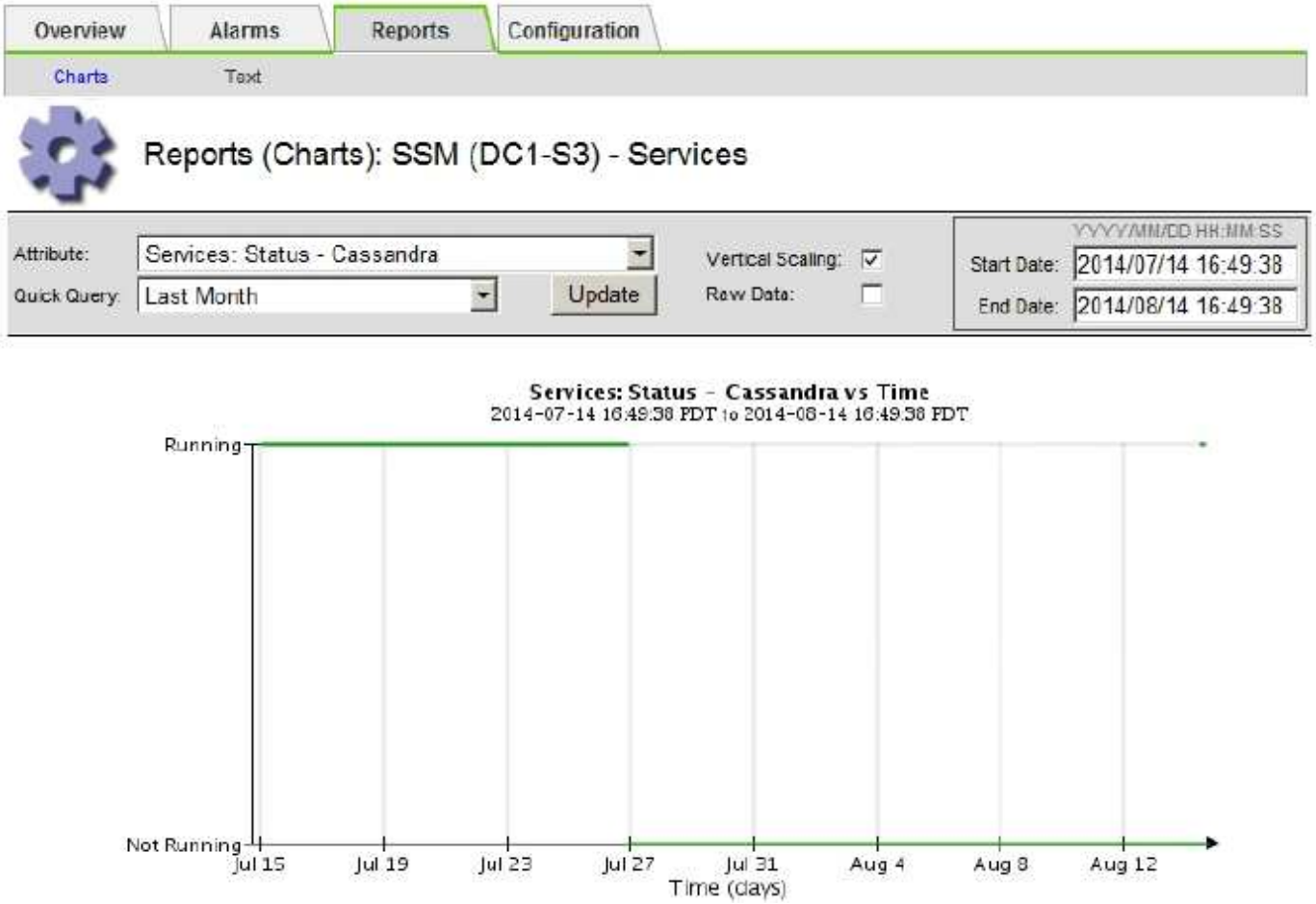
   Puede determinar cuánto tiempo ha estado inactivo Cassandra trazando una entrada de datos o revisando el archivo servermanager.log.

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.



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

   a. Inicie sesión en el nodo de grid:

      i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

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

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

      iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo. Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

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

      Se muestra el contenido del archivo servermanager.log.

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

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

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

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

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

   Para 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.

Solucionar errores de Cassandra fuera de memoria (alarma SMTT)

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

Acerca de esta tarea

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

Pasos

1. Para ver el evento, seleccione **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, active la casilla de verificación **Restablecer** para el recuento de errores de memoria de Cassandra. A continuación, seleccione **aplicar cambios**.

   > Para restablecer los recuentos de eventos, debe tener el permiso Configuración de 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.

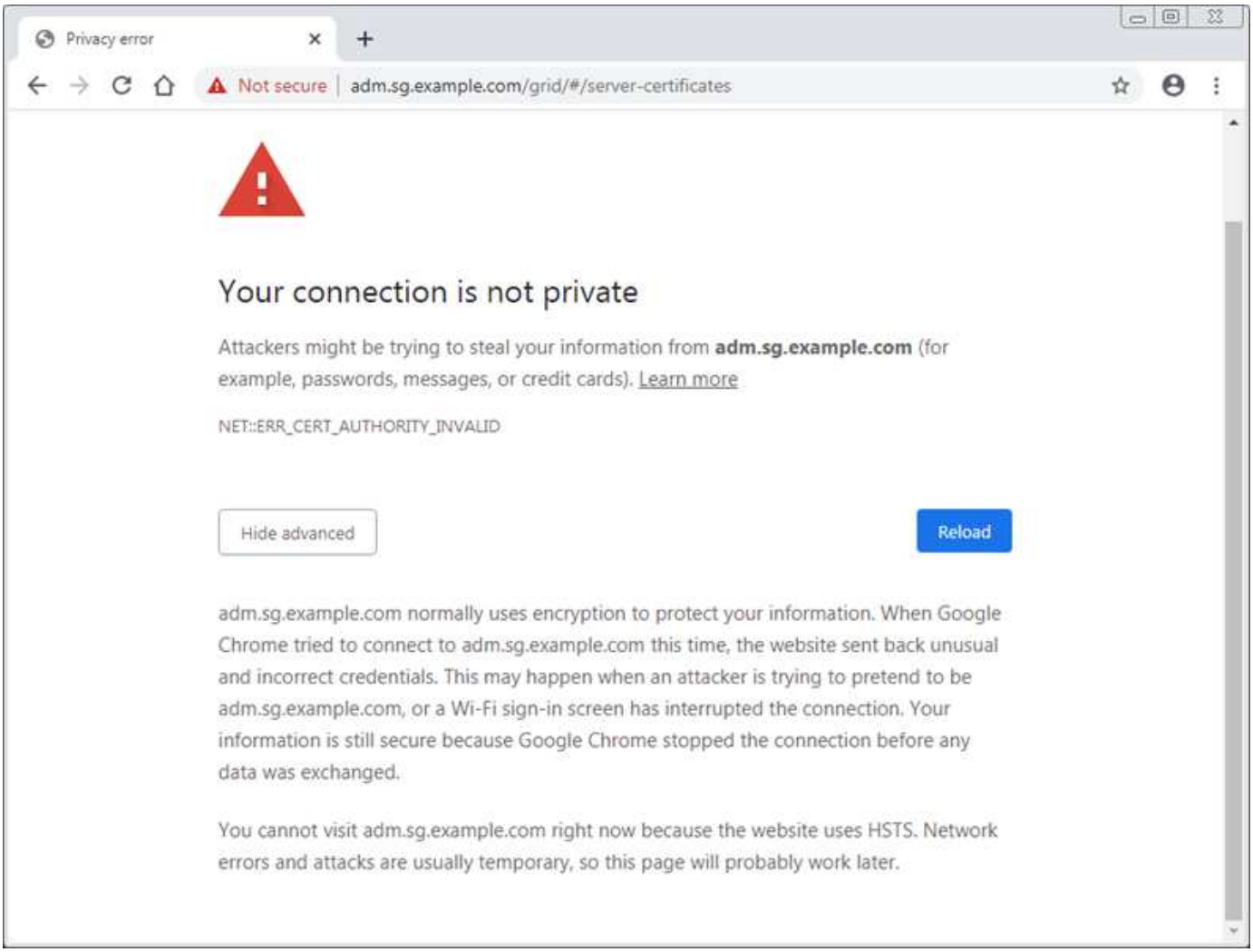
Acerca de esta tarea

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

Cuando se utilizan certificados de cliente para la integración de Prometheus externa, los errores de certificado pueden producirse por el certificado 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 exploradores 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.

Solucionar errores de inicio de sesión

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

Lo que necesitará

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

Acerca de esta tarea

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

- `Your credentials for this account were invalid. Please try again.`

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

Pasos

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

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

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

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

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

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

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

   - Si el usuario local puede iniciar sesión:
     i. Revise las alarmas mostradas.
     ii. Seleccione **CONFIGURACIÓN** > **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 paso siguiente.
6. Utilice Secure Shell (ssh) para iniciar sesión en el nodo de administración:
   a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
   d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

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

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

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

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

8. Confirme que el 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.

Solucionar problemas de la interfaz de usuario

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

La interfaz Web no responde de la manera esperada

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

Si tiene problemas con la interfaz web:

- Asegúrese de utilizar un navegador web compatible.

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

- Borre la caché del navegador web.

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

Compruebe el estado de un nodo administrador que no está disponible

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

Lo que necesitará

Debe tener permisos de acceso específicos.

Pasos

1. Desde un nodo de administración disponible, inicie sesión en Grid Manager 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.

Overview | Alarms | Reports | Configuration

Main

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

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

Operating System:	Linux 3.16.0-4-amd64

Services

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

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

Información relacionada

Administre StorageGRID

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.

Solucionar errores "'422: Entidad no procesable'"

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

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

Mensaje de error	Causa raíz y acción correctiva

`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 usar uno de los cifrados compatibles con StorageGRID para conexiones TLS salientes, tal y como se muestra en las instrucciones para administrar StorageGRID.

Información relacionada

Administre StorageGRID

solucione los problemas de la alerta de discrepancia de MTU de red de red de cuadrícula

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

Acerca de esta tarea

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

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

Pasos

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

Información relacionada

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG5600

Solucione los problemas de la alarma error de recepción de red (NRER)

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

Acerca de esta tarea

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

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

Pasos

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

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

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

      i. Compruebe el estado de FEC del puerto en el interruptor conectado al dispositivo StorageGRID.

      ii. Compruebe la integridad física de los cables del aparato al interruptor.

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

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

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

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

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

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

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

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

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

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

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

2. Después de resolver el problema subyacente, restablezca el contador de errores.
   a. Seleccione **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

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

Referencia de alarmas (sistema heredado)

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG5600

Servicios de aplicaciones SG100 y SG1000

Solucionar errores de sincronización de tiempo

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

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

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

Información relacionada

Recuperación y mantenimiento

Linux: Problemas de conectividad de red

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

Clonación de direcciones MAC

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

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

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

Modo promiscuo

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

Información relacionada

Instale Red Hat Enterprise Linux o CentOS

Instalar Ubuntu o Debian

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

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

Acerca de esta tarea

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

- Compruebe los registros en busca de errores y mensajes.
- Intente iniciar de nuevo el nodo.
- Si es necesario, utilice los comandos 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
   ```

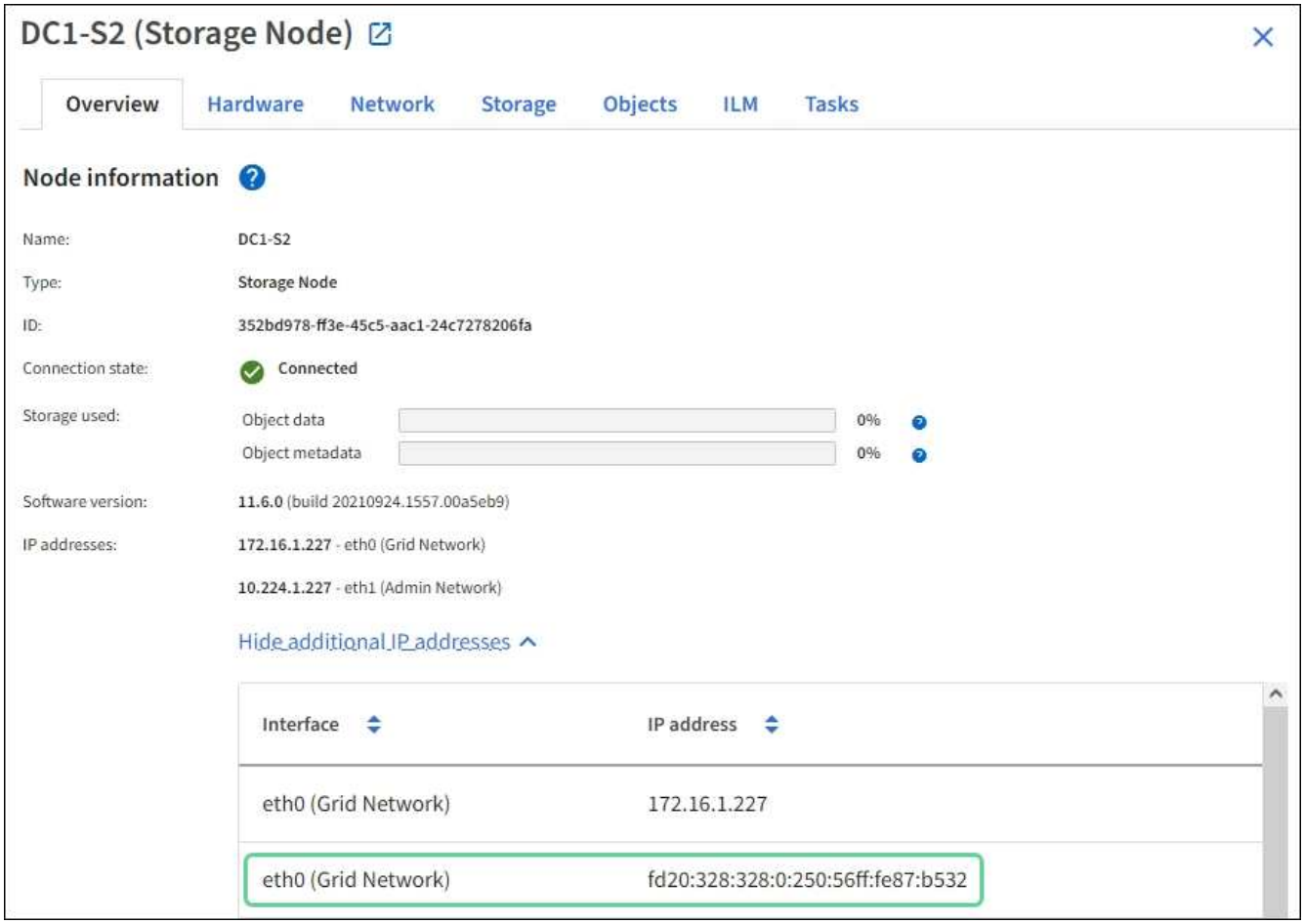
Linux: Solucione problemas de compatibilidad con IPv6

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 del servidor de syslog externo y se enumeran las acciones correctivas.

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

Mensaje de error	Descripción y acciones recomendadas
Host inaccesible	El servidor de syslog se encuentra en una subred de conexión directa (subred que utilizan los nodos mostrados para sus direcciones IP de grid, administrador o cliente). Los nodos intentaron enviar mensajes de prueba, pero no recibieron respuestas a las solicitudes ARP para la dirección MAC del servidor syslog. 1. Compruebe que haya introducido el FQDN o la dirección IP correctos para el servidor de syslog. 2. Compruebe que el host que ejecuta el servicio de syslog esté configurado.
Tiempo de espera de conexión agotado	Se ha realizado un intento de conexión TCP/TLS, pero no se ha recibido respuesta del servidor de syslog durante mucho tiempo. Es posible que haya una configuración incorrecta de enrutamiento o que un firewall esté borrando el tráfico sin enviar ninguna respuesta (una configuración común). 1. Compruebe que haya introducido el FQDN o la dirección IP correctos para el servidor de syslog. 2. Para cada nodo de la lista, compruebe la lista de subredes de redes de cuadrícula, las listas de subredes de redes de administración y las puertas de enlace de red de cliente. Confirme que esta configuración se configuró para enrutar el tráfico al servidor de syslog a través de la interfaz de red y la puerta de enlace (Grid, Admin o Client) sobre la cual espera que se alcance el 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.
	  a. Compruebe que haya introducido el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor de syslog.
	  b. 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.
	  c. Compruebe que un firewall intermedio no está configurado para cerrar las conexiones TCP inactivas.

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

Referencia de alertas

En la siguiente tabla, se enumeran todas las alertas StorageGRID predeterminadas. Según sea necesario, puede crear reglas de alerta personalizadas que se ajusten a su enfoque de administración del sistema.

Consulte la información acerca de Métricas de Prometheus que se usan habitualmente para obtener más información sobre las métricas utilizadas en algunas de estas alertas.

Nombre de alerta	Descripción y acciones recomendadas
La batería del dispositivo ha caducado	La batería de la controladora de almacenamiento del dispositivo caducó. 1. Sustituya la batería. Los pasos para quitar y reemplazar una batería se incluyen en el procedimiento para sustituir una controladora de almacenamiento. Consulte las instrucciones para su dispositivo de almacenamiento: ◦ Dispositivos de almacenamiento SG5600 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG6000 2. Si esta alerta persiste, póngase en contacto con el soporte técnico.
Error de la batería del aparato	Se produjo un error en la batería de la controladora de almacenamiento del dispositivo. 1. Sustituya la batería. Los pasos para quitar y reemplazar una batería se incluyen en el procedimiento para sustituir una controladora de almacenamiento. Consulte las instrucciones para su dispositivo de almacenamiento: ◦ Dispositivos de almacenamiento SG5600 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG6000 2. Si esta alerta persiste, póngase en contacto con el soporte técnico.
La batería del aparato no tiene suficiente capacidad adquirida	La batería de la controladora de almacenamiento del aparato no tiene suficiente capacidad adquirida. 1. Sustituya la batería. Los pasos para quitar y reemplazar una batería se incluyen en el procedimiento para sustituir una controladora de almacenamiento. Consulte las instrucciones para su dispositivo de almacenamiento: ◦ Dispositivos de almacenamiento SG5600 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG6000 2. Si esta alerta persiste, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
La batería del aparato está a punto de agotarse	La batería del controlador de almacenamiento del dispositivo está casi agotada. 1. Sustituya la batería pronto. Los pasos para quitar y reemplazar una batería se incluyen en el procedimiento para sustituir una controladora de almacenamiento. Consulte las instrucciones para su dispositivo de almacenamiento: ◦ Dispositivos de almacenamiento SG5600 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG6000 2. Si esta alerta persiste, póngase en contacto con el soporte técnico.
Se quitó la batería del aparato	Falta la batería del controlador de almacenamiento del aparato. 1. Instale una batería. Los pasos para quitar y reemplazar una batería se incluyen en el procedimiento para sustituir una controladora de almacenamiento. Consulte las instrucciones para su dispositivo de almacenamiento: ◦ Dispositivos de almacenamiento SG5600 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG6000 2. Si esta alerta persiste, póngase en contacto con el soporte técnico.
La batería del aparato está demasiado caliente	La batería del controlador de almacenamiento del aparato se sobrecalienta. 1. Determine si hay otra alerta que afecte a este nodo. Es posible que esta alerta se resuelva cuando se resuelve la otra alerta. 2. Investigue las posibles razones del aumento de temperatura, como un fallo del ventilador o del sistema HVAC. 3. Si esta alerta persiste, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
Error de comunicación de la BMC del dispositivo	Se ha perdido la comunicación con el controlador de administración de la placa base (BMC). 1. Confirme que el BMC funciona con normalidad. Seleccione **NODES** y, a continuación, seleccione la ficha **hardware** para el nodo del dispositivo. Busque el campo Compute Controller BMC IP y desplácese hasta esa IP. 2. Intente restaurar las comunicaciones de BMC colocando el nodo en modo de mantenimiento y, a continuación, apagando y volviendo a encender el dispositivo. Consulte las instrucciones del aparato: ◦ Servicios de aplicaciones SG100 y SG1000 ◦ Dispositivos de almacenamiento SG6000 3. Si esta alerta persiste, póngase en contacto con el soporte técnico.
Error del dispositivo de backup de la caché del dispositivo	Se produjo un error en un dispositivo de backup de caché persistente. 1. Determine si hay otra alerta que afecte a este nodo. Es posible que esta alerta se resuelva cuando se resuelve la otra alerta. 2. Póngase en contacto con el soporte técnico.
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. Póngase en contacto con el soporte técnico.
Dispositivo de backup de la caché de dispositivo con protección contra escritura	Un dispositivo de backup de caché está protegido contra escritura. Póngase en contacto con el soporte técnico.
El tamaño de la memoria caché del dispositivo no coincide	Las dos controladoras del dispositivo tienen distintos tamaños de caché. Póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
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. 1. Compruebe si los componentes de hardware están sobrecalentados y siga las acciones recomendadas: ◦ Si tiene un SG100, SG1000 o SG6000, utilice el BMC. ◦ Si tiene SG5600 o SG5700, utilice System Manager de SANtricity. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Servicios de aplicaciones SG100 y SG1000 ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600
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. 1. Compruebe si los componentes de hardware están sobrecalentados y siga las acciones recomendadas: ◦ Si tiene un SG100, SG1000 o SG6000, utilice el BMC. ◦ Si tiene SG5600 o SG5700, utilice System Manager de SANtricity. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Servicios de aplicaciones SG100 y SG1000 ◦ Dispositivos de almacenamiento SG5600 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG6000

Nombre de alerta	Descripción y acciones recomendadas
La controladora de computación del dispositivo requiere atención	Se detectó un error de hardware en la controladora de computación de un dispositivo StorageGRID. 1. Compruebe los componentes de hardware en busca de errores y siga las acciones recomendadas: ◦ Si tiene un SG100, SG1000 o SG6000, utilice el BMC. ◦ Si tiene SG5600 o SG5700, utilice System Manager de SANtricity. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Servicios de aplicaciones SG100 y SG1000 ◦ Dispositivos de almacenamiento SG5600 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG6000
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. Esta alerta puede indicar que el suministro de alimentación ha fallado o que tiene un problema de alimentación. 1. Compruebe los componentes de hardware en busca de errores y siga las acciones recomendadas: ◦ Si tiene un SG100, SG1000 o SG6000, utilice el BMC. ◦ Si tiene SG5600 o SG5700, utilice System Manager de SANtricity. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Servicios de aplicaciones SG100 y SG1000 ◦ Dispositivos de almacenamiento SG5600 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG6000

Nombre de alerta	Descripción y acciones recomendadas
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. Esta alerta puede indicar que el suministro de alimentación ha fallado o que tiene un problema de alimentación. 1. Compruebe los componentes de hardware en busca de errores y siga las acciones recomendadas: ◦ Si tiene un SG100, SG1000 o SG6000, utilice el BMC. ◦ Si tiene SG5600 o SG5700, utilice System Manager de SANtricity. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Servicios de aplicaciones SG100 y SG1000 ◦ Dispositivos de almacenamiento SG5600 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG6000
El servicio de supervisión del hardware de computación del dispositivo está estancado	El servicio que supervisa el estado del hardware de almacenamiento ha detenido la generación de informes. 1. Comprobar el estado del servicio de estado del sistema eos en el so básico 2. Si el servicio está en estado detenido o error, reinicie el servicio. 3. Si esta alerta persiste, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
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. Esta alerta puede indicar que hay un problema con la conexión de Fibre Channel entre las controladoras de almacenamiento y los recursos informáticos en el dispositivo. 1. Compruebe los componentes de hardware en busca de errores (**NODES** > ***Appliance node*** > **hardware**). Si el estado de alguno de los componentes no es "'nominal'", realice las siguientes acciones: a. Confirmar que los cables de Fibre Channel entre controladoras están completamente conectados. b. Asegúrese de que los cables Fibre Channel están libres de pliegues excesivos. c. Confirme que los módulos SFP+ están correctamente asentados. **Nota:** Si este problema persiste, el sistema StorageGRID podría desconectar automáticamente la conexión problemática. 2. Si es necesario, sustituir los componentes. Consulte las instrucciones del aparato: ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG6000
Error en el puerto HBA del Fibre Channel del dispositivo	Un puerto HBA Fibre Channel está fallando o ya falló. Póngase en contacto con el soporte técnico.
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. 1. Sustituya las unidades de caché SSD. Consulte las instrucciones del aparato: ◦ Dispositivos de almacenamiento SG5600 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG6000 2. Si esta alerta persiste, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
Se quitó la interconexión del dispositivo/el contenedor de batería	Falta el contenedor de interconexión/batería. 1. Sustituya la batería. Los pasos para quitar y reemplazar una batería se incluyen en el procedimiento para sustituir una controladora de almacenamiento. Consulte las instrucciones del dispositivo de almacenamiento. ◦ Dispositivos de almacenamiento SG5600 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG6000 2. Si esta alerta persiste, póngase en contacto con el soporte técnico.
Falta el puerto LACP del dispositivo	Un puerto de un dispositivo StorageGRID no participa en el enlace LACP. 1. Compruebe la configuración del interruptor. Asegúrese de que la interfaz está configurada en el grupo de agregación de vínculos correcto. 2. Si esta alerta persiste, póngase en contacto con el soporte técnico.
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. 1. Compruebe el estado de la fuente De alimentación A y B para determinar qué fuente de alimentación funciona de forma anormal y siga las acciones recomendadas: ◦ Si tiene un SG100, SG1000 o SG6000, utilice el BMC. ◦ Si tiene SG5600 o SG5700, utilice System Manager de SANtricity. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600 ◦ Servicios de aplicaciones SG100 y SG1000

Nombre de alerta	Descripción y acciones recomendadas
Fallo de la controladora A del almacenamiento del dispositivo	Se produjo un error en la controladora De almacenamiento A de un dispositivo StorageGRID. 1. Use System Manager de SANtricity para comprobar los componentes de hardware y seguir las acciones recomendadas. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600
Fallo del controlador B de almacenamiento del dispositivo	Error de la controladora de almacenamiento B en un dispositivo StorageGRID. 1. Use System Manager de SANtricity para comprobar los componentes de hardware y seguir las acciones recomendadas. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600
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. 1. Use System Manager de SANtricity para comprobar los componentes de hardware y seguir las acciones recomendadas. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600
Problema de hardware de la controladora de almacenamiento del dispositivo	El software SANtricity informa "necesita atención" para un componente de un dispositivo StorageGRID. 1. Use System Manager de SANtricity para comprobar los componentes de hardware y seguir las acciones recomendadas. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600

Nombre de alerta	Descripción y acciones recomendadas
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. 1. Use System Manager de SANtricity para comprobar los componentes de hardware y seguir las acciones recomendadas. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600
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. 1. Use System Manager de SANtricity para comprobar los componentes de hardware y seguir las acciones recomendadas. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600
El servicio de supervisión del hardware de almacenamiento del dispositivo está estancado	El servicio que supervisa el estado del hardware de almacenamiento ha detenido la generación de informes. 1. Comprobar el estado del servicio de estado del sistema eos en el so básico 2. Si el servicio está en estado detenido o error, reinicie el servicio. 3. Si esta alerta persiste, póngase en contacto con el soporte técnico.
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. 1. Use System Manager de SANtricity para comprobar los componentes de hardware y seguir las acciones recomendadas. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600

Nombre de alerta	Descripción y acciones recomendadas
Se ha superado la temperatura del aparato	Se ha excedido la temperatura nominal o máxima del controlador de almacenamiento del aparato. 1. Determine si hay otra alerta que afecte a este nodo. Es posible que esta alerta se resuelva cuando se resuelve la otra alerta. 2. Investigue las posibles razones del aumento de temperatura, como un fallo del ventilador o del sistema HVAC. 3. Si esta alerta persiste, póngase en contacto con el soporte técnico.
Se ha eliminado el sensor de temperatura del aparato	Se ha quitado un sensor de temperatura. Póngase en contacto con el soporte técnico.
Error del compactador automático de Cassandra	El compactador automático Cassandra ha experimentado un error. El compactador automático Cassandra existe en todos los nodos de almacenamiento y gestiona el tamaño de la base de datos Cassandra para sobrescribir y eliminar cargas de trabajo pesadas. Mientras esta condición persiste, determinadas cargas de trabajo experimentan un consumo de metadatos inesperadamente alto. 1. Determine si hay otra alerta que afecte a este nodo. Es posible que esta alerta se resuelva cuando se resuelve la otra alerta. 2. Póngase en contacto con el soporte técnico.
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. 1. Asegúrese de que el servicio rsyslog esté en ejecución en el nodo. 2. Si es necesario, reinicie el servicio rsyslog en el nodo mediante el comando `service rsyslog restart`. 3. Si no se puede reiniciar el servicio rsyslog y no se guardan mensajes de auditoría en los nodos de administrador, póngase en contacto con el soporte técnico. Los registros de auditoría se perderán si esta condición no se corrige.
Las métricas del compactador automático de Cassandra no están actualizadas	Las métricas que describen al compactador automático Cassandra no están actualizadas. El compactador automático Cassandra existe en todos los nodos de almacenamiento y gestiona el tamaño de la base de datos Cassandra para sobrescribir y eliminar cargas de trabajo pesadas. Mientras la alerta persiste, determinadas cargas de trabajo experimentan un consumo de metadatos inesperadamente alto. 1. Determine si hay otra alerta que afecte a este nodo. Es posible que esta alerta se resuelva cuando se resuelve la otra alerta. 2. Póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
Error de comunicación de Cassandra	Los nodos que ejecutan el servicio Cassandra tienen problemas para comunicarse entre sí. Esta alerta indica que algo está interfiriendo con las comunicaciones entre nodos. Es posible que haya un problema de red o que el servicio Cassandra esté inactivo en uno o más nodos de almacenamiento. 1. Determine si hay otra alerta que afecte a uno o más nodos de almacenamiento. Es posible que esta alerta se resuelva cuando se resuelve la otra alerta. 2. Compruebe si hay un problema de red que pueda afectar a uno o más nodos de almacenamiento. 3. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. 4. Para cada nodo de almacenamiento del sistema, seleccione **SSM** > **Servicios**. Compruebe que el estado del servicio Cassandra sea "en ejecución". 5. Si Cassandra no está en ejecución, siga los pasos de iniciar o reiniciar un servicio. 6. Si ahora se están ejecutando todas las instancias del servicio Cassandra y no se resuelve la alerta, póngase en contacto con el soporte técnico.
Compacciones de Cassandra sobrecargadas	El proceso de compactación de Cassandra está sobrecargado. Si se sobrecarga el proceso de compactación, es posible que el rendimiento de lectura se degrade y que se pueda utilizar RAM. Es posible que el servicio Cassandra también deje de responder o se bloquee. 1. Reinicie el servicio Cassandra siguiendo los pasos de reinicio de un servicio. 2. Si esta alerta persiste, póngase en contacto con el soporte técnico.
Las métricas de reparación de Cassandra están desfasadas	Las métricas que describen los trabajos de reparación de Cassandra están desactualizadas. Si esta condición persiste durante más de 48 horas, las consultas de cliente, como los listados de cubos, podrían mostrar datos eliminados. 1. Reiniciar el nodo. En Grid Manager, vaya a **NODES**, seleccione el nodo y seleccione la ficha tareas. 2. Si esta alerta persiste, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
El progreso de reparación de Cassandra es lento	El progreso de las reparaciones de la base de datos de Cassandra es lento. Cuando las reparaciones de la base de datos son lentas, las operaciones de coherencia de datos de Cassandra se ven obstaculizadas. Si esta condición persiste durante más de 48 horas, las consultas de cliente, como los listados de cubos, podrían mostrar datos eliminados. 1. Confirme que todos los nodos de almacenamiento están en línea y no hay alertas relacionadas con la red. 2. Supervise esta alerta hasta durante 2 días para ver si el problema se resuelve por sí solo. 3. Si las reparaciones de la base de datos continúan avanzando lentamente, póngase en contacto con el soporte técnico.
El servicio de reparación de Cassandra no está disponible	El servicio de reparación de Cassandra no está disponible. El servicio de reparación de Cassandra existe en todos los nodos de almacenamiento y proporciona funciones de reparación cruciales para la base de datos Cassandra. Si esta condición persiste durante más de 48 horas, las consultas de cliente, como los listados de cubos, podrían mostrar datos eliminados. 1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. 2. Para cada nodo de almacenamiento del sistema, seleccione **SSM** > **Servicios**. Asegúrese de que el estado del servicio Cassandra Reaper es "en ejecución". 3. Si Cassandra Reaper no está en funcionamiento, siga los pasos para seguir los pasos de iniciar o reiniciar un servicio. 4. Si todas las instancias del servicio Cassandra Reaper se están ejecutando y la alerta no se resuelve, póngase en contacto con el soporte técnico.
Tablas dañadas en Cassandra	Cassandra detectó daños en la tabla. Cassandra se reinicia automáticamente si detecta daños en la tabla. Póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
Error de conectividad del pool de almacenamiento en cloud	La comprobación del estado de Cloud Storage Pools detectó uno o más errores nuevos. 1. Vaya a la sección Cloud Storage Pools de la página Storage Pools. 2. Mire la columna Last error para determinar qué pool de almacenamiento en cloud tiene un error. 3. Consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.
El arrendamiento DHCP ha caducado	El arrendamiento DHCP de una interfaz de red caducó. Si el arrendamiento DHCP ha caducado, siga las acciones recomendadas: 1. Compruebe que haya conectividad entre este nodo y el servidor DHCP en la interfaz afectada. 2. Compruebe que haya direcciones IP disponibles para asignarlas en la subred afectada en el servidor DHCP. 3. Compruebe que haya una reserva permanente para la dirección IP configurada en el servidor DHCP. También puede usar la herramienta StorageGRID Change IP para asignar una dirección IP estática fuera del grupo de direcciones DHCP. Consulte instrucciones de recuperación y mantenimiento.
El arrendamiento DHCP caduca pronto	El arrendamiento DHCP de una interfaz de red caduca pronto. Para evitar que caduque el arrendamiento DHCP, siga las acciones recomendadas: 1. Compruebe que haya conectividad entre este nodo y el servidor DHCP en la interfaz afectada. 2. Compruebe que haya direcciones IP disponibles para asignarlas en la subred afectada en el servidor DHCP. 3. Compruebe que haya una reserva permanente para la dirección IP configurada en el servidor DHCP. También puede usar la herramienta StorageGRID Change IP para asignar una dirección IP estática fuera del grupo de direcciones DHCP. Consulte instrucciones de recuperación y mantenimiento.

Nombre de alerta	Descripción y acciones recomendadas
Servidor DHCP no disponible	El servidor DHCP no está disponible. El nodo StorageGRID no puede comunicarse con el servidor DHCP. El arrendamiento DHCP de la dirección IP del nodo no se puede validar. 1. Compruebe que haya conectividad entre este nodo y el servidor DHCP en la interfaz afectada. 2. Compruebe que haya direcciones IP disponibles para asignarlas en la subred afectada en el servidor DHCP. 3. Compruebe que haya una reserva permanente para la dirección IP configurada en el servidor DHCP. También puede usar la herramienta StorageGRID Change IP para asignar una dirección IP estática fuera del grupo de direcciones DHCP. Consulte instrucciones de recuperación y mantenimiento.
La actividad de I/o del disco es muy lenta	Una I/o de disco muy lenta puede afectar al rendimiento de la StorageGRID. 1. Si el problema está relacionado con un nodo de un dispositivo de almacenamiento, use System Manager de SANtricity para comprobar si hay unidades defectuosas, unidades con fallos previstos o reparaciones de la unidad en curso. Compruebe también el estado de los enlaces de Fibre Channel o SAS entre las controladoras de almacenamiento y de computación del dispositivo para ver si hay algún enlace inactivo o si se muestran tasas de error excesivas. 2. Examine el sistema de almacenamiento que aloja los volúmenes de este nodo para determinar y corregir la causa raíz de la actividad de I/o lenta 3. Si esta alerta persiste, póngase en contacto con el soporte técnico. **Nota:** los nodos afectados podrían desactivar los servicios y reiniciarse para evitar que el rendimiento general de la red se vea afectado. Cuando se borra la condición subyacente y estos nodos detectan el rendimiento de I/o normal, este regresa al servicio completo automáticamente.

Nombre de alerta	Descripción y acciones recomendadas

Fallo de reequilibrio de EC	La tarea de reequilibrar los datos codificados para borrado en los nodos de almacenamiento ha fallado o ha sido pausada por el usuario.
	
	1. Compruebe que todos los nodos de almacenamiento del sitio que se va a reequilibrar estén en línea y disponibles.
	2. Asegúrese de que no hay fallos de volumen en el sitio que se está reequilibra. Si lo hay, finalice el trabajo de reequilibrio de EC para poder ejecutar un trabajo de reparación.
	
	`'rebalance-data terminate --job-id <ID>'`
	
	3. Asegúrese de que no hay fallos de servicio en el sitio que se está reteniendo. Si un servicio no se está ejecutando, siga los pasos para iniciar o reiniciar un servicio en las instrucciones de recuperación y mantenimiento.
	4. Después de resolver cualquier problema, reinicie el trabajo ejecutando el siguiente comando en el nodo de administración principal:
	
	`'rebalance-data start --job-id <ID>'`
	
	5. Si no puede resolver el problema, póngase en contacto con el soporte técnico.

Fallo de reparación de EC	Se ha producido un error o se ha detenido un trabajo de reparación de datos codificados mediante borrado. 1. Asegúrese de que haya suficientes nodos de almacenamiento o volúmenes disponibles para sustituir el volumen o el nodo de almacenamiento con errores. 2. Compruebe que haya suficientes nodos de almacenamiento disponibles para cumplir la política de ILM activa. 3. Asegúrese de que no haya problemas de conectividad de red. 4. Después de resolver cualquier problema, reinicie el trabajo ejecutando el siguiente comando en el nodo de administración principal: `'repair-data start-ec-node-repair --repair-id <ID>'` 5. Si no puede resolver el problema, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
Reparación EC bloqueada	Se ha detenido una tarea de reparación de datos codificados mediante borrado. 1. Asegúrese de que haya suficientes nodos de almacenamiento o volúmenes disponibles para sustituir el volumen o el nodo de almacenamiento con errores. 2. Asegúrese de que no haya problemas de conectividad de red. 3. Después de resolver cualquier problema, compruebe si la alerta se resuelve. Para ver un informe más detallado sobre el progreso de la reparación, ejecute el siguiente comando en el nodo de administración principal: `'repair-data show-ec-repair-status --repair-id <ID>'` 4. Si no puede resolver el problema, póngase en contacto con el soporte técnico.
Error en la notificación por correo electrónico	No se pudo enviar la notificación por correo electrónico para una alerta. Esta alerta se activa cuando falla una notificación por correo electrónico de alerta o no se puede entregar un correo electrónico de prueba (enviado desde la página **ALERTAS** > **Configuración de correo electrónico**). 1. Inicie sesión en Grid Manager desde el nodo de administración indicado en la columna **Sitio/nodo** de la alerta. 2. Vaya a la página **ALERTS** > **Configuración de correo electrónico**, compruebe los ajustes y cámbielos si es necesario. 3. Haga clic en **Enviar correo electrónico de prueba** y compruebe el correo electrónico en la bandeja de entrada de un destinatario de prueba. Es posible que se active una nueva instancia de esta alerta si no se puede enviar el correo electrónico de prueba. 4. Si no se ha podido enviar el correo electrónico de prueba, confirme que el servidor de correo electrónico está en línea. 5. Si el servidor funciona, seleccione **SUPPORT** > **Tools** > **Logs** y recoja el registro del nodo Admin. Especifique un período de tiempo que sea 15 minutos antes y después del momento de la alerta. 6. Extraiga el archivo descargado y revise el contenido de `prometheus.log` (`_/GID<gid><time_stamp>/<site_node>/<time_stamp>/metrics/prometheus.log`). 7. Si no puede resolver el problema, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
Caducidad de los certificados de cliente configurados en la página certificados	Uno o varios certificados de cliente configurados en la página certificados están a punto de expirar. 1. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación, seleccione la ficha **Cliente**. 2. Seleccione un certificado que caducará pronto. 3. Seleccione **Adjuntar nuevo certificado** a. cargar o generar un nuevo certificado. 4. Repita estos pasos para cada certificado que caducará pronto.
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. 1. Seleccione **CONFIGURACIÓN** > **Red** > **terminales de equilibrador de carga**. 2. Seleccione un extremo que tenga un certificado que caducará pronto. 3. Seleccione **Editar punto final** para cargar o generar un nuevo certificado. 4. Repita estos pasos para cada extremo que tenga un certificado caducado o uno que caducará pronto. Para obtener más información acerca de la gestión de los puntos finales del equilibrador de carga, consulte Instrucciones para administrar StorageGRID.
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. 1. Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados**. 2. En la ficha **Global**, seleccione **Certificado de interfaz de administración**. 3. Cargue un nuevo certificado de interfaz de gestión.
Caducidad de certificado de servidor global para la API de S3 y Swift	El certificado de servidor utilizado para acceder a los 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.

Nombre de alerta	Descripción y acciones recomendadas
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. 1. Actualice el certificado de CA en el servidor de syslog externo. 2. Obtenga una copia del certificado de CA actualizado. 3. Desde Grid Manager, vaya a **CONFIGURACIÓN** > **Supervisión** > **servidor de auditoría y syslog**. 4. Seleccione **Editar servidor syslog externo**. 5. Seleccione **examinar** para cargar el nuevo certificado. 6. Complete el asistente de configuración para guardar el nuevo certificado y la nueva clave.
Vencimiento del certificado de cliente de syslog externo	El certificado de cliente para un servidor de syslog externo está a punto de expirar. 1. Desde Grid Manager, vaya a **CONFIGURACIÓN** > **Supervisión** > **servidor de auditoría y syslog**. 2. Seleccione **Editar servidor syslog externo**. 3. Seleccione **examinar** para cargar el nuevo certificado. 4. Seleccione **examinar** para cargar la nueva clave privada. 5. Complete el asistente de configuración para guardar el nuevo certificado y la nueva clave.
Vencimiento del certificado de servidor de syslog externo	El certificado de servidor presentado por el servidor de syslog externo está a punto de expirar. 1. Actualice el certificado de servidor en el servidor de syslog externo. 2. Si anteriormente utilizó la API de Grid Manager para proporcionar un certificado de servidor para la validación de certificados, cargue el certificado de servidor actualizado con la API.
Error de reenvío del servidor de syslog externo	El nodo no puede reenviar registros al servidor de syslog externo. 1. Desde Grid Manager, vaya a **CONFIGURACIÓN** > **Supervisión** > **servidor de auditoría y syslog**. 2. Seleccione **Editar servidor syslog externo**. 3. Avance a través del asistente de configuración hasta que pueda seleccionar **Enviar mensajes de prueba**. 4. Seleccione **Enviar mensajes de prueba** para determinar por qué no se pueden reenviar registros al servidor syslog externo. 5. Resuelva los problemas notificados.

Nombre de alerta	Descripción y acciones recomendadas
Discrepancia de MTU de red de grid	La configuración de la unidad de transmisión máxima (MTU) para la interfaz de red de cuadrícula (eth0) difiere significativamente entre los nodos de la cuadrícula. 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. Consulte las instrucciones para la alerta de discrepancia de MTU de red de cuadrícula en Solucionar problemas de red, hardware y plataforma.
Uso de montón Java alto	Se está utilizando un alto porcentaje de espacio de pila Java. Si el montón de Java se llena, los servicios de metadatos pueden dejar de estar disponibles y las solicitudes de cliente pueden fallar. 1. Revise la actividad de ILM en la consola. Esta alerta puede resolverse por sí sola cuando se reduce la carga de trabajo de ILM. 2. Determine si hay otra alerta que afecte a este nodo. Es posible que esta alerta se resuelva cuando se resuelve la otra alerta. 3. Si esta alerta persiste, póngase en contacto con el soporte técnico.
Alta latencia para consultas de metadatos	El tiempo medio para las consultas de metadatos de Cassandra es demasiado largo. Un aumento en la latencia de las consultas puede deberse a un cambio de hardware, como la sustitución de un disco, un cambio de carga de trabajo, como un aumento repentino de las búsquedas o un cambio de red, como un problema de comunicación entre nodos y sitios. 1. Determine si hubo cambios de hardware, carga de trabajo o red en torno al momento en que aumentó la latencia de consulta. 2. Si no puede resolver el problema, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
Fallo de sincronización de la federación de identidades	No se pueden sincronizar los grupos federados y los usuarios del origen de identidades. 1. Confirmar que el servidor LDAP configurado está en línea y disponible. 2. Revise la configuración en la página Federación de identidades. Confirme que todos los valores son actuales. Consulte Usar la federación de identidades En las instrucciones para administrar StorageGRID. 3. Haga clic en **probar conexión** para validar la configuración del servidor LDAP. 4. Si no puede resolver el problema, póngase en contacto con el soporte técnico.
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. 1. Inicie sesión en el Administrador de inquilinos. 2. Confirmar que el servidor LDAP configurado por el inquilino está en línea y disponible. 3. Revise la configuración en la página Federación de identidades. Confirme que todos los valores son actuales. Consulte Usar la federación de identidades en las instrucciones de uso de una cuenta de inquilino. 4. Haga clic en **probar conexión** para validar la configuración del servidor LDAP. 5. Si no puede resolver el problema, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
Se puede lograr una colocación de ILM	No se puede obtener una instrucción de colocación en una regla de ILM para ciertos objetos. Esta alerta indica que un nodo requerido por una instrucción de colocación no está disponible o que una regla de ILM está mal configurada. Por ejemplo, una regla puede especificar más copias replicadas que los nodos de almacenamiento. 1. Asegúrese de que todos los nodos estén en línea. 2. Si todos los nodos están en línea, revise las instrucciones de colocación de todas las reglas de ILM que estén utilizadas la política activa de ILM. Confirme que hay instrucciones válidas para todos los objetos. Consulte instrucciones para gestionar objetos con la gestión del ciclo de vida de la información. 3. Si es necesario, actualice la configuración de reglas y active una nueva directiva. **Nota:** la alerta puede tardar hasta 1 día en aclararse. 4. Si el problema persiste, póngase en contacto con el soporte técnico. **Nota:** esta alerta puede aparecer durante una actualización y puede persistir durante 1 día después de que la actualización se haya completado correctamente. Cuando una actualización activa esta alerta, se desactiva por sí sola.

Nombre de alerta	Descripción y acciones recomendadas
El periodo de análisis de ILM es demasiado largo	El tiempo necesario para analizar, evaluar objetos y aplicar ILM es demasiado largo. Si el tiempo estimado para completar un análisis completo de ILM de todos los objetos es demasiado largo (consulte **período de análisis - estimado** en el Panel), la política de ILM activa podría no aplicarse a los objetos recién procesados. Es posible que los cambios en la política de ILM no se apliquen a los objetos existentes. 1. Determine si hay otra alerta que afecte a este nodo. Es posible que esta alerta se resuelva cuando se resuelve la otra alerta. 2. Confirme que todos los nodos de almacenamiento están en línea. 3. Reduzca temporalmente la cantidad de tráfico de clientes. Por ejemplo, en Grid Manager, seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico** y cree una directiva que limite el ancho de banda o el número de solicitudes. 4. Si se sobrecargan las operaciones de I/o de disco o la CPU, intente reducir la carga o aumente el recurso. 5. Si es necesario, actualice las reglas de ILM para usar la ubicación síncrona (predeterminado para las reglas creadas después de StorageGRID 11.3). 6. Si esta alerta persiste, póngase en contacto con el soporte técnico. Administre StorageGRID
Tasa baja de análisis de ILM	La tasa de análisis de ILM se establece en menos de 100 objetos por segundo. Esta alerta indica que alguien ha cambiado la tasa de análisis de ILM del sistema a menos de 100 objetos por segundo (valor predeterminado: 400 objetos por segundo). Es posible que la política de ILM activa no se aplique a los objetos recién procesados. Los cambios posteriores en la política de ILM no se aplicarán a los objetos existentes. 1. Determine si se realizó un cambio temporal en la tasa del análisis de ILM como parte de una investigación de soporte en curso. 2. Póngase en contacto con el soporte técnico. No cambie nunca la tasa de análisis de ILM sin contactar con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
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. 1. Con el software KMS, actualice el certificado de CA para el servidor de gestión de claves. 2. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**. 3. Seleccione el KMS que tiene una advertencia de estado de certificado. 4. Seleccione **Editar**. 5. Seleccione **Siguiente** para ir a Paso 2 (cargar certificado de servidor). 6. Seleccione **examinar** para cargar el nuevo certificado. 7. Seleccione **Guardar**. Administre StorageGRID
Vencimiento del certificado de cliente DE KMS	El certificado de cliente para un servidor de gestión de claves está a punto de expirar. 1. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**. 2. Seleccione el KMS que tiene una advertencia de estado de certificado. 3. Seleccione **Editar**. 4. Seleccione **Siguiente** para ir al Paso 3 (cargar certificados de cliente). 5. Seleccione **examinar** para cargar el nuevo certificado. 6. Seleccione **examinar** para cargar la nueva clave privada. 7. Seleccione **Guardar**. Administre StorageGRID
No se ha podido cargar la configuración DE KMS	La configuración del servidor de gestión de claves existe, pero no pudo cargar. 1. Determine si hay otra alerta que afecte a este nodo. Es posible que esta alerta se resuelva cuando se resuelve la otra alerta. 2. Si esta alerta persiste, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
Error de conectividad DE KMS	Un nodo de dispositivo no pudo conectarse con el servidor de gestión de claves para su sitio. 1. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**. 2. Confirmar que las entradas del puerto y el nombre de host son correctas. 3. Confirme que el certificado de servidor, el certificado de cliente y la clave privada del certificado de cliente son correctos y no han caducado. 4. Asegúrese de que la configuración del firewall permite que el nodo del dispositivo se comunique con el KMS especificado. 5. Corrija cualquier problema con las redes o con DNS. 6. Si necesita ayuda o esta alerta continúa, póngase en contacto con el soporte técnico.
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. 1. Confirme que el KMS asignado al sitio está utilizando el nombre correcto para la clave de cifrado y cualquier versión anterior. 2. Si necesita ayuda o esta alerta continúa, póngase en contacto con el soporte técnico.
Error en la rotación de la clave de cifrado DE KMS	Todos los volúmenes de dispositivos se descifraron, pero uno o más volúmenes no pudieron girar a la última clave.Póngase en contacto con el soporte técnico.
KMS no está configurado	No existe ningún servidor de gestión de claves para este sitio. 1. En Grid Manager, seleccione **CONFIGURACIÓN** > **Seguridad** > **servidor de administración de claves**. 2. Agregue un KMS para este sitio o agregue un KMS predeterminado. Administre StorageGRID
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. 1. Determine si hay otra alerta que afecte a este nodo. Es posible que esta alerta se resuelva cuando se resuelve la otra alerta. 2. Asegúrese de que el servidor de gestión de claves (KMS) tenga la clave de cifrado configurada y las versiones anteriores de claves. 3. Si necesita ayuda o esta alerta continúa, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
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. 1. Con el software KMS, actualice el certificado de servidor para el servidor de gestión de claves. 2. Si necesita ayuda o esta alerta continúa, póngase en contacto con el soporte técnico. Administre StorageGRID
Cola de auditoría grande	La cola de discos para los mensajes de auditoría está llena. 1. Compruebe la carga en el sistema. Si ha habido un número importante de transacciones, la alerta se debería resolver por sí misma con el tiempo y puede ignorar la alerta. 2. Si la alerta 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. 3. Reduzca la velocidad de funcionamiento 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 Desactivada (**CONFIGURATION** > **Monitoring** > **Audit and syslog Server**). Revisar los registros de auditoría
Se ha detectado una actividad de equilibrador de carga de CLB heredada	Algunos clientes podrían conectarse al servicio de equilibrio de carga CLB obsoleto usando el certificado API S3 y Swift predeterminado. 1. Para simplificar futuras actualizaciones, instale un certificado de API Swift y S3 personalizado en la ficha **Global** de la página **certificados**. A continuación, asegúrese de que todos los clientes S3 o Swift que se conectan al CLB heredado tengan el nuevo certificado. 2. Cree uno o varios puntos finales del equilibrador de carga. A continuación, dirija todos los clientes de S3 y Swift existentes a estos extremos. Si necesita reasignar el puerto del cliente, póngase en contacto con el soporte técnico. Otra actividad podría activar esta alerta, incluidos los análisis de puertos. Para determinar si el servicio CLB obsoleto está en uso, consulte `storagegrid_private_clb_http_connection_established_successful` Métrica Prometheus. Si es necesario, silencia o desactiva esta regla de alerta si el servicio CLB ya no está en uso.

Nombre de alerta	Descripción y acciones recomendadas
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. 1. Desde Grid Manager, vaya a **CONFIGURACIÓN** > **Supervisión** > **servidor de auditoría y syslog**. 2. Seleccione **Editar servidor syslog externo**. 3. Avance a través del asistente de configuración hasta que pueda seleccionar **Enviar mensajes de prueba**. 4. Seleccione **Enviar mensajes de prueba** para determinar por qué no se pueden reenviar registros al servidor syslog externo. 5. Resuelva los problemas notificados.
Capacidad de disco de registro de auditoría baja	El espacio disponible para los registros de auditoría es bajo. 1. Supervise esta alerta para ver si el problema se resuelve por sí solo y el espacio en disco vuelve a estar disponible. 2. Póngase en contacto con el soporte técnico si el espacio disponible sigue disminuyendo.
Memoria del nodo baja disponible	La cantidad de RAM disponible en un nodo es baja. Una RAM disponible baja podría indicar un cambio en la carga de trabajo o una pérdida de memoria con uno o más nodos. 1. Supervise esta alerta para ver si el problema se resuelve por sí solo. 2. Si la memoria disponible está por debajo del umbral de alerta principal, póngase en contacto con el soporte técnico.
Poco espacio libre para la piscina de almacenamiento	La cantidad de espacio disponible para almacenar datos de objetos en una agrupación de almacenamiento es baja. 1. Seleccione **ILM** > **agrupaciones de almacenamiento**. 2. Seleccione la agrupación de almacenamiento que aparece en la alerta y seleccione **Ver detalles**. 3. Determine dónde se requiere capacidad de almacenamiento adicional. Es posible añadir nodos de almacenamiento a cada sitio del pool de almacenamiento o añadir volúmenes de almacenamiento (LUN) a uno o varios nodos de almacenamiento existentes. 4. Lleve a cabo un procedimiento de ampliación para aumentar la capacidad de almacenamiento. Amplíe su grid

Nombre de alerta	Descripción y acciones recomendadas
Memoria del nodo instalada baja	La cantidad de memoria instalada en un nodo es baja. Aumente la cantidad de RAM disponible para la máquina virtual o el host Linux. Compruebe el valor de umbral de la alerta principal para determinar los requisitos mínimos predeterminados para un nodo StorageGRID. Consulte las instrucciones de instalación de su plataforma: • Instale Red Hat Enterprise Linux o CentOS • Instalar Ubuntu o Debian • Instale VMware
Almacenamiento de metadatos bajo	El espacio disponible para almacenar metadatos de objetos es bajo. **Alerta crítica** 1. Detenga la ingestión de objetos. 2. Añada inmediatamente nodos de almacenamiento en un procedimiento de ampliación. **Alerta mayor** Añada inmediatamente nodos de almacenamiento en un procedimiento de ampliación. **Alerta menor** 1. Supervise la velocidad a la que se está utilizando el espacio de metadatos de los objetos. Seleccione **NODES** > ***Storage Node*** > **Storage**, y vea el gráfico almacenamiento usado - metadatos de objeto. 2. Añada nodos de almacenamiento en un procedimiento de expansión Lo antes posible.. 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 las instrucciones para la alerta de almacenamiento de metadatos bajos en Solucionar problemas de metadatos.
Capacidad de disco de métrica baja	El espacio disponible para la base de datos de métricas es bajo. 1. Supervise esta alerta para ver si el problema se resuelve por sí solo y el espacio en disco vuelve a estar disponible. 2. Póngase en contacto con el soporte técnico si el espacio disponible sigue disminuyendo.

Nombre de alerta	Descripción y acciones recomendadas
Almacenamiento de objetos bajo	El espacio disponible para almacenar datos de objeto es bajo. Realice un procedimiento de expansión. Es posible añadir volúmenes de almacenamiento (LUN) a los nodos de almacenamiento existentes, o bien añadir nuevos nodos de almacenamiento. Solucionar problemas de la alerta de almacenamiento de datos de objeto bajo Amplíe su grid
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. Para saber cómo se resuelve esta alerta, vaya a. Solucionar los problemas de las alertas de anulación de la Marca de agua de sólo lectura baja.
Baja capacidad de disco raíz	El espacio disponible para el disco raíz es bajo. 1. Supervise esta alerta para ver si el problema se resuelve por sí solo y el espacio en disco vuelve a estar disponible. 2. Póngase en contacto con el soporte técnico si el espacio disponible sigue disminuyendo.
Baja capacidad de datos del sistema	El espacio disponible para los datos del sistema StorageGRID en la `/var/local` el sistema de archivos es bajo. 1. Supervise esta alerta para ver si el problema se resuelve por sí solo y el espacio en disco vuelve a estar disponible. 2. Póngase en contacto con el soporte técnico si el espacio disponible sigue disminuyendo.
Bajo espacio libre en el directorio tmp	El espacio disponible en el directorio /tmp es bajo. 1. Supervise esta alerta para ver si el problema se resuelve por sí solo y el espacio en disco vuelve a estar disponible. 2. Póngase en contacto con el soporte técnico si el espacio disponible sigue disminuyendo.

Nombre de alerta	Descripción y acciones recomendadas
Error de conectividad de red de los nodos	Se han producido errores al transferir datos entre nodos. Los errores de conectividad de red pueden aclararse sin intervención manual. Si los errores no se borran, póngase en contacto con el soporte técnico. Consulte las instrucciones para la alarma de error de recepción de red (NRER) en Solucionar problemas de red, hardware y plataforma.
Error de trama de recepción de red del nodo	Un alto porcentaje de las tramas de red recibidas por un nodo tiene errores. Esta alerta puede indicar un problema de hardware, como un cable defectuoso o un transceptor fallido en cualquiera de los extremos de la conexión Ethernet. 1. Si utiliza un dispositivo, intente reemplazar cada transceptor SFP+ o SFP28 y cable, uno a la vez, para ver si la alerta se borra. 2. Si esta alerta persiste, póngase en contacto con el soporte técnico.
El nodo no está sincronizado con el servidor NTP	La hora del nodo no está sincronizada con el servidor del protocolo de hora de red (NTP). 1. Compruebe que ha especificado al menos cuatro servidores NTP externos, cada uno de los cuales proporciona una referencia estratum 3 o superior. 2. Compruebe que todos los servidores NTP funcionan con normalidad. 3. Compruebe las conexiones con los servidores NTP. Asegúrese de que no están bloqueados por un firewall.
El nodo no está bloqueado con el servidor NTP	El nodo no está bloqueado por un servidor de protocolo de tiempo de red (NTP). 1. Compruebe que ha especificado al menos cuatro servidores NTP externos, cada uno de los cuales proporciona una referencia estratum 3 o superior. 2. Compruebe que todos los servidores NTP funcionan con normalidad. 3. Compruebe las conexiones con los servidores NTP. Asegúrese de que no están bloqueados por un firewall.
La red del nodo que no sea del dispositivo está inactiva	Uno o más dispositivos de red están inactivos o desconectados. Esta alerta indica que no se puede acceder a una interfaz de red (eth) para un nodo instalado en una máquina virtual o un host de Linux. Póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
Error en la comprobación de la existencia del objeto	Error en el trabajo de comprobación de la existencia del objeto. 1. Seleccione **MANTENIMIENTO > verificación de existencia de objeto**. 2. Anote el mensaje de error. Realice las acciones correctivas oportunas: **Error al iniciar**, **pérdida de conexión**, **error desconocido** a. Asegúrese de que los nodos de almacenamiento y los volúmenes que se incluyen en el trabajo estén en línea y disponibles. b. Compruebe que no se produzcan errores de volumen o servicio en los nodos de almacenamiento. Si un servicio no está en ejecución, inicie o reinicie el servicio. Consulte instrucciones de recuperación y mantenimiento. c. Asegúrese de que el control de consistencia seleccionado puede estar satisfecho. d. Después de resolver cualquier problema, seleccione **Reintentar**. El trabajo se reanudará desde el último estado válido. **Error crítico de almacenamiento en volumen** e. Recupere el volumen con errores. Consulte instrucciones de recuperación y mantenimiento. f. Seleccione **Reintentar**. g. Una vez completado el trabajo, cree otro trabajo para que los volúmenes restantes del nodo coman en busca de errores adicionales. 3. Si no puede resolver los problemas, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
Comprobación de existencia de objeto bloqueada	El trabajo de comprobación de la existencia del objeto se ha detenido. El trabajo de comprobación de la existencia de objetos no puede continuar. Uno o varios nodos de almacenamiento o volúmenes incluidos en el trabajo no tienen conexión o no responden, o el control de coherencia seleccionado ya no se puede satisfacer porque hay demasiados nodos inactivos o no disponibles. 1. Asegúrese de que todos los nodos y volúmenes de almacenamiento que se van a comprobar estén en línea y disponibles (seleccione **NODOS**). 2. Asegúrese de que hay suficientes nodos de almacenamiento en línea y disponibles para permitir que el nodo de coordinador actual lea metadatos del objeto mediante el control de consistencia seleccionado. Si es necesario, inicie o reinicie un servicio. Consulte instrucciones de recuperación y mantenimiento. Cuando se resuelven los pasos 1 y 2, el trabajo comenzará automáticamente donde lo dejó. 3. Si el control de coherencia seleccionado no se puede satisfacer, cancele el trabajo e inicie otro con un control de coherencia inferior. 4. Si no puede resolver los problemas, póngase en contacto con el soporte técnico.
Objetos perdidos	Se han perdido uno o más objetos de la cuadrícula. Esta alerta puede indicar que los datos se han perdido de forma permanente y que no se pueden recuperar. 1. Investigue esta alerta inmediatamente. Es posible que deba tomar medidas para evitar la pérdida de datos adicional. También puede restaurar un objeto perdido si realiza una acción rápida. Solucionar problemas de datos de objetos perdidos o faltantes 2. Cuando se resuelva el problema subyacente, restablezca el contador: a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. b. Para el nodo de almacenamiento que generó la alerta, seleccione ***site*** > ***grid node*** > **LDR** > **Data Store** > **Configuración** > **Principal**. c. Seleccione **Restablecer el recuento de objetos perdidos** y haga clic en **aplicar cambios**.

Nombre de alerta	Descripción y acciones recomendadas
Servicios de plataforma no disponibles	Hay muy pocos nodos de almacenamiento con el servicio RSM en ejecución o disponibles en un sitio. Asegúrese de que la mayoría de los nodos de almacenamiento que tienen el servicio RSM en el sitio afectado están en ejecución y en estado no-error. Consulte «"solución de problemas de servicios de plataforma" en la Instrucciones para administrar StorageGRID.
S3 PUT Object size demasiado grande	Un cliente de S3 intenta realizar una operación PUT Object que supera los límites de tamaño de S3. 1. Utilice el ID de inquilino que se muestra en los detalles de la alerta para identificar la cuenta de inquilino. 2. Vaya a **Soporte** > **Herramientas** > **registros** y recopile los registros de la aplicación para el nodo de almacenamiento que se muestra en los detalles de la alerta. Especifique un período de tiempo que sea 15 minutos antes y después del momento de la alerta. 3. Extraiga el archivo descargado y desplácese a la ubicación de `bycast.log` (`/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log`). 4. Busque el contenido de `bycast.log` para `"method=PUT"` E identifique la dirección IP del cliente S3 mirando el `clientIP` campo. 5. Informe a todos los usuarios clientes de que el tamaño máximo DE PUT Object es de 5 GIB. 6. Utilice cargas en varias partes para objetos de más de 5 GIB.

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.
	
	1. Compruebe el cable y la conexión física al puerto de red de administración 1.
	2. Resuelva cualquier problema de conexión. Consulte las instrucciones de instalación y mantenimiento del hardware del dispositivo.
	3. Si este puerto está desconectado a propósito, desactive esta regla. En Grid Manager, seleccione **ALERTS** > **Reglas**, seleccione la regla y haga clic en **Editar regla**. A continuación, desactive la casilla de verificación **Activado**.
	  ◦ Servicios de aplicaciones SG100 y SG1000
	  ◦ Deshabilitar reglas de alerta

Nombre de alerta	Descripción y acciones recomendadas
Enlace del dispositivo de servicios inactivo en la red de administración (o la red de clientes)	La interfaz del dispositivo con la red de administración (eth1) o la red de cliente (eth2) se reduce o se desconecta. 1. Compruebe los cables, SFP y conexiones físicas a la red StorageGRID. 2. Resuelva cualquier problema de conexión. Consulte las instrucciones de instalación y mantenimiento del hardware del dispositivo. 3. Si este puerto está desconectado a propósito, desactive esta regla. En Grid Manager, seleccione **ALERTS** > **Reglas**, seleccione la regla y haga clic en **Editar regla**. A continuación, desactive la casilla de verificación **Activado**. ◦ Servicios de aplicaciones SG100 y SG1000 ◦ Deshabilitar reglas de alerta
El dispositivo de servicios está desconectado en el puerto de red 1, 2, 3 o 4	El puerto de red 1, 2, 3 o 4 del dispositivo está inactivo o desconectado. 1. Compruebe los cables, SFP y conexiones físicas a la red StorageGRID. 2. Resuelva cualquier problema de conexión. Consulte las instrucciones de instalación y mantenimiento del hardware del dispositivo. 3. Si este puerto está desconectado a propósito, desactive esta regla. En Grid Manager, seleccione **ALERTS** > **Reglas**, seleccione la regla y haga clic en **Editar regla**. A continuación, desactive la casilla de verificación **Activado**. ◦ Servicios de aplicaciones SG100 y SG1000 ◦ Deshabilitar reglas de alerta

Nombre de alerta	Descripción y acciones recomendadas
La conectividad del almacenamiento del dispositivo de servicios está degradada	Uno de los dos SSD de un dispositivo de servicios ha fallado o está desincronado con el otro. La funcionalidad del dispositivo no se ve afectada, pero deberá solucionar el problema inmediatamente. Si ambas unidades fallan, el dispositivo ya no funcionará. 1. En Grid Manager, seleccione **NODES** > ***Services appliance* y, a continuación, seleccione la ficha hardware**. 2. Revise el mensaje en el campo **Storage RAID Mode**. 3. Si el mensaje muestra el progreso de una operación de resincronización, espere a que se complete la operación y confirme que se resolvió la alerta. Un mensaje de resincronización significa que el SSD se reemplazó recientemente o que está siendo resincronizado por otro motivo. 4. Si el mensaje indica que uno de los SSD presenta errores, sustituya el Lo antes posible. de la unidad con fallos. Para obtener instrucciones sobre cómo sustituir una unidad en un dispositivo de servicios, consulte la guía de instalación y mantenimiento de los dispositivos SG100 y SG1000. Servicios de aplicaciones SG100 y SG1000
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. 1. Compruebe el cable y la conexión física al puerto de red de administración 1. 2. Resuelva cualquier problema de conexión. Consulte las instrucciones de instalación y mantenimiento del hardware del dispositivo. 3. Si este puerto está desconectado a propósito, desactive esta regla. En Grid Manager, seleccione **ALERTS** > **Reglas**, seleccione la regla y haga clic en **Editar regla**. A continuación, desactive la casilla de verificación **Activado**. ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600 ◦ Deshabilitar reglas de alerta

Nombre de alerta	Descripción y acciones recomendadas
Enlace del dispositivo de almacenamiento inactivo en red de administrador (o red de cliente)	La interfaz del dispositivo con la red de administración (eth1) o la red de cliente (eth2) se reduce o se desconecta. 1. Compruebe los cables, SFP y conexiones físicas a la red StorageGRID. 2. Resuelva cualquier problema de conexión. Consulte las instrucciones de instalación y mantenimiento del hardware del dispositivo. 3. Si este puerto está desconectado a propósito, desactive esta regla. En Grid Manager, seleccione **ALERTS** > **Reglas**, seleccione la regla y haga clic en **Editar regla**. A continuación, desactive la casilla de verificación **Activado**. ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600 ◦ Deshabilitar reglas de alerta
El dispositivo de almacenamiento está desconectado en el puerto de red 1, 2, 3 o 4	El puerto de red 1, 2, 3 o 4 del dispositivo está inactivo o desconectado. 1. Compruebe los cables, SFP y conexiones físicas a la red StorageGRID. 2. Resuelva cualquier problema de conexión. Consulte las instrucciones de instalación y mantenimiento del hardware del dispositivo. 3. Si este puerto está desconectado a propósito, desactive esta regla. En Grid Manager, seleccione **ALERTS** > **Reglas**, seleccione la regla y haga clic en **Editar regla**. A continuación, desactive la casilla de verificación **Activado**. ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600 ◦ Deshabilitar reglas de alerta

Nombre de alerta	Descripción y acciones recomendadas
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. 1. Vaya al aparato para comprobar las luces indicadoras del puerto. 2. Si las luces de un puerto están apagadas, confirme que el cable está conectado correctamente. Si es necesario, sustituya el cable. 3. Espere hasta cinco minutos. **Nota:** Si es necesario sustituir un segundo cable, no lo desenchufe durante al menos 5 minutos. De lo contrario, el volumen raíz podría ser de sólo lectura, lo que requeriría reiniciar el hardware. 4. En Grid Manager, seleccione **NODES**. A continuación, seleccione la pestaña hardware del nodo que tenía el problema. Compruebe que la condición de alerta se ha resuelto.
Dispositivo de almacenamiento inaccesible	No se puede acceder a un dispositivo de almacenamiento. Esta alerta indica que no se puede montar un volumen ni acceder a él debido a un problema con un dispositivo de almacenamiento subyacente. 1. Compruebe el estado de todos los dispositivos de almacenamiento utilizados para el nodo: ◦ Si el nodo está instalado en una máquina virtual o un host Linux, siga las instrucciones de su sistema operativo para ejecutar diagnósticos de hardware o realizar una comprobación del sistema de archivos. ▪ Instale Red Hat Enterprise Linux o CentOS ▪ Instalar Ubuntu o Debian ▪ Instale VMware ◦ Si el nodo está instalado en un dispositivo SG100, SG1000 o SG6000, utilice el BMC. ◦ Si el nodo está instalado en un dispositivo SG5600 o SG5700, utilice System Manager de SANtricity. 2. Si es necesario, sustituir el componente. Consulte las instrucciones del aparato: ◦ Dispositivos de almacenamiento SG6000 ◦ Dispositivos de almacenamiento SG5700 ◦ Dispositivos de almacenamiento SG5600

Nombre de alerta	Descripción y acciones recomendadas
Uso de cuota de inquilino alto	Se está utilizando un porcentaje alto del espacio de cuota de arrendatario. Si un inquilino supera su cuota, se rechazan las nuevas ingests. **Nota:** esta regla de alerta está desactivada de forma predeterminada porque podría generar muchas notificaciones. 1. En Grid Manager, seleccione **ARRENDATARIOS**. 2. Ordene la tabla por **utilización de cuota**. 3. Seleccione un arrendatario cuya utilización de cuota sea cercana al 100%. 4. Realice una o ambas de las siguientes acciones: ◦ Seleccione **Editar** para aumentar la cuota de almacenamiento del arrendatario. ◦ Notifique al inquilino que su utilización de cuota es alta.
No es posible comunicarse con el nodo	Uno o varios servicios no responden o no se puede acceder al nodo. Esta alerta indica que un nodo está desconectado por un motivo desconocido. 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. Supervise esta alerta para ver si el problema se resuelve por sí solo. Si el problema persiste: 1. Determine si hay otra alerta que afecte a este nodo. Es posible que esta alerta se resuelva cuando se resuelve la otra alerta. 2. Confirme que todos los servicios de este nodo se están ejecutando. Si se detiene un servicio, intente iniciar el servicio. Consulte instrucciones de recuperación y mantenimiento. 3. Compruebe que el host para el nodo esté encendido. Si no lo es, inicie el host. **Nota:** Si se apaga más de un host, consulte instrucciones de recuperación y mantenimiento. 4. Determine si existe un problema de conectividad de red entre este nodo y el nodo de administrador. 5. Si no puede resolver la alerta, póngase en contacto con el soporte técnico.

Nombre de alerta	Descripción y acciones recomendadas
Reinicio de nodo inesperado	Un nodo se reinició de forma inesperada en las últimas 24 horas. 1. Supervise esta alerta. La alerta se borrará después de 24 horas. Sin embargo, si el nodo se reinicia de forma inesperada, esta alerta se volverá a activar. 2. Si no puede resolver la alerta, puede haber un error de hardware. Póngase en contacto con el soporte técnico.
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. 1. Determine si hay algún problema con el almacenamiento subyacente en un nodo de almacenamiento. Por ejemplo, ejecute diagnósticos de hardware o realice una comprobación del sistema de archivos. 2. Después de resolver cualquier problema de almacenamiento, ejecute la comprobación de existencia de objetos Para determinar si faltan copias replicadas, según lo definido en la política de ILM. 3. Supervise esta alerta. La alerta se borrará después de 24 horas, pero se activará de nuevo si el problema no se ha solucionado. 4. Si no puede resolver la alerta, póngase en contacto con el soporte técnico.

Métricas de Prometheus que se usan habitualmente

El servicio Prometheus en nodos de administración recopila métricas de series temporales de los servicios de todos los nodos. Aunque Prometheus recopila más de mil métricas, se requiere una cantidad relativamente pequeña para supervisar las operaciones de StorageGRID más importantes.

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.

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

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

En la siguiente tabla se enumeran las métricas Prometheus que se más utilizan. Puede consultar esta lista para comprender mejor las condiciones de las reglas de alerta predeterminadas o para crear las condiciones para reglas de alerta personalizadas.

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.

Métrica Prometheus	Descripción
alertmanager_retifations_failed_total	El número total de notificaciones de alertas con errores.
node_filesystem_avail_bytes	La cantidad de espacio de sistema de archivos disponible para usuarios que no son raíz en bytes.
Node_Memory_MemAvailable_bytes	Campo de información de memoria MemAvailable_bytes.
node_network_carrier	Valor de operador 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 están en estado óptimo.
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.

Métrica Prometheus	Descripción
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.

Métrica Prometheus	Descripción
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 por un servidor de protocolo de tiempo de red (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.

Métrica Prometheus	Descripción
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
storagegrid_storage_utilization_bytes	Una estimación del tamaño total de los datos de objetos codificados de replicación y borrado en el nodo de almacenamiento.

Métrica Prometheus	Descripción
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.

Métrica Prometheus	Descripción
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.

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 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.
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, no se pueden procesar las transacciones de procesamiento o recuperación. 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.

Codificación	Nombre	Servicio	Acción recomendada
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 o repositorio de auditoría, los mensajes se almacenan en una cola de disco. 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 multipath aparece como "degradado" (seleccione **SOPORTE** > **Herramientas** > **Topología de cuadrícula** y seleccione ***sitio*** > ***nodo de cuadrícula*** > **SSM** > **Eventos**), 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 que haya transcurrido al menos cinco minutos después de enchufarlo 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** > **Recursos** y compruebe que el estado de "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 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 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 de 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 de 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 de 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, o seleccione **SUPPORT** > **Tools** > **Grid topolog**, a continuación, seleccione ***site*** > ***grid node*** > **DDS** > **Resources** > **Overview** > **Main**. Si el problema persiste, póngase en contacto con el soporte técnico.
CAIH	Número de destinos de procesamiento disponibles	CLB	Esta alarma está obsoleta.

Codificación	Nombre	Servicio	Acción recomendada
CAQH	Número de destinos disponibles	CLB	Esta alarma se borra cuando se corrigen los problemas subyacentes de los servicios LDR disponibles. Asegúrese de que el componente HTTP de los servicios LDR esté en línea y funcionando normalmente. Si el problema persiste, póngase en contacto con el soporte técnico.
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.
CES	Sesiones entrantes: Establecido	CLB	Esta alarma se activa si hay 20,000 o más sesiones HTTP activas actualmente (abiertas) en el nodo de puerta de enlace. Si un cliente tiene demasiadas conexiones, puede ver fallos de conexión. Debe reducir la carga de trabajo.
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 en Grid Manager. Debe realizar un procedimiento de ampliación para añadir un nuevo Lo antes posible. a los nodos de almacenamiento. Consulte Amplíe su grid. 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.
CLBA	Estado CLB	CLB	Si se activa una alarma, seleccione **SOPORTE** > **Herramientas** > **topología de cuadrícula** y, a continuación, seleccione ***sitio*** > ***nodo de cuadrícula*** > **CLB** > **Descripción general** > **Principal** y **CLB** > **Alarmas** > **Principal** para determinar la causa de la alarma y solucionar el problema. Si el problema persiste, póngase en contacto con el soporte técnico.

Codificación	Nombre	Servicio	Acción recomendada
CLBE	Estado CLB	CLB	Si el valor del estado CLB es en espera, continúe supervisando la situación y, si el problema persiste, póngase en contacto con el servicio técnico. Si el estado es sin conexión y no hay problemas conocidos de hardware del servidor (por ejemplo, el servidor está desconectado) o tiempo de inactividad programado, reinicie el servicio. Si el problema persiste, póngase en contacto con el soporte técnico.
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.

Codificación	Nombre	Servicio	Acción recomendada
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.
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 codificado por 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 se aumenta, puede que haya un problema con el almacenamiento subyacente del nodo de almacenamiento. No se considera que falte una copia de los datos del objeto codificados para borrado hasta que el número de fragmentos perdidos o corruptos incumpla la tolerancia a fallos del código de borrado; por lo tanto, es posible tener un fragmento dañado y aún poder 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.

Codificación	Nombre	Servicio	Acción recomendada
HSTE	Estado HTTP	LDR	Consulte acciones recomendadas para HSTU.
HSTU	Estado HTTP	LDR	HSTE y HSTU están relacionados con el protocolo HTTP para todo el tráfico de LDR, incluidos S3, Swift y otro tráfico interno de StorageGRID. Una alarma indica que se ha producido una de las siguientes situaciones: • El protocolo 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 el protocolo HTTP está sin conexión, colocarlo en línea. Compruebe que el atributo HTTP de inicio automático está habilitado. Si el protocolo HTTP permanece 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, no se pueden informar los eventos de auditoría. 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 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 del estado NMS es sin conexión, 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 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 se encuentra en un estado donde 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 error de autenticación o fallo de autenticación, volver a conectarse, 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 la 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 para una tarea de cuadrícula que se está anulando es error, intente cancelar 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 Configuración de 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 el software de SANtricity indica que hay un problema de "'necesita atención'" con un componente de un dispositivo StorageGRID. Seleccione **NODES**. A continuación, seleccione **Appliance Storage Node** > **hardware**. Desplácese hacia abajo para ver el estado de cada componente. En el software SANtricity, 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 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 del estado SSM es sin conexión, 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 Offline puede indicar que no se puede montar el volumen ni acceder a él 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.

Alarmas que generan notificaciones SNMP (sistema heredado)

En la siguiente tabla se enumeran las alarmas heredadas que generan notificaciones SNMP. A diferencia de las alertas, no todas las alarmas generan notificaciones SNMP. Sólo las alarmas mostradas generan notificaciones SNMP y sólo con la gravedad o superior indicadas.

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

Codificación	Nombre	Gravedad
ACMS	Servicios de metadatos disponibles	Crítico
AITE	Recuperar estado	Menor
UIT	Recuperar estado	Importante
AQS	Mensajes de auditoría en cola	Aviso
AOTE	Estado de la tienda	Menor
UOT	Estado de la tienda	Importante
ROQ	Objetos en cola	Menor
ARRF	Fallos de solicitudes	Importante
ARRV	Errores de verificación	Importante
ARVF	Errores de almacenamiento	Importante
ASXP	Acciones de auditoría	Menor
AUMA	Estado de AMS	Menor
AUXS	Estado de exportación de auditoría	Menor

Codificación	Nombre	Gravedad
BTOF	Desviación	Aviso
CAHP	Porcentaje de uso de Java Heap	Importante
CAQH	Número de destinos disponibles	Aviso
CASA	Estado del almacén de datos	Importante
CDLP	Espacio usado de metadatos (porcentaje)	Importante
CLBE	Estado CLB	Crítico
DNST	Estado de DNS	Crítico
ECST	Estado de verificación	Importante
HSTE	Estado HTTP	Importante
HTA	HTTP de inicio automático	Aviso
PERDIDO	Objetos perdidos	Importante
MINQ	Notificaciones de correo electrónico en cola	Aviso
MIN	Estado de las notificaciones por correo electrónico	Menor
NANG	Configuración de negociación automática de red	Aviso
NDUP	Configuración dúplex de red	Menor
NLNK	Detección de enlace de red	Menor
NRER	Recibir errores	Aviso
NSPD	Velocidad	Aviso
NTER	Errores de transmisión	Aviso
NTFQ	Compensación de frecuencia NTP	Menor
NTLK	Bloqueo NTP	Menor
NOTF	Ajuste de tiempo NTP	Menor

Codificación	Nombre	Gravedad
NTSJ	Variación de origen de tiempo seleccionada	Menor
NTSU	Estado de NTP	Importante
OPST	Estado general de la alimentación	Importante
ORSU	Estado de replicación saliente	Aviso
PSA	Estado del suministro de alimentación de	Importante
PSBS	Estado de la fuente de alimentación B	Importante
RDTE	Estado de Tivoli Storage Manager	Aviso
RDTU	Estado de Tivoli Storage Manager	Importante
VICEPRESIDENTE	Espacio útil total (porcentaje)	Aviso
SHLH	Salud	Aviso
SLSA	Promedio de carga de CPU	Aviso
SMTT	Total de eventos	Aviso
SNST	Estado	
SEDA	Estado del sistema operativo de almacenamiento	Aviso
SST	Estado del almacenamiento	Aviso
VST DE NETAPP	Estado	Aviso
TMEM	Memoria instalada	Menor
UMEM	Memoria disponible	Menor
VMST	Estado	Menor
VPRI	Prioridad de verificación	Aviso
VSTU	Estado de verificación de objetos	Aviso

Referencia de archivos de registro

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

Los registros se clasifican de la siguiente manera:

- Registros del software StorageGRID
- Registros de implementación y mantenimiento
- 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.

Para acceder a los registros, puede recopilar archivos de registro y datos del sistema de uno o más nodos como un único archivo de registro (**SUPPORT** > **Tools** > **Logs**). 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.

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 del grupo EC por ID de perfil.

Ubicación del archivo	Descripción
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 del equilibrador de carga. También incluye los registros de tráfico de Grid Manager y del gestor de inquilinos.
nginx-gw	Archivos y registros de configuración del equilibrador de carga.
ntp	Registros y archivo de configuración NTP.
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.
snmp	Configuración del agente SNMP y listas de permiso/denegación de alarma utilizadas para enviar notificaciones SNMP.

Ubicación del archivo	Descripción
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.

Información relacionada

Recopilar archivos de registro y datos del sistema

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
`/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. El archivo `` `/var/local/core/kexec_cmd `` normalmente existe en los nodos del dispositivo y no indica un error.	Todos los nodos

Registros de Server Manager

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

Registros para servicios 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

Nombre de archivo	Notas	Encontrado en
`/var/local/log/clb.errlog`	Información de error para el servicio CLB. **Nota:** el servicio CLB está en desuso.	Nodos de puerta de enlace
`/var/local/log/cmn.errlog`		Nodos de administración
`/var/local/log/cms.errlog`	Este archivo de registro puede estar presente en los sistemas que se han actualizado desde una versión anterior de StorageGRID. Contiene información heredada.	Nodos de almacenamiento
`/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

Nombre de archivo	Notas	Encontrado en
`/var/local/log/jaeger.log`	El registro asociado al servicio jaeger, que se utiliza para la recopilación de trazas.	Todos los nodos
`/var/local/log/kstn.errlog`		Nodos de almacenamiento que ejecutan el servicio ADC
`/var/local/log/lambda*`	Contiene registros del servicio S3 Select.	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 de los puertos de administrador restringidos en los nodos de administrador y para el servicio Load Balancer, que proporciona un balanceo de carga del tráfico de S3 y Swift de clientes a nodos de almacenamiento.	Nodos de administrador y nodos de puerta de enlace

Nombre de archivo	Notas	Encontrado en
`/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
`/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

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

Información relacionada

Acerca de bycast.log

Use 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/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. El archivo `mysql.err` captura los errores y eventos de la base de datos, como startups y apagados. El archivo `mysql-slow.log` (El registro de consulta lento) captura las sentencias SQL que tardaron más de 10 segundos en ejecutarse.	Nodos de administración

Categoría	Nombre de archivo	Notas	Encontrado en
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
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. La `/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
Samba	/var/local/log/samba/	El directorio de registro Samba incluye un archivo de registro para cada proceso Samba (smb, nmb y winbind) y cada nombre de host/IP de cliente.	Nodo de administrador configurado para exportar el recurso compartido de auditoría a través de CIFS

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

Segmento de mensaje	Valor en ejemplo
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

Código de error	Significado
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
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

Número de error	Código de error	Significado
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
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

Número de error	Código de error	Significado
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
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

Número de error	Código de error	Significado
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
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

Número de error	Código de error	Significado
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
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

Número de error	Código de error	Significado
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 provocó la interrupción de la conexión
104	ECONNRESET	La conexión se restablece por el interlocutor
105	ENOBUFS	No hay espacio de búfer disponible
106	EISCONN	El extremo de transporte ya está conectado
107	ENOTCONN	El extremo de transporte no está conectado
108	ESHUTDOWN	No se puede enviar después de cerrar el 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

Número de error	Código de error	Significado
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
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

Amplíe su grid

Amplíe su grid: Descripción general

Siga estas instrucciones para ampliar la capacidad o las funcionalidades de su sistema StorageGRID sin interrumpir las operaciones del sistema.

Acerca de estas instrucciones

Estas instrucciones describen cómo realizar una ampliación StorageGRID para añadir volúmenes de almacenamiento a los nodos de almacenamiento, nuevos nodos grid a un sitio existente o un sitio nuevo

completo.

Estas instrucciones son para el personal técnico responsable de la configuración y el soporte del sistema StorageGRID después de su instalación.

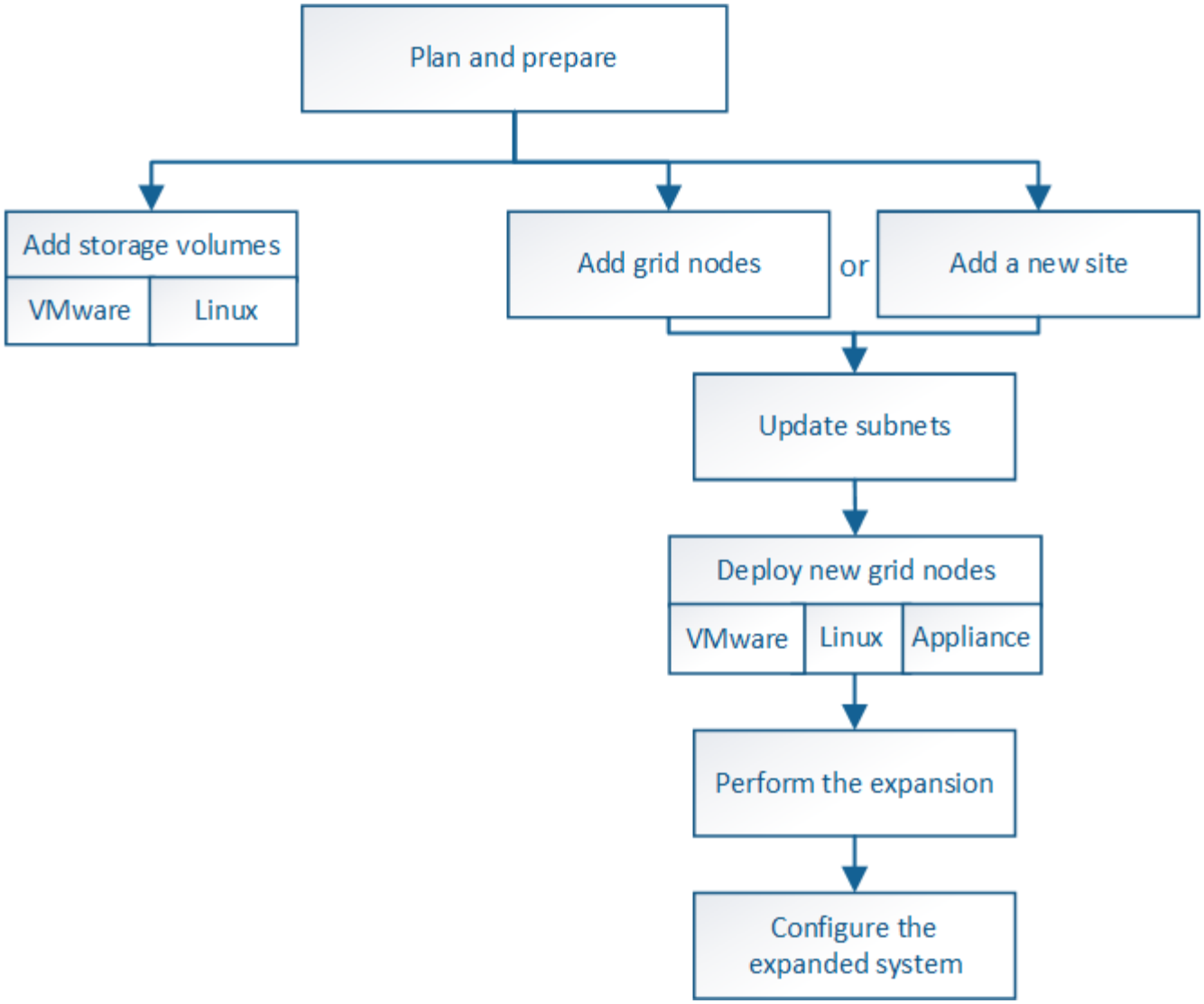
Descripción general del procedimiento de expansión

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.

Tal y como se muestra en el diagrama de flujo de trabajo, los pasos para realizar una ampliación dependen de si se añaden volúmenes de almacenamiento a un nodo de almacenamiento, se añaden nodos nuevos a un sitio existente o se añade un sitio nuevo. En todos los casos, puede realizar la expansión sin interrumpir el funcionamiento del sistema actual.

Los pasos para añadir nodos también dependen de si va a añadir dispositivos StorageGRID o hosts que ejecuten VMware o Linux.

> '''Linux''' se refiere a una implementación de Red Hat® Enterprise Linux®, Ubuntu®, CentOS o Debian®. Utilice la "Herramienta de matriz de interoperabilidad de NetApp (IMT)" para obtener una lista de las versiones compatibles.



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 actuales de ILM para determinar dónde y cuándo añadir volúmenes de almacenamiento con el fin de aumentar el almacenamiento disponible para los objetos replicados o codificados de borrado. Consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de

la información.

- No es posible aumentar la capacidad de metadatos del sistema con la adición de volúmenes de almacenamiento, ya que los metadatos del objeto 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 o SG6060X. Cada bandeja de expansión añade 16 volúmenes de almacenamiento. Con las dos bandejas de ampliación instaladas, SG6060 y SG6060X pueden 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 a la vez que se realiza una actualización del sistema, una operación de recuperación u otra ampliación.

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 o SG6060X, vaya a. Añada la bandeja de expansión al SG6060 o SG6060X implementado.
- Para un nodo basado en software, siga las instrucciones deAñadir 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 actuales de ILM para determinar dónde y cuándo añadir nodos de almacenamiento con el fin de aumentar el almacenamiento disponible para los objetos replicados o codificados de borrado. Consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.
- 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. Como no puede retirar un nodo de almacenamiento si se conservan muy pocos servicios ADC, esto garantiza que haya un nuevo servicio ADC disponible antes de que se elimine el servicio antiguo.
- No puede agregar el servicio ADC a un nodo después de haberlo implementado.

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 una cuadrícula de dos sitios y una regla de gestión del ciclo de vida de la información que crea una copia de objeto en cada sitio, debe añadir almacenamiento a cada sitio para aumentar la capacidad general de los objetos del grid. Consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

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 supervisar y representar la capacidad de almacenamiento tal y como se describe en las instrucciones de Supervisión y solución de problemas de StorageGRID.

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 Gestión de objetos con ILM.

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 conducen a esta recomendación o para desarrollar un plan más preciso para su sitio, revise la siguiente sección. Para obtener una recomendación personalizada optimizada para su situación, póngase en contacto con su representante de cuentas de NetApp.

Calcule el número de nodos de ampliación de almacenamiento que se van a añadir para los objetos de código de borrado

Para optimizar la forma de ampliar una puesta en marcha que almacena objetos de código de borrado, debe tener en cuenta muchos factores:

- Esquema de codificación de borrado en uso
- Características del pool de almacenamiento utilizado para la codificación de borrado, incluido el número de nodos en cada sitio y la cantidad de espacio libre en cada nodo
- Si el grid se expandió anteriormente (porque la cantidad de espacio libre por nodo de almacenamiento podría no ser aproximadamente igual en todos los nodos)
- La naturaleza exacta de la política de ILM, como si las reglas de ILM hacen tanto objetos replicados como códigos de borrado

Los siguientes ejemplos pueden ayudarle a comprender el impacto del esquema de codificación de borrado, el número de nodos del pool de almacenamiento y la cantidad de espacio libre en cada nodo.

Consideraciones similares afectan a los cálculos de la normativa ILM que almacena datos replicados y con código de borrado, así como los cálculos de una cuadrícula que se ha ampliado anteriormente.

> Los ejemplos de esta sección representan las mejores prácticas para añadir capacidad de almacenamiento a un sistema StorageGRID. Si no puede añadir el número recomendado de nodos, puede que tenga que ejecutar el procedimiento de reequilibrio de EC para permitir que se almacenen más objetos de código de borrado. Consulte Reequilibre los datos con código de borrado.

Ejemplo 1: Expanda la cuadrícula de un sitio que utiliza codificación de borrado 2+1

Este ejemplo muestra cómo expandir un grid simple que solo incluye tres nodos de almacenamiento.

> Este ejemplo solo utiliza tres nodos de almacenamiento para mayor simplicidad. Sin embargo, no se recomienda utilizar sólo tres nodos de almacenamiento: Una cuadrícula de producción real debe utilizar un mínimo de *k+m* + 1 nodos de almacenamiento para redundancia, lo que equivale a cuatro nodos de almacenamiento (2+1+1) para este ejemplo.

Se debe asumir lo siguiente:

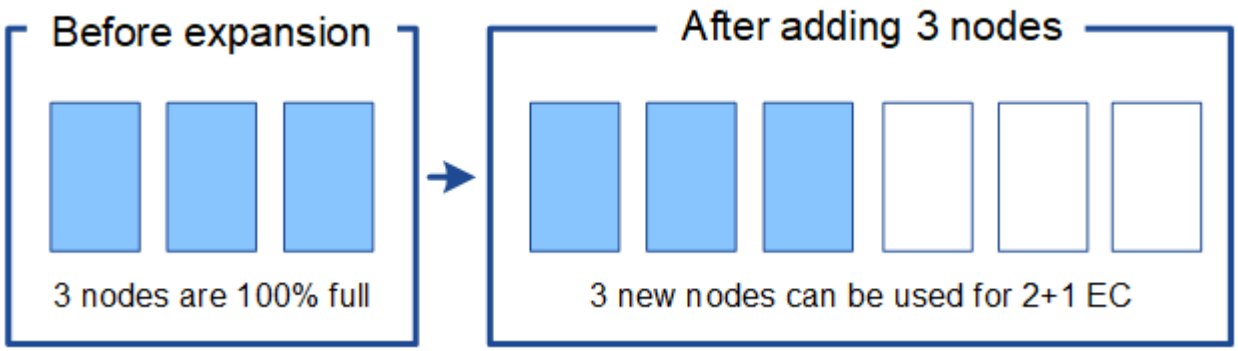
- Todos los datos se almacenan mediante el esquema de codificación de borrado 2+1. Con el esquema de codificación de borrado 2+1, cada objeto se almacena en tres fragmentos y cada fragmento se guarda en un nodo de almacenamiento distinto.
- Tiene un sitio con tres nodos de almacenamiento. Cada nodo de almacenamiento tiene una capacidad total de 100 TB.
- Desea ampliar añadiendo nuevos nodos de almacenamiento de 100 TB.
- Finalmente, se desea equilibrar los datos codificados con borrado en los nodos antiguos y nuevos.

Dispone de una serie de opciones, según el nivel de llenado que están los nodos de almacenamiento cuando se realiza la ampliación.

- **Agregue tres nodos de almacenamiento de 100 TB cuando los nodos existentes estén llenos un 100%**

  En este ejemplo, los nodos existentes están llenos al 100 %. Como no hay capacidad libre, se deben añadir inmediatamente tres nodos para continuar con la codificación de borrado de 2+1.

  Una vez finalizada la ampliación, cuando los objetos estén codificados con borrado, todos los fragmentos se colocarán en los nodos nuevos.

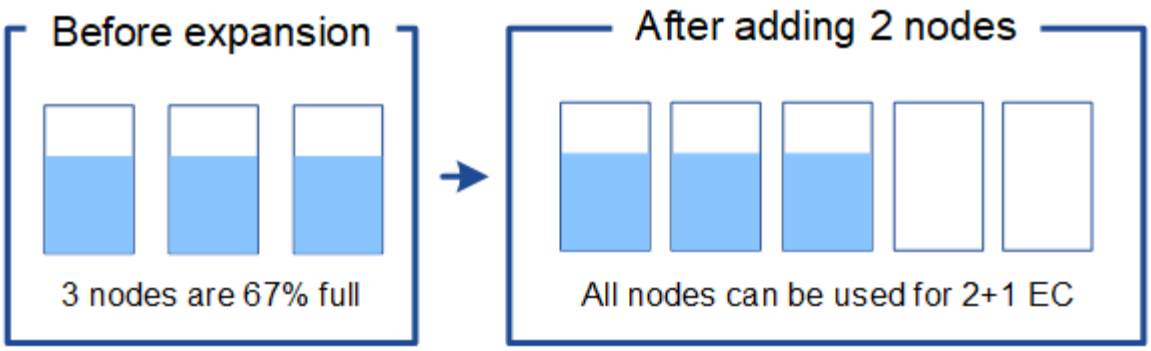


> Esta expansión agrega *k+m* nodes. Se recomienda añadir cuatro nodos para redundancia. Si agrega sólo los nodos de expansión *k+m* cuando los nodos existentes están llenos al 100%, todos los objetos nuevos se almacenan en los nodos de expansión. Si alguno de los nuevos nodos deja de estar disponible, incluso de forma temporal, StorageGRID no puede cumplir con los requisitos de ILM.

- **Agregue dos nodos de almacenamiento de 100 TB, cuando los nodos de almacenamiento existentes estén llenos un 67%**

  En este ejemplo, los nodos existentes están llenos al 67 %. Como hay 100 TB de capacidad libre en los nodos existentes (33 TB por nodo), solo tiene que añadir dos nodos si realiza la ampliación ahora.

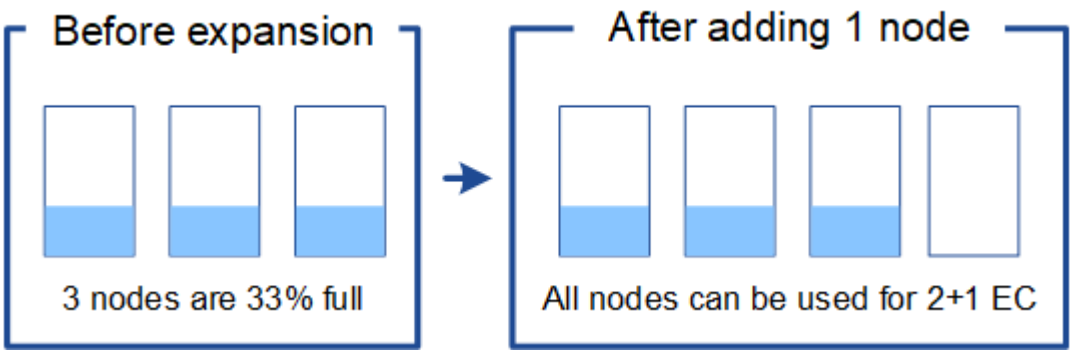
  Si añade 200 TB de capacidad adicional, podrá continuar con un código de borrado al 2+1 y equilibrar datos codificados de borrado en algún momento entre todos los nodos.



- **Agregue un nodo de almacenamiento de 100 TB cuando los nodos de almacenamiento existentes estén llenos un 33%**

  En este ejemplo, los nodos existentes están llenos al 33 %. Como hay 200 TB de capacidad libre en los nodos existentes (67 TB por nodo), solo tiene que añadir un nodo si realiza la ampliación ahora.

  Si añade 100 TB de capacidad adicional, podrá continuar con un código de borrado al 2+1 y equilibrar datos codificados de borrado en algún momento entre todos los nodos.



Ejemplo 2: Expanda la cuadrícula de tres sitios que utiliza codificación de borrado 6+3

Este ejemplo muestra cómo desarrollar un plan de expansión para una cuadrícula multisitio que tiene un esquema de codificación a borrado con un número mayor de fragmentos. A pesar de las diferencias entre estos ejemplos, el plan de expansión recomendado es muy similar.

Se debe asumir lo siguiente:

- Todos los datos se almacenan mediante el esquema de codificación de borrado 6+3. Con el esquema de codificación de borrado 6+3, cada objeto se almacena como 9 fragmentos y cada fragmento se guarda en un nodo de almacenamiento distinto.
- Tiene tres sitios y cada sitio tiene cuatro nodos de almacenamiento (12 nodos en total). Cada nodo tiene una capacidad total de 100 TB.
- Desea ampliar añadiendo nuevos nodos de almacenamiento de 100 TB.
- Finalmente, se desea equilibrar los datos codificados con borrado en los nodos antiguos y nuevos.

Dispone de una serie de opciones, según el nivel de llenado que están los nodos de almacenamiento cuando se realiza la ampliación.

- **Agregue nueve nodos de almacenamiento de 100 TB (tres por sitio), cuando los nodos existentes estén llenos del 100%**

En este ejemplo, los 12 nodos existentes están llenos al 100 %. Como no hay capacidad libre, debe añadir inmediatamente nueve nodos (900 TB de capacidad adicional) para continuar con la codificación de borrado 6+3.

Una vez finalizada la ampliación, cuando los objetos estén codificados con borrado, todos los fragmentos se colocarán en los nodos nuevos.

> Esta expansión agrega *k+m* nodes. Se recomienda añadir 12 nodos (cuatro por sitio) para redundancia. Si agrega sólo los nodos de expansión *k+m* cuando los nodos existentes están llenos al 100%, todos los objetos nuevos se almacenan en los nodos de expansión. Si alguno de los nuevos nodos deja de estar disponible, incluso de forma temporal, StorageGRID no puede cumplir con los requisitos de ILM.

- **Agregue seis nodos de almacenamiento de 100 TB (dos por sitio), cuando los nodos existentes estén llenos del 75%**

  En este ejemplo, los 12 nodos existentes están llenos al 75 %. Como hay 300 TB de capacidad libre (25 TB por nodo), solo tiene que añadir seis nodos si realiza la ampliación en este momento. Se agregarían dos nodos a cada uno de los tres sitios.

  Añadir 600 TB de capacidad de almacenamiento le permitirá continuar con un código de borrado de 6+3 y equilibrar los datos codificados de borrado en algún momento entre todos los nodos.

- **Agregue tres nodos de almacenamiento de 100 TB (uno por sitio), cuando los nodos existentes estén llenos del 50%**

  En este ejemplo, los 12 nodos existentes están llenos al 50 %. Como hay 600 TB de capacidad libre (50 TB por nodo), solo tiene que añadir tres nodos si realiza la ampliación en este momento. Agregaría un nodo a cada uno de los tres sitios.

  Añadir 300 TB de capacidad de almacenamiento le permitirá continuar con un código de borrado de 6+3 y equilibrar los datos codificados de borrado en algún momento entre todos los nodos.

Consideraciones que tener en cuenta al reequilibrar los datos codificados a borrado

Si va a realizar una ampliación para añadir nodos de almacenamiento y la política de gestión de la información incluye una o varias reglas de gestión de la información para borrar los datos de código, puede que tenga que realizar el procedimiento de reequilibrio de EC una vez completada la ampliación.

Por ejemplo, si no puede añadir el número recomendado de nodos de almacenamiento para el esquema de codificación de borrado que está usando, puede que deba ejecutar el procedimiento de reequilibrio de EC para permitir que se almacenen los objetos de código de borrado adicionales.

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 se ejecuta el procedimiento de reequilibrio de EC, StorageGRID redistribuye los fragmentos codificados con borrado entre los nodos de almacenamiento

existentes y los que se han ampliado recientemente 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 se tiene en cuenta el uso de datos replicados en cada nodo de almacenamiento al determinar dónde se deben mover los datos codificados de borrado

Una vez finalizado el procedimiento de reequilibrio de EC:

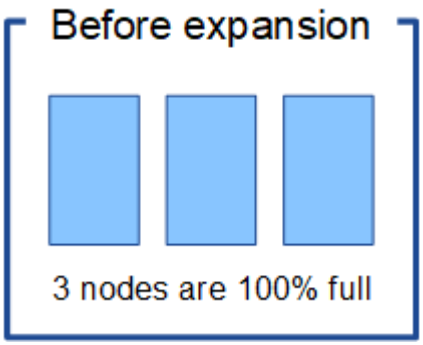
- Los datos con código de borrado se mueven de los nodos de almacenamiento con menos espacio disponible a los nodos de almacenamiento con más espacio disponible.
- Los valores usados (%) pueden seguir siendo diferentes entre nodos de almacenamiento, ya que el procedimiento de reequilibrio de EC no mueve copias de objetos replicadas.
- La protección de datos de los objetos codificados de borrado no cambiará.

Cuando se ejecuta el procedimiento de reequilibrio de EC, el rendimiento de las operaciones de ILM y las operaciones del cliente S3 y Swift probablemente se verán afectadas. Por este motivo, solo debe realizar este procedimiento en casos limitados.

Cuándo no realizar el reequilibrio de EC

Como ejemplo de cuándo no necesita realizar un reequilibrio de EC, tenga en cuenta lo siguiente:

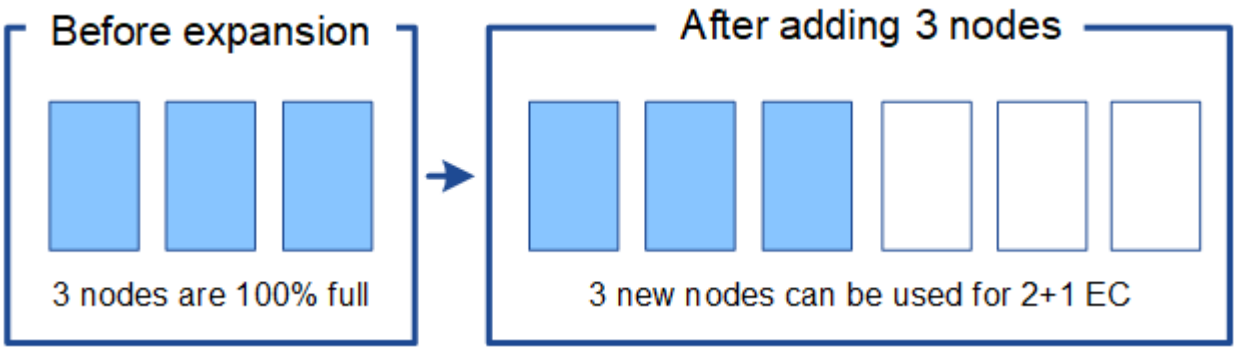
- StorageGRID se ejecuta en un solo sitio, que contiene tres nodos de almacenamiento.
- La política de ILM usa una regla de codificación de borrado de 2+1 para todos los objetos de mayor tamaño que 1.0 MB y una regla de replicación de 2 copias para los objetos más pequeños.
- Todos los nodos de almacenamiento se han llenado completamente y la alerta **almacenamiento de objetos bajo** se ha activado en el nivel de gravedad principal. La acción recomendada es realizar un procedimiento de ampliación para añadir nodos de almacenamiento.



Para expandir el sitio en este ejemplo, se recomienda añadir tres o más nodos de almacenamiento nuevos. StorageGRID requiere tres nodos de almacenamiento para la codificación de borrado al 2+1 con el fin de poder colocar los dos fragmentos de datos y el fragmento de paridad en diferentes nodos.

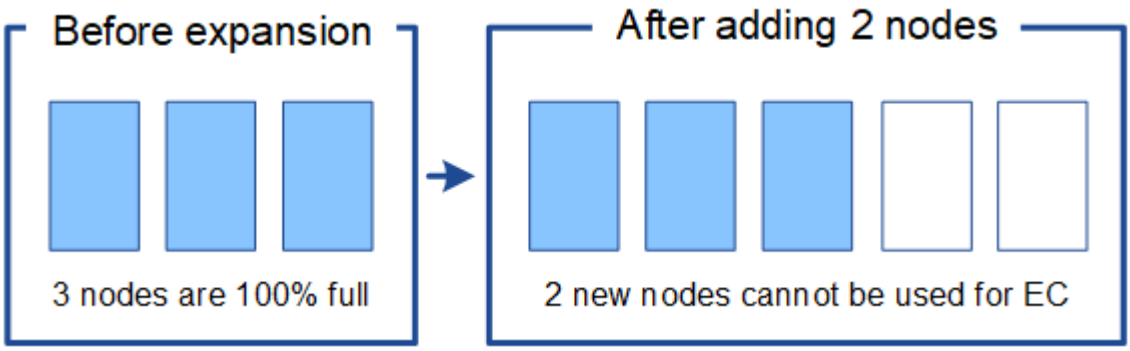
Después de añadir los tres nodos de almacenamiento, los nodos de almacenamiento originales permanecen llenos, pero se pueden seguir ingiriendo los objetos en el esquema de código de borrado 2+1 de los nuevos

nodos. No se recomienda ejecutar el procedimiento de reequilibrio de EC en este caso: Al ejecutar el procedimiento se reducirá temporalmente el rendimiento, lo que podría afectar a las operaciones del cliente.

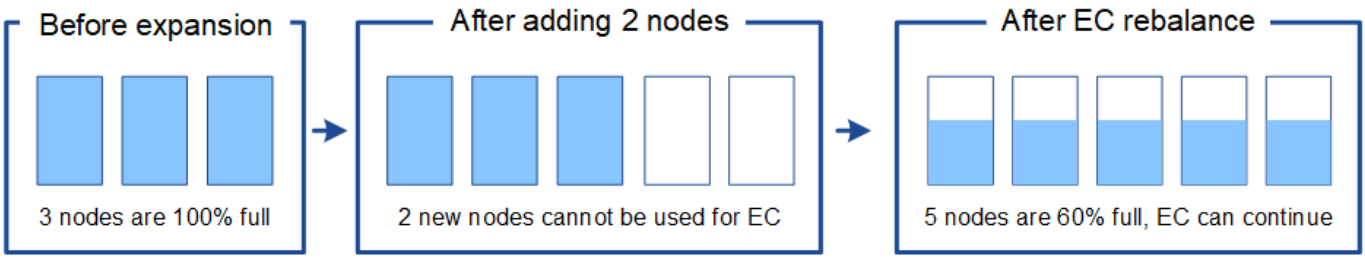


Cuándo realizar el reequilibrio de EC

Como ejemplo de cuándo debe realizar el procedimiento de reequilibrio de EC, tenga en cuenta el mismo ejemplo, pero suponga que solo puede agregar dos nodos de almacenamiento. Dado que la codificación de borrado 2+1 requiere al menos tres nodos de almacenamiento, los nuevos nodos no pueden utilizarse para los datos codificados de borrado.



Para resolver este problema y utilizar los nuevos nodos de almacenamiento, puede ejecutar el procedimiento de reequilibrio de EC. Cuando se ejecuta este procedimiento, StorageGRID redistribuye los datos codificados con borrado y los fragmentos de paridad entre todos los nodos de almacenamiento del sitio. En este ejemplo, cuando se completa el procedimiento de reequilibrio de EC, los cinco nodos ahora están llenos de solo un 60 % y los objetos se pueden seguir ingiriendo en el esquema de codificación de borrado 2+1 de todos los nodos de almacenamiento.



Requisitos para el reequilibrio de la CE

En general, sólo debe ejecutar el procedimiento de reequilibrio de EC en casos limitados. En concreto, sólo debe realizar el reequilibrio de EC si se cumplen todas las siguientes afirmaciones:

- 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 el número recomendado de nuevos nodos de almacenamiento para el esquema de código de borrado que se está utilizando. 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.

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 nuevos nodos de almacenamiento en una ampliación, debe esperar a ejecutar el procedimiento de reequilibrio de EC hasta que se hayan añadido todos los nodos nuevos. Si hay un procedimiento de reequilibrio de EC en curso al añadir nuevos nodos de almacenamiento, no se moverán los datos a esos nodos.
Procedimiento de actualización	No Si necesita actualizar el software StorageGRID, debe realizar 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	Permitido durante el procedimiento de reequilibrio de EC?
Procedimiento de clonación del nodo de dispositivos	No Si necesita clonar un nodo de almacenamiento de dispositivos, debe esperar a ejecutar el procedimiento de reequilibrio de EC hasta que se haya añadido el nuevo nodo. Si hay un procedimiento de reequilibrio de EC en curso al añadir nuevos nodos de almacenamiento, no se moverán los datos a esos nodos.
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 el ILM, debe anular 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:

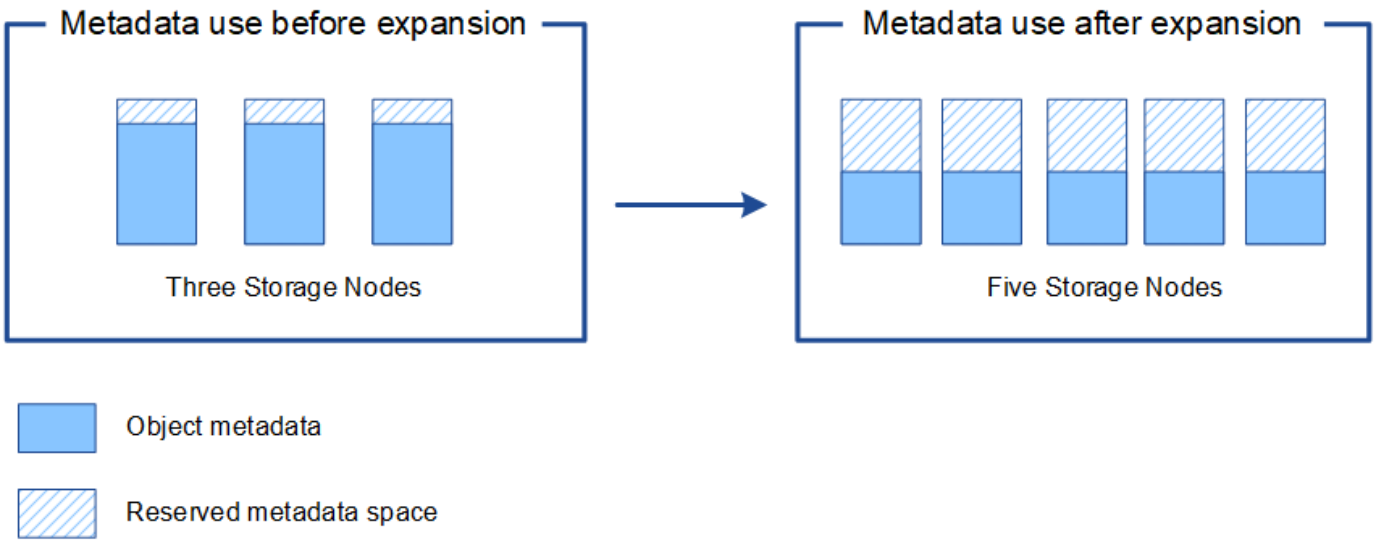
- Suponiendo que haya suficiente capacidad de almacenamiento de objetos disponible, tener más espacio disponible para los metadatos de objetos aumenta el número de objetos que se pueden almacenar en su sistema StorageGRID.
- Es posible aumentar la capacidad de metadatos de un grid si se añaden uno o 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. Consulte las instrucciones para Administración de StorageGRID.
- No puede aumentar la capacidad de metadatos si se añaden volúmenes de almacenamiento a los nodos de almacenamiento existentes, ya que los metadatos se almacenan solo en el volumen 0.
- No es posible aumentar la capacidad de metadatos si se añade 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.

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 adicionales para admitir la creación de grupos de alta disponibilidad de nodos de puerta de enlace, 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
- Nodos de archivado

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 es posible añadir un nodo de administrador principal durante una ampliación.
- 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 va a agregar nodos de archivado, tenga en cuenta que cada nodo de archivado sólo admite cinta mediante el middleware Tivoli Storage Manager (TSM).
- Si la opción **Red cliente de nodo nuevo** predeterminada* se establece en **no confiable** en la página redes de cliente no confiables, las aplicaciones cliente que se conecten a nodos de expansión mediante la red cliente deben conectarse utilizando un puerto de extremo de equilibrador de carga (**CONFIGURACIÓN** > **Red** > **redes de cliente no confiables**). Consulte las instrucciones para Administración de StorageGRID para cambiar la configuración del nuevo nodo y configurar los extremos del equilibrador 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 se pueden añadir nodos de cuadrícula 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 sitio nuevo 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 acerca del cambio de ILM al añadir un sitio nuevo, consulte el ejemplo de cambio de una política de ILM en las instrucciones de Gestión de objetos con 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 va a añadir volúmenes de almacenamiento nuevos a nodos de almacenamiento existentes o a instalar un dispositivo StorageGRID nuevo.
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
	  ◦ Instale Red Hat Enterprise Linux o CentOS
	  ◦ Instalar Ubuntu o Debian
	  ◦ Instale VMware

La documentación actual de su plataforma	Para conocer las versiones compatibles, consulte "Matriz de interoperabilidad".

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 la página de descargas de NetApp para StorageGRID.

   "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 para 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 o CentOS	`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 o CentOS, 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 RPM para instalar las imágenes de nodo StorageGRID en sus hosts RHEL o CentOS.
	PAQUETE RPM para instalar el servicio host StorageGRID en sus hosts RHEL o CentOS.
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.
	Un archivo de configuración en blanco para usar con el `configure-storagegrid.py` guión.
	Ejemplo de rol de Ansible y libro de estrategia para configurar hosts de RHEL o CentOS para puesta en marcha del contenedor StorageGRID. Puede personalizar el rol o el libro de estrategia según sea necesario.
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede utilizar estos esquemas para confirmar que cualquier código que haya escrito para utilizar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no dispone de un entorno StorageGRID que no sea de producción para la comprobación de compatibilidad de actualizaciones.

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.
	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.
	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.

Ruta y nombre de archivo	Descripción
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede utilizar estos esquemas para confirmar que cualquier código que haya escrito para utilizar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no dispone de un entorno StorageGRID que no sea de producción para la comprobación de compatibilidad de actualizaciones.

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.
	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.

Ruta y nombre de archivo	Descripción
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.
	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.
	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.
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede utilizar estos esquemas para confirmar que cualquier código que haya escrito para utilizar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no dispone de un entorno StorageGRID que no sea de producción para la comprobación de compatibilidad de actualizaciones.

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.

Ruta y nombre de archivo	Descripción
	Suma de comprobación del paquete DE instalación DE DEB utilizado por el instalador de dispositivos de StorageGRID para validar que el paquete está intacto tras la carga.

> 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).
- 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 cuadrícula entre nodos de cuadrícula o entre sitios 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. Sólo se admite el uso de NAT para tender un puente entre la red Grid a través de un segmento de red pública si se utiliza una aplicación de túnel que sea transparente para todos los nodos de la cuadrícula, lo que significa que los nodos de la cuadrícula no necesitan conocimientos de 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.

Lo que necesitará

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 o SG6060X implementado Para obtener información sobre cómo añadir volúmenes de almacenamiento al SG6060 o SG6060X mediante la instalación de bandejas de ampliación. No es posible expandir otros nodos de almacenamiento del dispositivo.

Acerca de esta tarea

El almacenamiento subyacente de un nodo de almacenamiento se divide en una serie de 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 a nivel mundial de cada disco coincide con el identificador a nivel mundial (WWID) de volumen que se muestra cuando se ven las propiedades de volumen estándar en el software 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.

Lo que necesitará

- Tendrá acceso a las instrucciones de instalación de StorageGRID para implementaciones de VMware.
  - Instale VMware
- Usted tiene la `Passwords.txt` archivo.
- Tiene permisos de acceso específicos.

> No intente añadir volúmenes de almacenamiento a un nodo de almacenamiento mientras hay una actualización de software, un procedimiento de recuperación u otro procedimiento de ampliación activo.

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 a menudo y son más fáciles de gestionar, mientras que los RDM pueden proporcionar un mejor rendimiento a las cargas de trabajo que utilizan tamaños de objeto más grandes (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** ni **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.

a. Introduzca **y** para aceptar el formato.

b. 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.

c. Cuando se le solicite, introduzca **y** para detener los servicios de almacenamiento.

Los servicios de almacenamiento se detienen, y el `setup_rangedbs.sh` el script se ejecuta automáticamente. Una vez que los volúmenes están listos para su uso como recedbs, los servicios se inician de nuevo.

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.

Lo que necesitará

- Tiene acceso a las instrucciones de instalación de StorageGRID para su plataforma Linux.
  - Instale Red Hat Enterprise Linux o CentOS
  - Instalar Ubuntu o Debian
- Usted tiene la `Passwords.txt` archivo.
- Tiene permisos de acceso específicos.

> No intente añadir volúmenes de almacenamiento a un nodo de almacenamiento mientras hay una actualización de software, un procedimiento de recuperación u otro procedimiento de ampliación activo.

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 de disco y actualice la configuración de la controladora RAID según sea necesario, o asigne nuevos LUN SAN en 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 tiene 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.

a. Introduzca **y** para formatear los volúmenes de almacenamiento.
b. 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.
c. Cuando se le solicite, introduzca **y** para detener los servicios de almacenamiento.

Los servicios de almacenamiento se detienen, y el `setup_rangedbs.sh` el script se ejecuta automáticamente. Una vez que los volúmenes están listos para su uso como recedbs, los servicios se inician de nuevo.

14. 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
```

15. 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**.

16. 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

Puede seguir este procedimiento para agregar nodos de cuadrícula a sitios existentes o para agregar un sitio nuevo, pero no puede realizar ambos tipos de expansión al mismo tiempo.

Lo que necesitará

- Tiene el permiso acceso raíz o 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.

Lo que necesitará

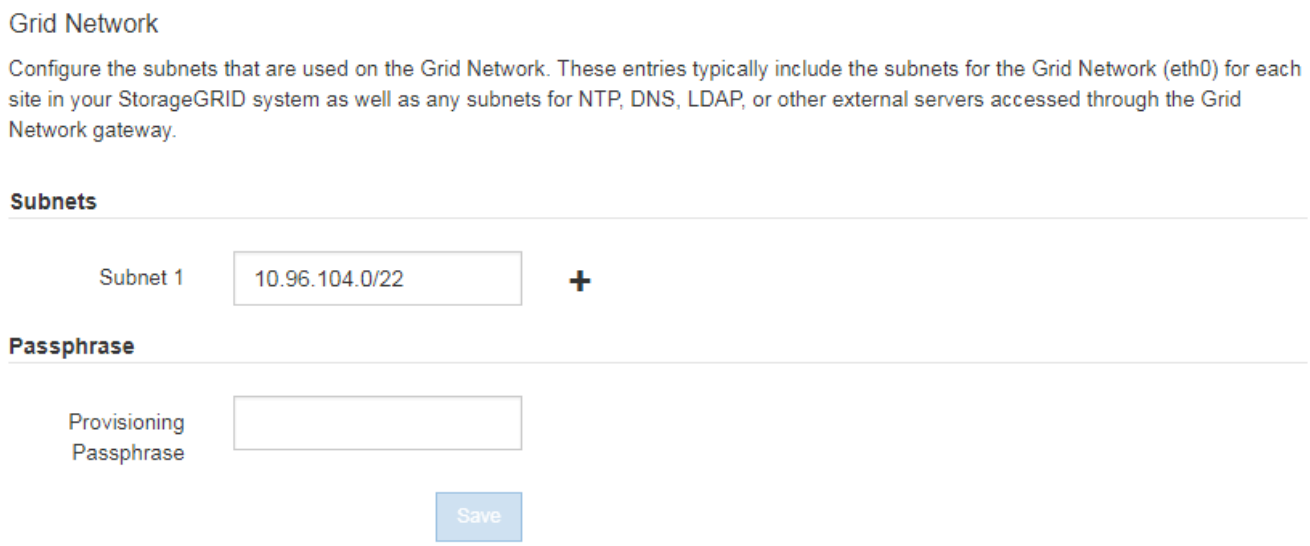
- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso de mantenimiento o acceso raíz.
- Tiene la clave de acceso de aprovisionamiento.
- Tiene las direcciones de red, en notación CIDR, de las subredes que desea configurar.

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. En la lista subredes, seleccione el signo más para añadir una nueva subred en notación CIDR.

   Por ejemplo, introduzca 10.96.104.0/22.

3. Introduzca la contraseña de aprovisionamiento y seleccione **Guardar**.

   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 la cuadrícula, los nodos que añade 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.

Lo que necesitará

- Tiene las instrucciones de instalación de StorageGRID para su versión de Linux y ha revisado los requisitos de hardware y almacenamiento.
  - Instale Red Hat Enterprise Linux o CentOS
  - Instalar 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 único 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 desde un sistema ONTAP de NetApp, confirme que el volumen no tiene habilitada la 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.

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.

Lo que necesitará

- El dispositivo se ha instalado en un rack o armario, conectado a las redes y encendido.
- Ha utilizado el instalador de dispositivos de StorageGRID para completar todos los pasos de las instrucciones de instalación y mantenimiento del dispositivo.
  - Servicios de aplicaciones SG100 y SG1000
  - Configurar el hardware (SG5600)
  - Configurar hardware (SG5700)
  - Configuración del hardware (SG6000)

  La configuración del hardware del dispositivo incluye los pasos necesarios para configurar las conexiones StorageGRID (enlaces de red y direcciones IP), así como los pasos opcionales para habilitar el cifrado de nodos, cambiar el modo RAID y volver a asignar 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. Por ejemplo, la versión 3.6 del instalador de dispositivos de StorageGRID es compatible con la versión 11.6 de StorageGRID. (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. Anule la selección de la casilla de verificación **Activar descubrimiento de nodo de administración**. 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.
Detección automática de todos los nodos principales de administración conectados	a. Active la casilla de verificación **Activar descubrimiento de nodos de administración**. 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.

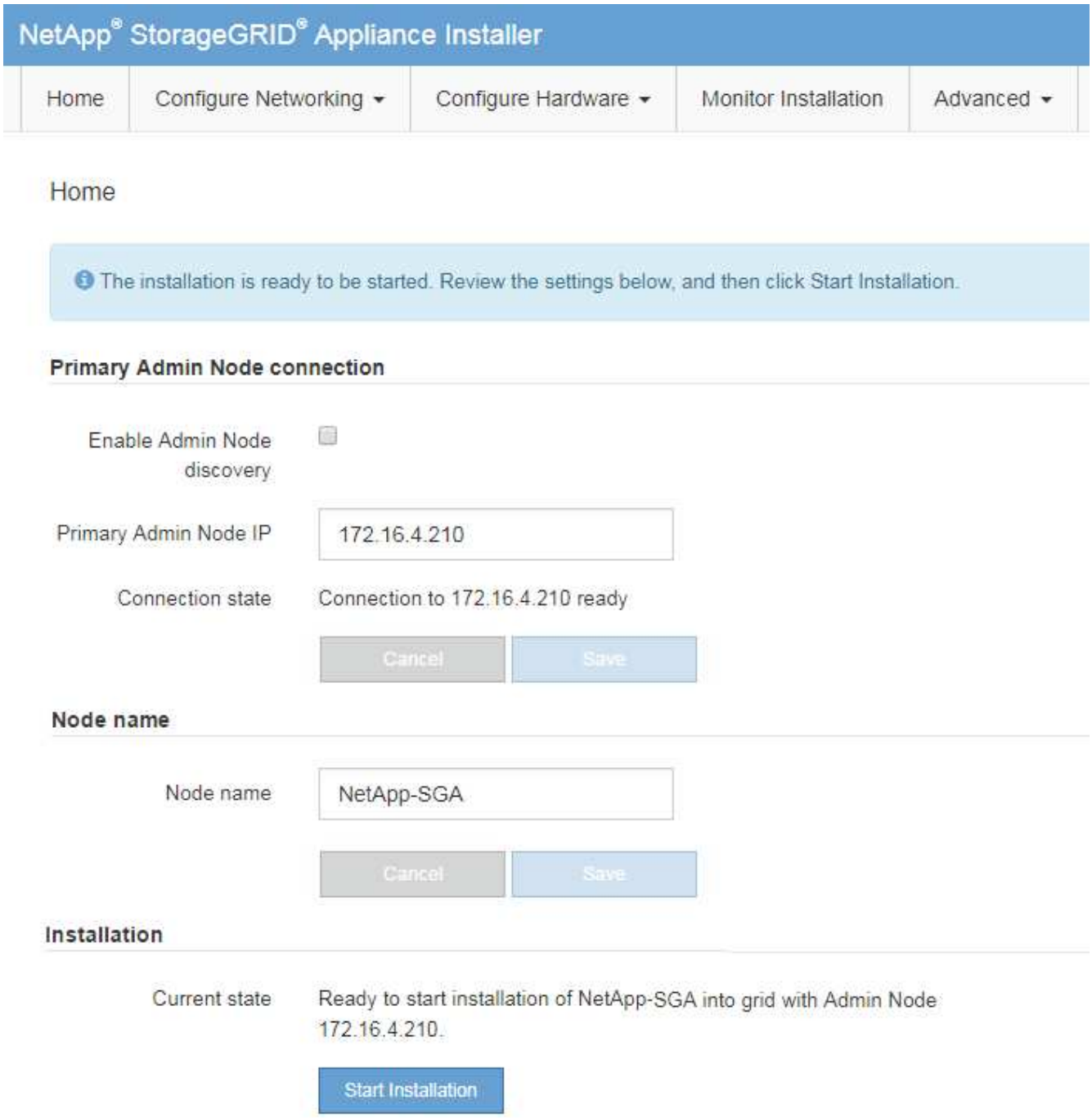
4. En el campo **Nombre de nodo**, introduzca el nombre que desea utilizar para este nodo de dispositivo y seleccione **Guardar**.

   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 **instalación**, confirme que el estado actual es "'Listo para iniciar la instalación de *nombre de nodo* en la cuadrícula con el nodo de administración principal *admin_ip*'" y que el botón **Iniciar instalación** 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 instalación y mantenimiento del aparato.

6. En la página de inicio del instalador de dispositivos StorageGRID, seleccione **Iniciar instalación**.



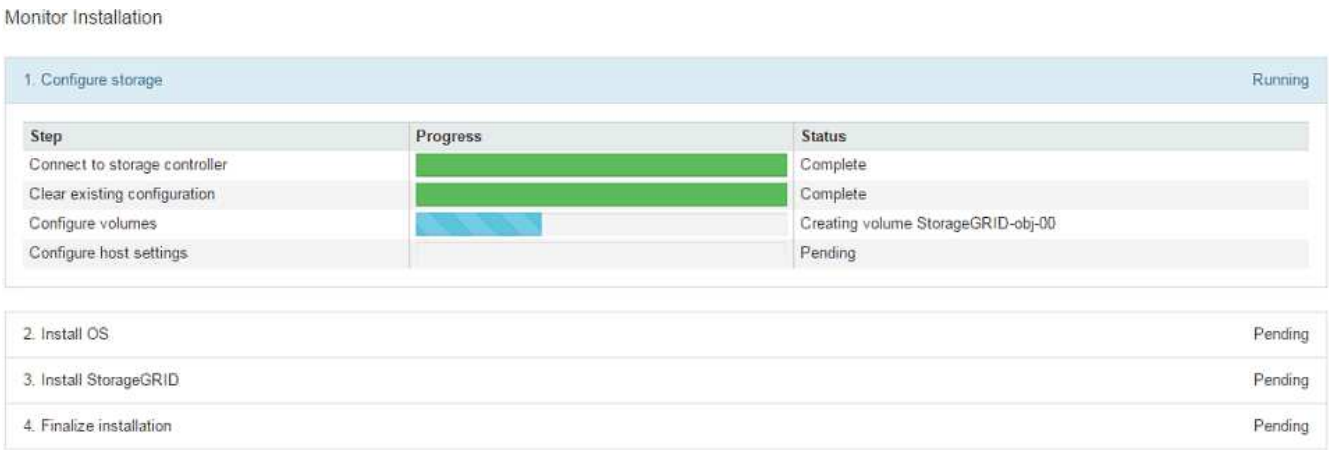
El estado actual cambia a "'instalación en curso'" y se muestra la página de instalación del monitor.

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.

> El instalador garantiza que no se vuelvan a ejecutar las tareas completadas en una instalación anterior. 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 de "Shided."

9. Revise el progreso de las dos primeras etapas de instalación.

   1. Configurar el dispositivo

   Durante esta fase, ocurre uno de los siguientes procesos:

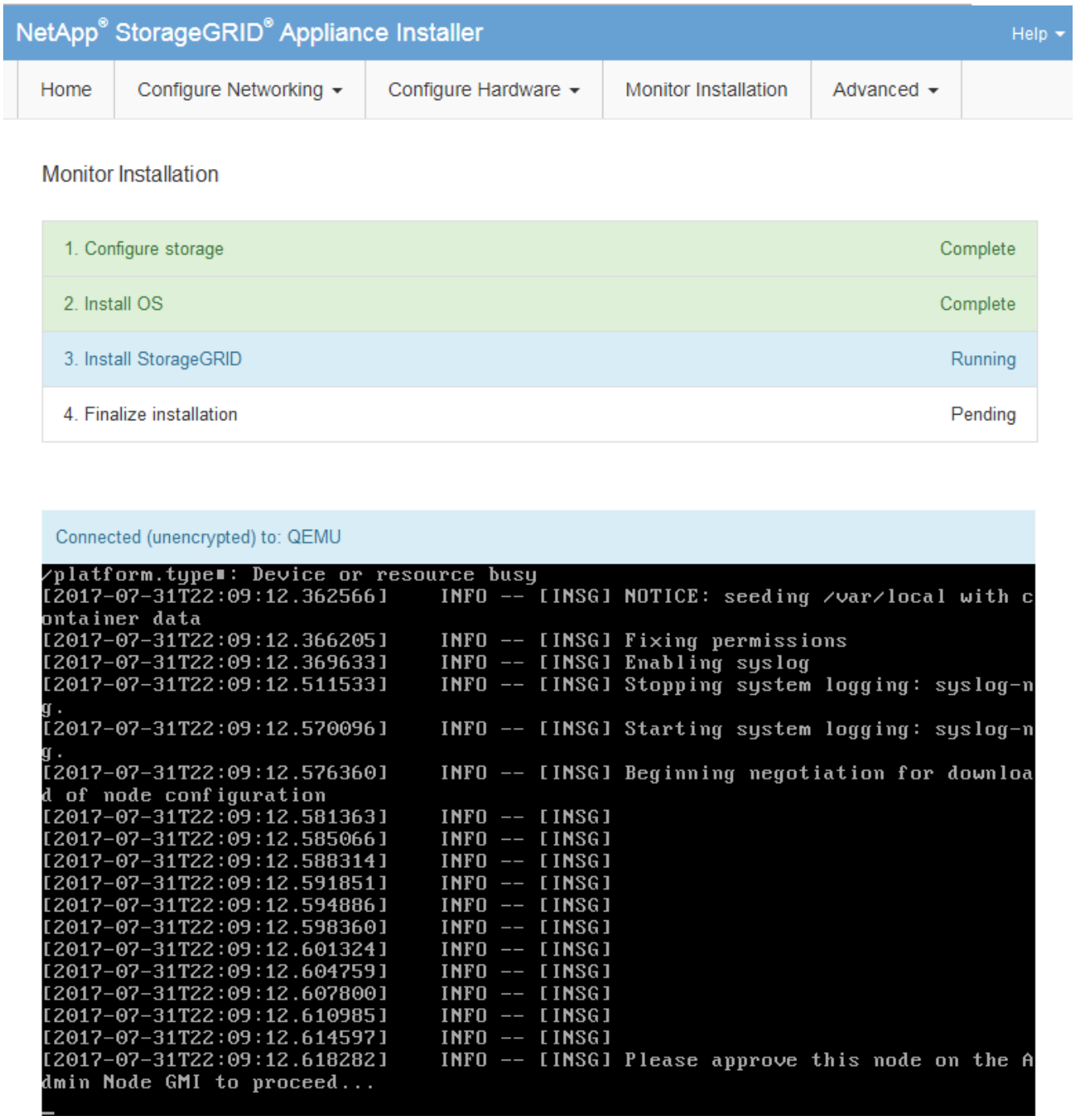
   - En el caso de un dispositivo de almacenamiento, el instalador se conecta al controlador de almacenamiento, borra la configuración existente, se comunica con el software SANtricity para configurar los volúmenes y configura los ajustes del host.
   - En un dispositivo de servicios, el instalador borra 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.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso de mantenimiento o acceso raíz.
- Tiene la clave de acceso de aprovisionamiento.
- Se han implementado todos los nodos de grid que se están añadiendo en esta ampliación.

- 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 agregar un sitio nuevo, debe revisar y actualizar las reglas de ILM antes de iniciar el procedimiento de expansión para asegurarse de que las copias de objetos no se almacenan en el sitio nuevo hasta que haya finalizado la expansión. Por ejemplo, si una regla utiliza el pool de almacenamiento predeterminado (todos los nodos de almacenamiento), debe crear un nuevo pool de almacenamiento que contenga solo los nodos de almacenamiento existentes y actualizar la regla 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. Consulte las instrucciones para Gestión de objetos con ILM.

Acerca de esta tarea

La realización de la ampliación incluye las siguientes fases:

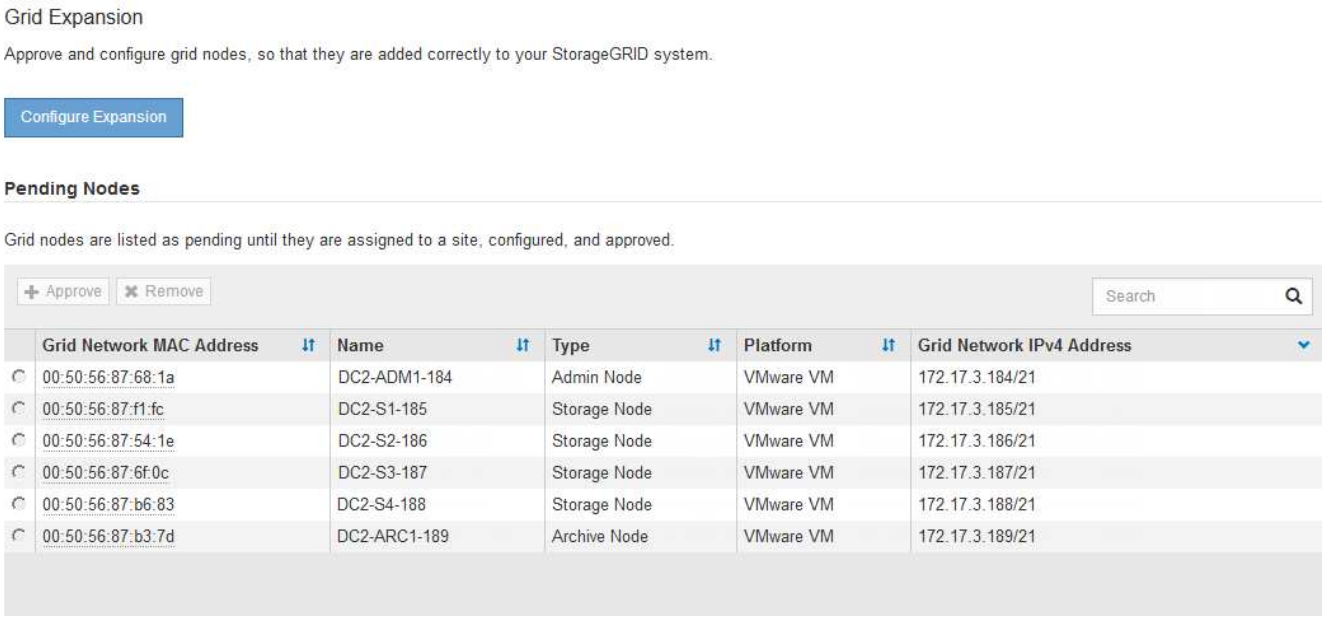
1. Para configurar la expansión, especifique si va a agregar nuevos nodos de cuadrícula o un sitio nuevo y aprueba los nodos de cuadrícula que desea agregar.
2. Se inicia la expansión.
3. Mientras se ejecuta el proceso de ampliación, se descarga un nuevo archivo de paquete de recuperación.
4. Supervisa el estado de las fases de configuración de la cuadrícula, que se ejecutan automáticamente. El conjunto de fases depende de los tipos de nodos de cuadrícula que se añadan y de si se va a añadir un sitio nuevo.

> Algunas etapas pueden tardar una cantidad significativa de tiempo en ejecutarse en una red 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 Cassandra" o "Inicio de Cassandra y transmisión de datos".

Pasos

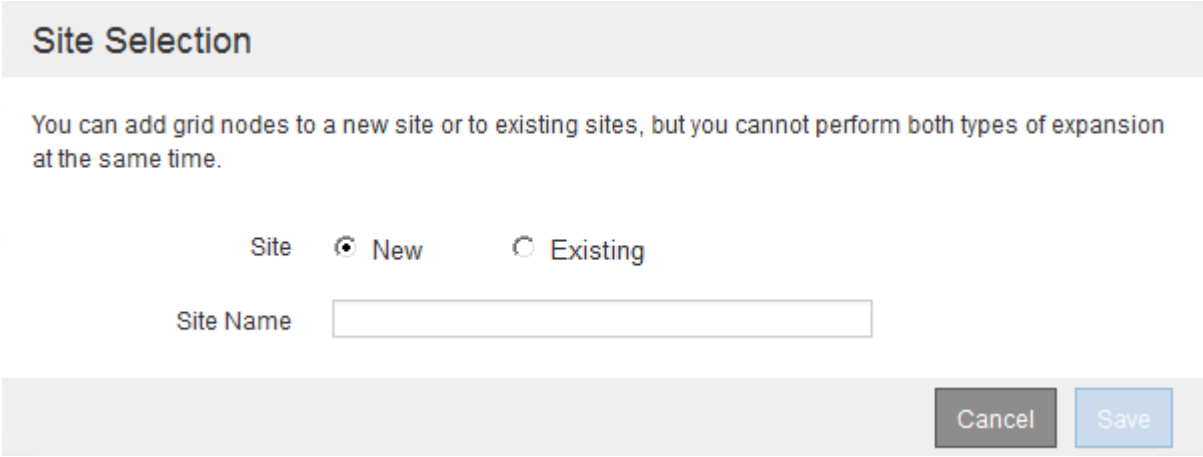
1. Seleccione **MANTENIMIENTO** > **tareas** > **expansión**.

   Aparece la página expansión de cuadrícula. En la sección Pending Nodes, se enumeran todos los nodos que están listos para añadirse.



2. Seleccione **Configurar expansión**.

   Aparece el cuadro de diálogo selección de sitio.



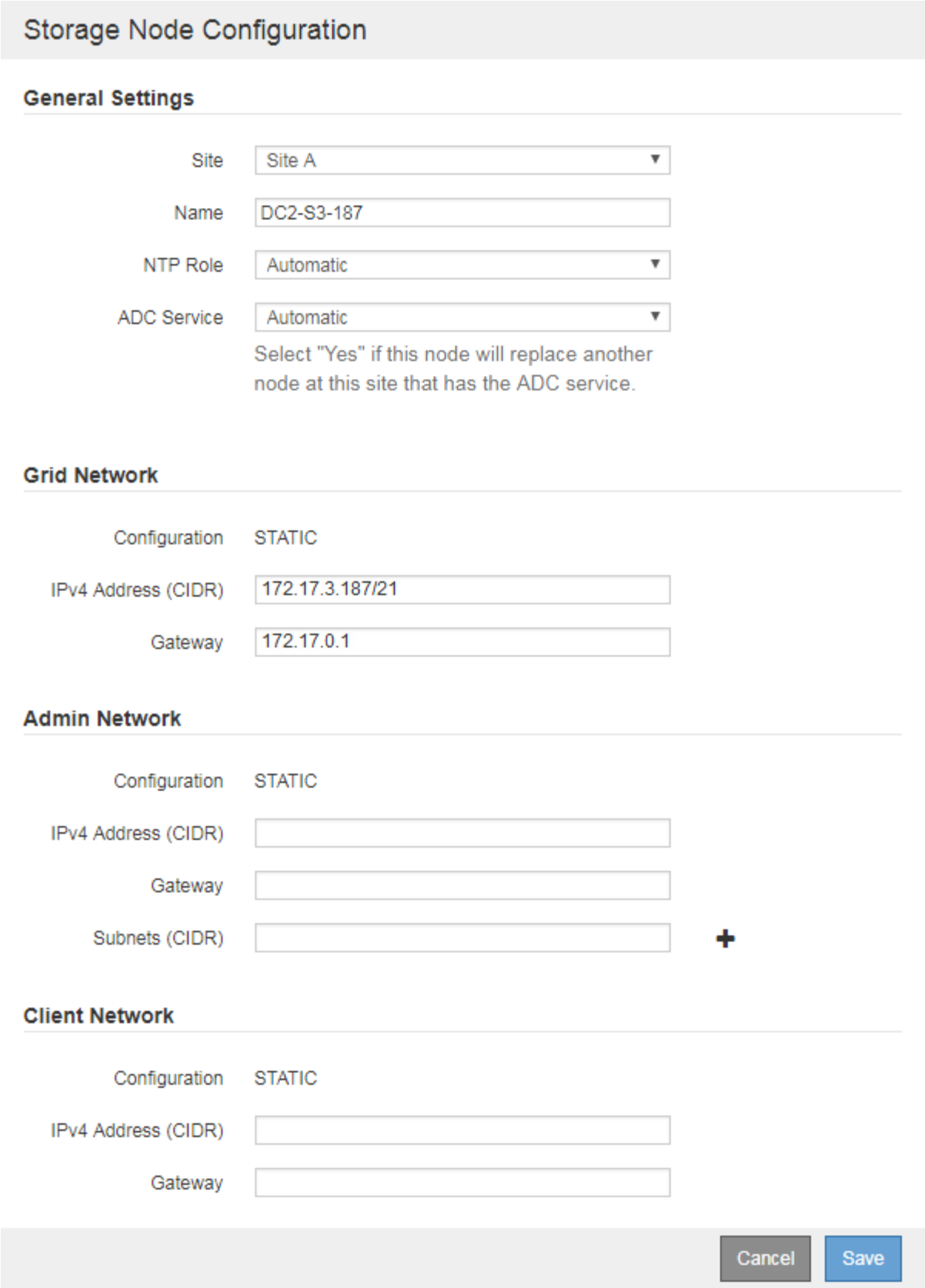
3. Seleccione el tipo de expansión que está iniciando:
   - Si va a añadir un sitio nuevo, seleccione **Nuevo** e introduzca el nombre del sitio nuevo.
   - Si va a agregar nodos de cuadrícula a un sitio existente, seleccione **existente**.
4. Seleccione **Guardar**.
5. Revise la lista **nodos pendientes** y confirme que muestra todos los nodos de cuadrícula que ha implementado.

   Según sea necesario, puede colocar el cursor sobre la dirección **red MAC** de un nodo para ver los detalles sobre ese nodo.

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

6. En la lista de nodos pendientes, apruebe los nodos de cuadrícula para 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:

- **Sitio**: El nombre del sitio con el que estará asociado el nodo Grid. 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 de host que se asignará al nodo y el nombre que se mostrará en Grid Manager.
- **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.

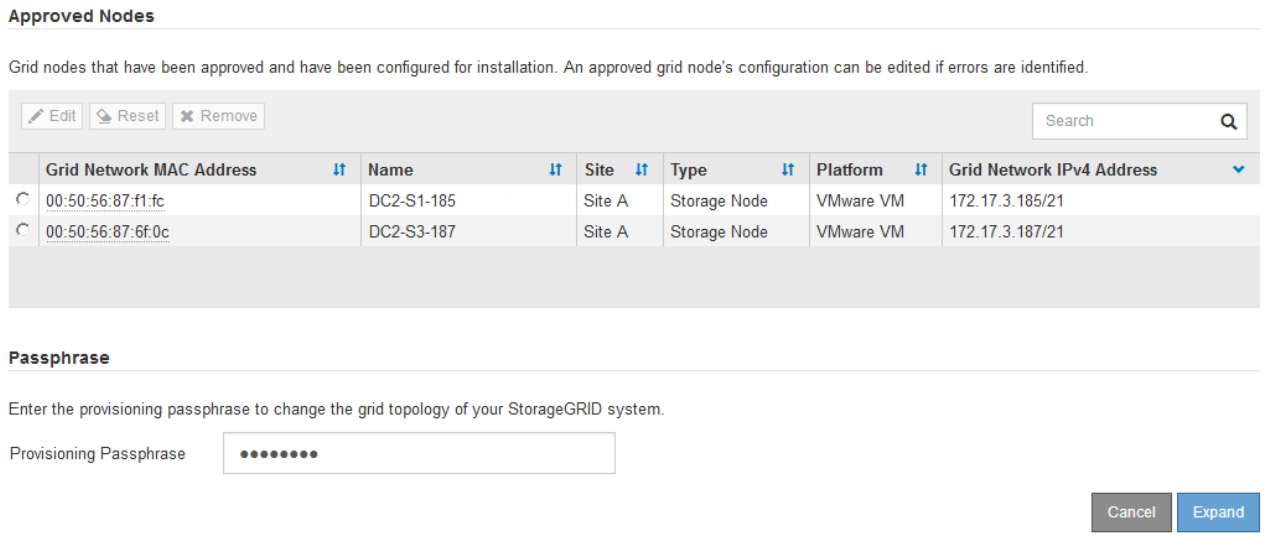
> Asigne el rol NTP primario al menos a dos nodos en cada sitio. Esto proporciona acceso redundante al sistema a fuentes de sincronización externas.

- **Servicio ADC** (sólo nodos de almacenamiento): Si este nodo de almacenamiento ejecutará 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 haberlo implementado.
  - Si va a agregar este nodo para reemplazar un nodo de almacenamiento, seleccione **Sí** si el nodo que va a reemplazar incluye el servicio ADC. Como no puede retirar un nodo de almacenamiento si se conservan muy pocos servicios ADC, esto garantiza que haya un nuevo servicio ADC disponible antes de que se elimine el servicio antiguo.
  - De lo contrario, seleccione **automático** para que el sistema pueda determinar si este nodo requiere el servicio ADC. Obtenga más información sobre el quórum de ADC aquí.

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
   - **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**.

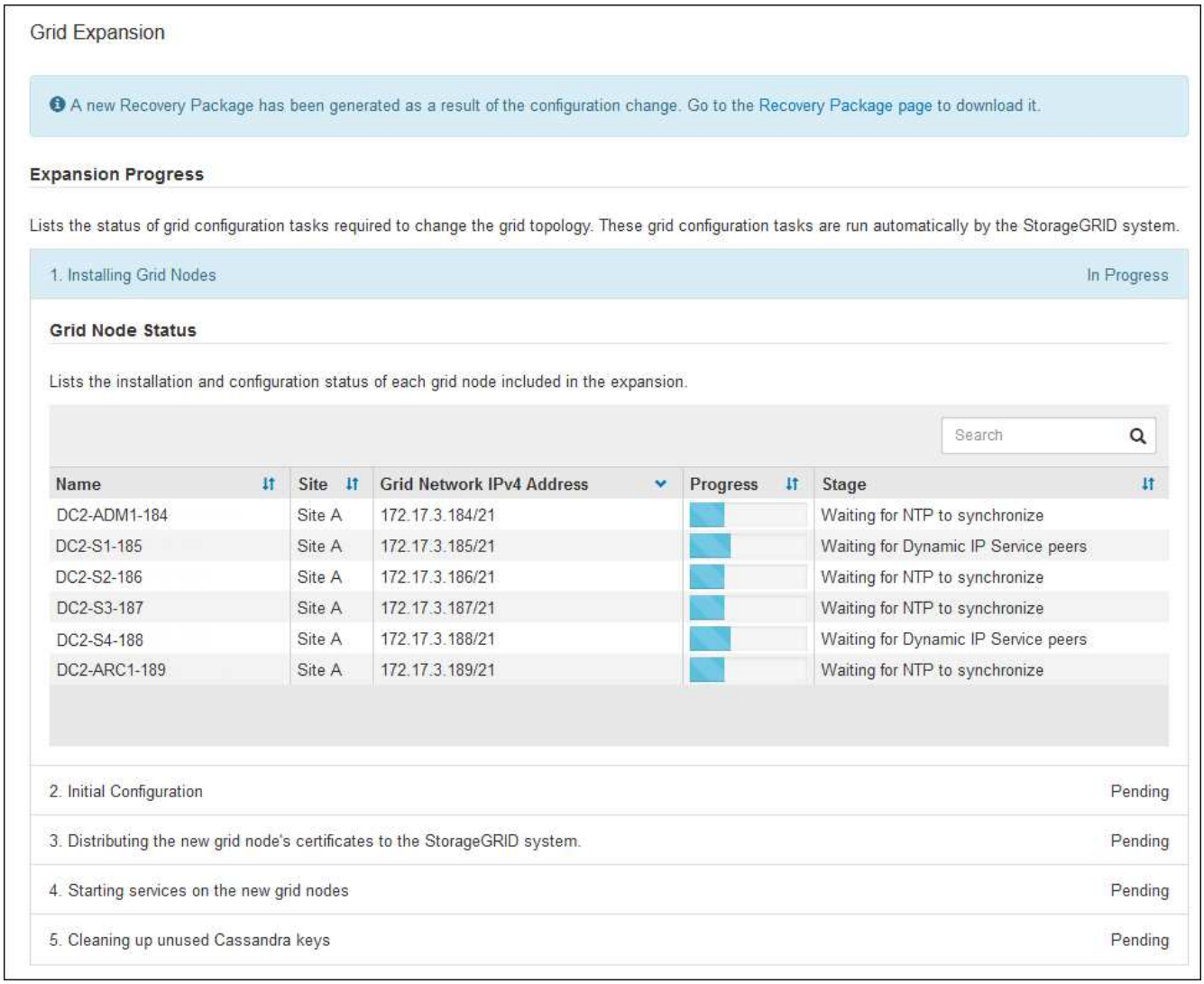
f. Repita estos pasos para cada nodo de cuadrícula pendiente que desee aprobar.

> 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 hay tareas que afectan a un nodo de cuadrícula individual en curso, la sección Estado del nodo de cuadrícula muestra el estado actual de cada nodo de cuadrícula.

> Durante este proceso, en el caso de los dispositivos, el instalador del dispositivo StorageGRID muestra el cambio de la instalación 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.

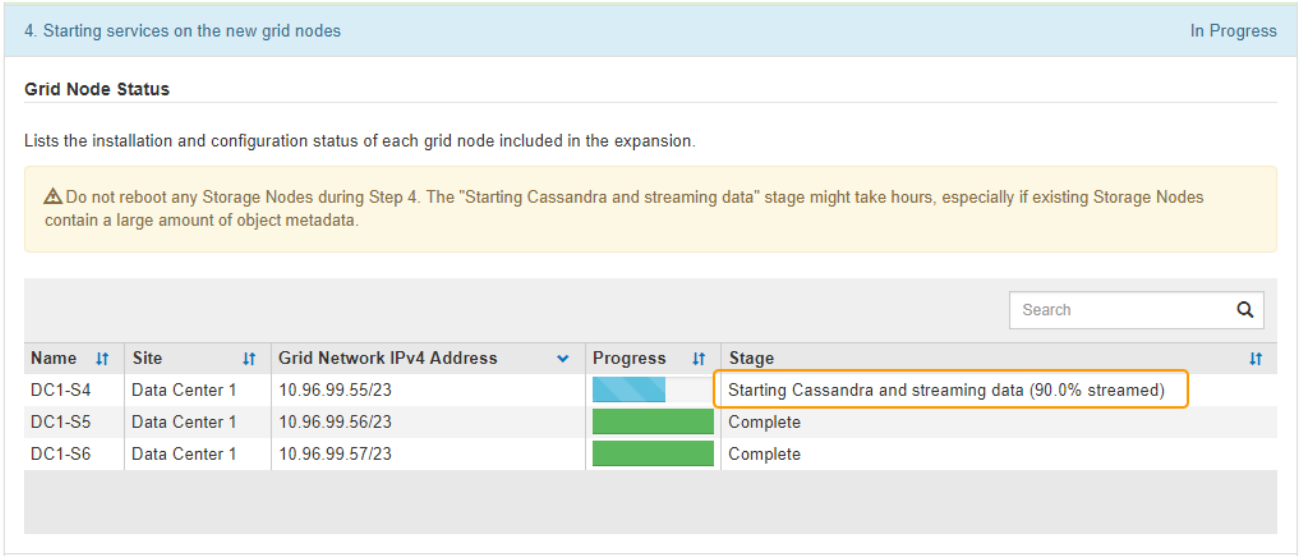
   a. Seleccione el enlace de descarga.
   b. Introduzca la frase de acceso de aprovisionamiento y seleccione **Iniciar descarga**.
   c. Cuando finalice la descarga, abra la `.zip` archivar y confirmar que incluye un `gpt-backup` directorio y a `_SAID.zip` archivo. A continuación, extraiga el `_SAID.zip` vaya a `/GID*_REV*` y confirme que puede abrir el `passwords.txt` archivo.
   d. Copie el archivo del paquete de recuperación descargado (.zip) 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.

9. Siga las instrucciones para añadir un nodo de almacenamiento a un sitio existente o añadir otro nuevo.

Añada el nodo de almacenamiento al sitio existente

Si va a añadir uno o más nodos de almacenamiento a un sitio existente, supervise el progreso de la etapa "iniciando Cassandra y streaming de datos" revisando el porcentaje que se muestra en el mensaje de estado.



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.

> No reinicie ningún nodo de almacenamiento durante las etapas de "expansión del clúster 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.

Agregar nuevo 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.

> No reinicie ningún nodo de almacenamiento durante las etapas de "expansión del clúster 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.

1. 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 añadido, debe realizar 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 enumeran a continuación para los nodos de grid que va a añadir en la ampliación. Algunas tareas pueden ser opcionales, en función de las opciones seleccionadas al instalar y administrar el sistema, y de cómo se desean configurar los nodos de cuadrícula agregados durante la expansión.

Pasos

1. Si añadió un nodo de almacenamiento, complete las siguientes tareas de configuración:
   a. Revise los pools de almacenamiento utilizados en las reglas de ILM para garantizar que se utilizará el nuevo almacenamiento. Consulte Gestión de objetos con ILM.
      - Si agregó un sitio, cree un pool de almacenamiento para el sitio y actualice las reglas de ILM para usar el nuevo pool de almacenamiento.
      - Si ha añadido un nodo de almacenamiento a un sitio existente, confirme que el nodo nuevo utiliza el grado de almacenamiento correcto.

      > De forma predeterminada, se asigna un nuevo nodo de almacenamiento al grado de almacenamiento todos los nodos de almacenamiento y se añade a los pools de almacenamiento que utilizan ese grado para el sitio. Si desea que un nodo nuevo utilice un grado de almacenamiento personalizado, debe asignarlo manualmente al grado personalizado (**ILM** > **grados de almacenamiento**).

   b. Compruebe que el nodo de almacenamiento ingiere objetos. Consulte Compruebe que el nodo de almacenamiento esté activo.
   c. Reequilibre los datos con código de borrado (solo si no pudo añadir el número recomendado de nodos de almacenamiento). ConsulteReequilibre los datos con código de borrado tras añadir nodos de almacenamiento.
2. Si agregó un nodo de puerta de enlace, complete la siguiente tarea de configuración:
   - 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 Administre StorageGRID.
3. Si añadió un nodo de administrador, complete las siguientes tareas de configuración:
   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 la confianza de la parte de confianza. ConsulteConfigurar 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 Administre StorageGRID.
   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.

f. De manera opcional, configure el acceso al sistema para realizar auditorías a través de un recurso compartido de archivos NFS o CIFS. Consulte Administre StorageGRID.

> La exportación de auditorías por CIFS/Samba ha sido obsoleta y se eliminará en una futura versión de StorageGRID.

g. Si lo desea, puede cambiar el remitente preferido para las notificaciones. Puede hacer que el nodo de administración de expansión sea el remitente preferido. De lo contrario, un nodo de administrador existente configurado como remitente preferido sigue enviando notificaciones, incluidos los mensajes de AutoSupport, las notificaciones SNMP, los correos electrónicos de alerta y los correos electrónicos de alarma (sistema heredado). Consulte Administre StorageGRID.

4. Si agregó un nodo de archivado, complete las siguientes tareas de configuración.

   a. Configure la conexión del nodo de archivado al sistema de almacenamiento de archivado externo de destino. Cuando complete la expansión, los nodos de archivo estarán en estado de alarma hasta que configure la información de conexión a través del componente **ARC** > **Target**. Consulte Administre StorageGRID.

   b. Actualice la política de ILM para archivar datos de objetos mediante el nuevo nodo de archivado. Consulte Gestión de objetos con ILM.

   c. Configurar alarmas personalizadas para los atributos que se utilizan para supervisar la velocidad y eficacia de la recuperación de datos de objetos desde los nodos de archivo. Consulte Administre StorageGRID.

5. Para comprobar si se han agregado nodos de expansión con una red cliente no confiable o si para cambiar si la red cliente de un nodo no es de confianza o no es de confianza, vaya a **CONFIGURACIÓN** > **Red** > **Red cliente no confiable**.

   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 Administre StorageGRID.

6. Configure el sistema de nombres de dominio (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.

   La práctica recomendada es que la lista de servidores DNS de toda la cuadrícula contenga algunos servidores DNS a los que se puede acceder localmente desde cada sitio. Si acaba de agregar un sitio nuevo, agregue nuevos servidores DNS para el sitio a la configuración DNS de toda la cuadrícula.

> Proporcione de dos a seis direcciones IPv4 para los servidores DNS. Debe seleccionar los servidores DNS a los que puede acceder cada sitio localmente en el caso de que la red sea de destino. Esto es para asegurar que un sitio de llanded siga teniendo acceso al servicio DNS. Después de configurar la lista de servidores DNS para toda la cuadrícula, puede personalizar aún más la lista de servidores DNS para cada nodo. Para obtener más información, consulte Modifique la configuración de DNS para un solo nodo de grid..

7. Si ha agregado un sitio nuevo, confirme que se puede acceder a los servidores de protocolo de tiempo de redes (NTP) desde ese sitio. Consulte Configure los 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.

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. Pase el cursor sobre el gráfico **almacenamiento usado - datos de objeto** para ver el valor de **utilizado**, que es la cantidad de espacio útil total 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.

Lo que necesitará

- 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.

Lo que necesitará

- 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.

Lo que necesitará

- 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. Cambie el nombre de `audit.log` Archivo para asegurarse de que no sobrescribe el archivo en el nodo de administración de expansión al que está copiando:

```
cd /var/local/audit/export
ls -l
mv audit.log new_name.txt
```

4. Copie todos los archivos de registro de auditoría en el nodo de administración de expansión:

```
scp -p * IP_address:/var/local/audit/export
```

5. 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.
6. Restaure el original `audit.log` archivo:

```
mv new_name.txt audit.log
```

7. Inicie el servicio AMS:

```
service ams start
```

8. Cierre la sesión en el servidor:

```
exit
```

9. 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 `#`.

10. Actualice la configuración del usuario y del grupo para los archivos de registro de auditoría:

```
cd /var/local/audit/export
chown ams-user:bycast *
```

11. Cierre la sesión en el servidor:

```
exit
```

Reequilibre los datos con código de borrado tras añadir nodos de almacenamiento

En algunos casos, es posible que deba reequilibrar los datos de código de borrado al añadir nuevos nodos de almacenamiento.

Lo que necesitará

- 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.

> Realice este procedimiento sólo si se ha activado la alerta **almacenamiento de objetos bajo** para uno o más nodos de almacenamiento de un sitio y no pudo agregar el número recomendado de nuevos nodos de almacenamiento.

- 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.

Acerca de esta tarea

Cuando se ejecuta el procedimiento de reequilibrio de EC, el rendimiento de las operaciones de ILM y las operaciones del cliente S3 y Swift probablemente se verán afectadas. Por este motivo, solo debe realizar este procedimiento en casos limitados.

> 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.

> Las operaciones de API de S3 y Swift para cargar objetos (o partes de objetos) pueden fallar durante el procedimiento de reequilibrio de EC si se necesitan más de 24 horas para completarse. Se producirá un error en las operaciones DE COLOCACIÓN de larga duración si la regla de ILM aplicable utiliza una ubicación estricta o equilibrada en el procesamiento. Se informará del siguiente error:
>
> `500 Internal Server Error`

Pasos

1. Revise los detalles del almacenamiento de objetos actual para el sitio que planea reequilibrar.
   a. Seleccione **NODES**.
   b. Seleccione el primer nodo de almacenamiento del sitio.
   c. Seleccione la ficha **almacenamiento**.
   d. Pase el cursor sobre el gráfico almacenamiento usado - datos de objetos para ver la cantidad actual de datos replicados y los datos codificados para 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. Introduzca el siguiente comando:

   ```
   rebalance-data start --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. Supervisar 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`

- Para ver el tiempo estimado hasta la finalización y el porcentaje de finalización del trabajo actual, seleccione **SUPPORT** > **Tools** > **Metrics**. 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**.

6. Realice pasos adicionales según el estado devuelto:
   - Si el estado es `In progress`, La operación de reequilibrio de EC todavía se está ejecutando. Deberá supervisar el procedimiento de forma periódica hasta que finalice.
   - Si el estado es `Failure`, realice la pasos de fallo.
   - Si el estado es `Success`, realice la paso del éxito.
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
   ```

   > Al finalizar un procedimiento de reequilibrio de EC, los fragmentos de datos que ya se hayan movido permanecen en la nueva ubicación. Los datos no se mueven de nuevo a la ubicación original.

9. Si el estado del procedimiento de reequilibrio de EC es `Failure`, siga estos pasos:
   a. Confirmar que todos los nodos de almacenamiento del sitio están conectados a la cuadrícula.
   b. Compruebe y resuelva las alertas que puedan afectar a estos nodos de almacenamiento.

      Para obtener información sobre alertas específicas, consulte las instrucciones de supervisión y solución de problemas.

   c. Reinicie el procedimiento de reequilibrio de EC:
      `rebalance-data start --job-id job-id`
   d. Si el estado del procedimiento de reequilibrio de la CE es todavía `Failure`, póngase en contacto con el soporte técnico.
10. Si el estado del procedimiento de reequilibrio de EC 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.

11. Si utiliza la codificación de borrado en más de una instalación, ejecute este procedimiento para el resto de las ubicaciones afectadas.

Póngase en contacto con el soporte técnico

Si se producen errores durante el proceso de expansión de cuadrícula que no puede resolver o si una tarea de cuadrícula falla, póngase en contacto con el soporte técnico.

Acerca de esta tarea

Cuando se pone en contacto con el soporte técnico, se deben proporcionar los archivos de registro necesarios para ayudar a solucionar los errores que se encuentran.

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.

   Una vez que haya iniciado sesión como root, el símbolo del sistema cambia de `$` 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)

Recuperación y mantenimiento

Recuperación y mantenimiento: Descripción general

Siga estas instrucciones para mantener su sistema StorageGRID y recuperarse de fallos.

Acerca de estas instrucciones

Estas instrucciones describen cómo aplicar una revisión de software, recuperar nodos de cuadrícula, recuperar un sitio fallido, retirar nodos de red o un sitio entero, realizar el mantenimiento de la red, realizar procedimientos de mantenimiento de nivel de host y middleware y realizar procedimientos de nodo de red.

> En estas instrucciones, '"Linux"' se refiere a una implementación de Red Hat® Enterprise Linux®, Ubuntu®, CentOS o Debian®. Utilice la "Herramienta de matriz de interoperabilidad de NetApp" para obtener una lista de las versiones compatibles.

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.
- Comprende 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 las instrucciones de instalación y mantenimiento de su dispositivo StorageGRID.

- Servicios de aplicaciones SG100 y SG1000
- Dispositivos de almacenamiento SG6000
- Dispositivos de almacenamiento SG5700
- Dispositivos de almacenamiento SG5600

Descargue el paquete de recuperación

El archivo de paquete de recuperación permite restaurar el sistema StorageGRID en caso de producirse un fallo.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener la clave de acceso de aprovisionamiento.
- Debe tener 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. Introduzca la frase de acceso de aprovisionamiento y seleccione **Iniciar descarga**.

   La descarga comienza inmediatamente.

3. Cuando finalice la descarga:
   a. Abra el `.zip` archivo.
   b. Confirme que incluye un directorio gpt-backup y un directorio interno `.zip` archivo.
   c. Extraer el interior `.zip` archivo.
   d. Confirme que puede abrir 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.

Información relacionada

Administre StorageGRID

Procedimiento de revisión de StorageGRID

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

Al aplicar una revisión, se aplica una serie acumulada de actualizaciones de software a los nodos de su sistema StorageGRID.

No puede aplicar una revisión StorageGRID cuando se ejecuta otro procedimiento de mantenimiento. Por ejemplo, no puede aplicar una revisión mientras se está ejecutando un procedimiento de retirada, 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 grid» 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.

   > Según sea necesario para que coincida con la versión de la cuadrícula, puede utilizar una versión secundaria al implementar el nodo; no es necesario poner en marcha la versión principal primero.

4. A continuación, aplica la revisión 11.*A.B.y* al nodo de administración principal.

Información relacionada

Configure el nodo de administración principal de reemplazo

Planifique y prepare una revisión

Debe planificar antes de aplicar una revisión para garantizar una interrupción mínima en su sistema StorageGRID.

Pasos

- Cómo se ve afectado el sistema cuando se aplica una revisión
- Obtener los materiales necesarios para una revisión
- Descargando el archivo de revisión
- Comprobación de la condición del sistema antes de aplicar una revisión

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 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, especificar subredes de red de cuadrícula o aprobar nodos de cuadrícula pendientes) hasta que la revisión se haya aplicado a todos los nodos.
- No actualice la configuración de ILM hasta que la revisión 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)	
Paquete de recuperación (`.zip`)	Antes de aplicar una revisión, Descargue el archivo más reciente del paquete de recuperación En caso de que se produzcan problemas durante la revisión.a continuación, después de que se haya aplicado la revisión, descargue una copia nueva del archivo de 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.

Elemento	Notas
Archivo Passwords.txt	Opcional y utilizado sólo si aplica una revisión manualmente mediante el cliente SSH. La `Passwords.txt` El archivo se incluye en DICHO paquete, que 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.

Información relacionada

Descargue el archivo de revisión

Descargue el archivo de revisión

Debe descargar el archivo de revisión antes de poder aplicar la revisión.

Pasos

1. Vaya a la página de descargas de NetApp para StorageGRID.

   "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 acaba de recuperar el nodo de administración principal y necesita aplicar una revisión, seleccione la misma versión de revisión que está instalada en los otros nodos de cuadrícula.

   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**.

Información relacionada

Configure el nodo de administración principal de reemplazo

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.

   Para obtener información sobre alertas específicas, consulte las instrucciones de supervisión y solución de problemas de StorageGRID.

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 StorageGRID cuando se ejecuta otro procedimiento de mantenimiento. Por ejemplo, no puede aplicar una revisión mientras se está ejecutando un procedimiento de retirada, 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.

Información relacionada

Supervisión y solución de problemas

Pausar y reanudar el proceso de retirada de los nodos de almacenamiento

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.

Lo que necesitará

- Ha revisado las consideraciones y completado los pasos de Planifique y prepare una revisión.
- Tiene la clave de acceso de aprovisionamiento.
- Tiene acceso raíz o permiso de mantenimiento.

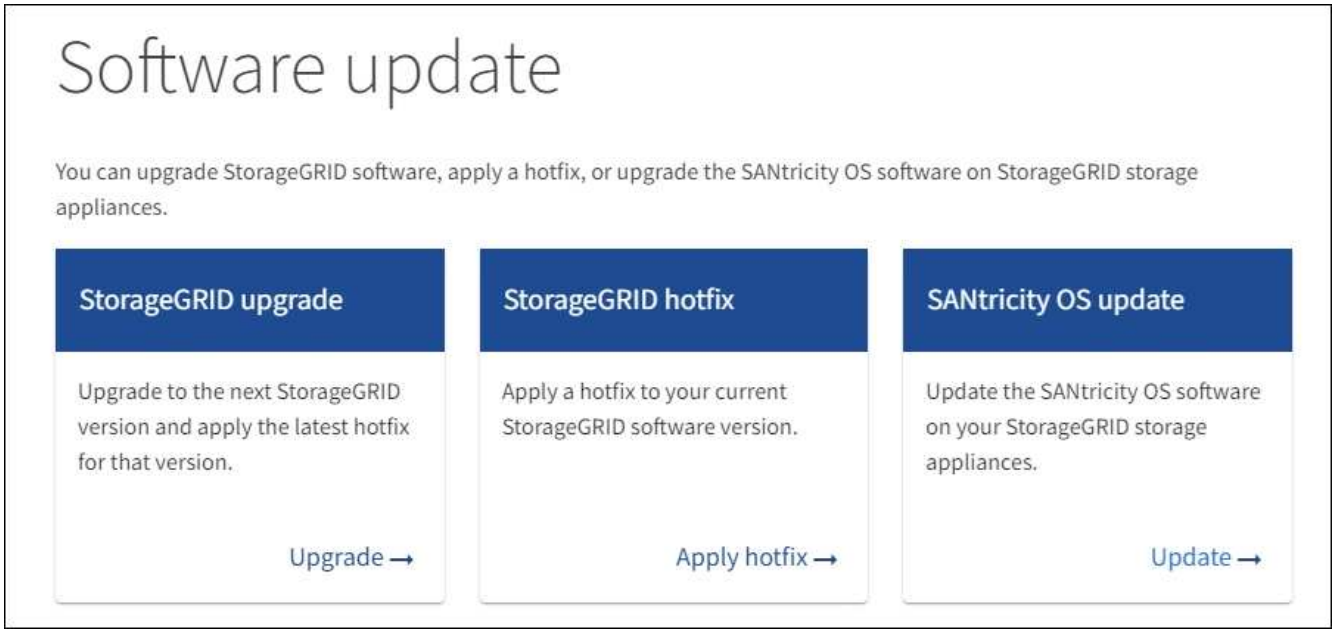
Acerca de esta tarea

- 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 revisión.

Pasos

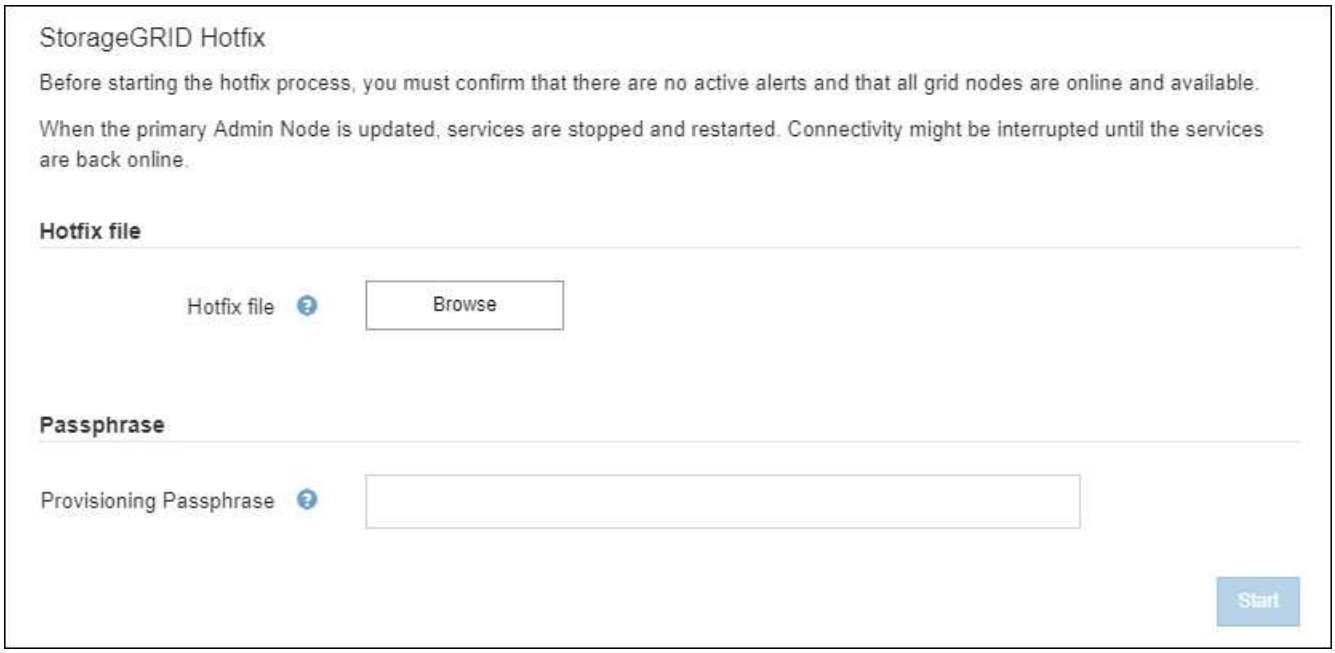
1. Inicie sesión en Grid Manager mediante una navegador web compatible.
2. Seleccione **MANTENIMIENTO** > **sistema** > **actualización de software**.

   Aparece la página actualización de software.



3. Seleccione **aplicar revisión**.

   Aparece la página de corrección de StorageGRID.



4. Seleccione el archivo de revisión 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.

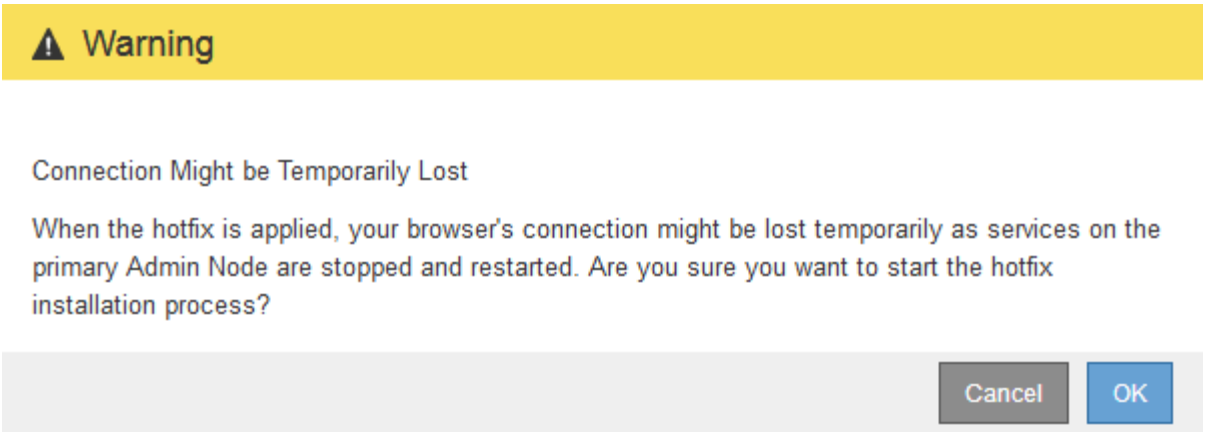
      No cambie el nombre del archivo ya que forma parte del proceso de verificación.

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:

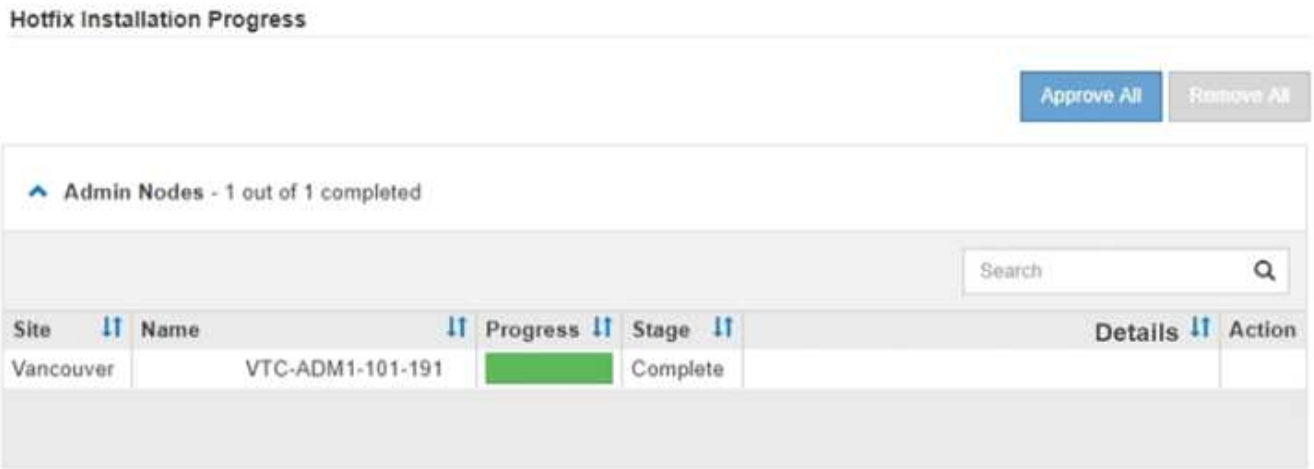
   a. Se ejecutan las validaciones de la revisión.

      > 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
      - Nodos de archivado

      > La barra de progreso llega a su finalización y, a continuación, se muestra primero el nodo de administración principal con la fase "'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 para un nodo a menos que esté seguro de que el nodo está listo para ser actualizado.cuando la revisión se aplica a un nodo de cuadrícula, algunos servicios de ese nodo podrían reiniciarse. 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.

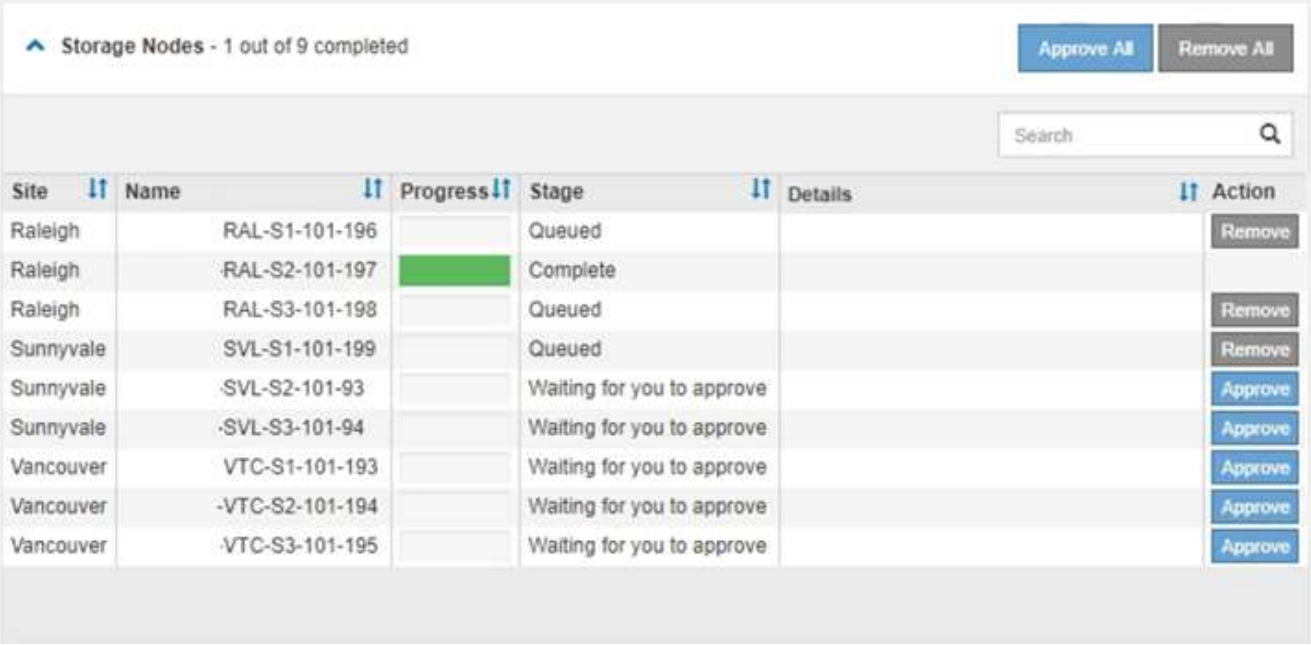
> El botón **aprobar todo** situado en la parte superior de la página aprueba todos los nodos enumerados en la página, mientras que el botón **aprobar todo** situado en la parte superior de una agrupación de tablas sólo aprueba todos los nodos de ese grupo. Si el orden en el que se actualizan los nodos 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 el escenario progresa más allá de "'Queued,'" el botón **Remove** está oculto y ya no puede quitar 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.

Información relacionada

Administre StorageGRID

Supervisión y solución de problemas

Procedimientos de recuperación de nodos de grid

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.

Información relacionada

Cómo realiza la recuperación del sitio el soporte técnico

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 snapshots 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 de instalador de dispositivos de StorageGRID del dispositivo de reemplazo coincide con la versión de software de su sistema StorageGRID, como se describe en instalación y mantenimiento del hardware para verificar y actualizar la versión de instalador de dispositivos de StorageGRID.
  - Servicios de aplicaciones SG100 y SG1000
  - Dispositivos de almacenamiento SG5600
  - Dispositivos de almacenamiento SG5700
  - Dispositivos de almacenamiento SG6000
- 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 con una dirección IP asignada actualmente a ningún 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.
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 para 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 o CentOS	`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 Red Hat Enterprise Linux o sistema CentOS, 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 RPM para instalar las imágenes de nodo StorageGRID en sus hosts RHEL o CentOS.
	PAQUETE RPM para instalar el servicio host StorageGRID en sus hosts RHEL o CentOS.
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.
	Un archivo de configuración en blanco para usar con el `configure-storagegrid.py` guión.
	Ejemplo de rol de Ansible y libro de estrategia para configurar hosts de RHEL o CentOS para puesta en marcha del contenedor StorageGRID. Puede personalizar el rol o el libro de estrategia según sea necesario.

Ruta y nombre de archivo	Descripción
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede utilizar estos esquemas para confirmar que cualquier código que haya escrito para utilizar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no dispone de un entorno StorageGRID que no sea de producción para la comprobación de compatibilidad de actualizaciones.

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.

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.
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede utilizar estos esquemas para confirmar que cualquier código que haya escrito para utilizar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no dispone de un entorno StorageGRID que no sea de producción para la comprobación de compatibilidad de actualizaciones.

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.
	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.

Ruta y nombre de archivo	Descripción
	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.
	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.
	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.

Ruta y nombre de archivo	Descripción
	Esquemas de API para StorageGRID. **Nota**: Antes de realizar una actualización, puede utilizar estos esquemas para confirmar que cualquier código que haya escrito para utilizar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no dispone de un entorno StorageGRID que no sea de producción para la comprobación de compatibilidad de actualizaciones.

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 del paquete DE instalación DE DEB utilizado por el instalador de dispositivos de StorageGRID para validar que el paquete está intacto tras la carga.

> 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 realiza la recuperación del sitio el soporte técnico
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 grid	Procedimiento de recuperación
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

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.	Debe comunicarse con el soporte técnico.	Si todos los nodos de almacenamiento con fallos se encuentran en el mismo sitio, es posible que sea necesario realizar un procedimiento de recuperación del sitio. El soporte técnico evaluará su situación y desarrollará un plan de recuperación. Cómo realiza la recuperación del sitio 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.
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.

Problema	Acción	Notas
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. Puede que note un resultado de script que menciona "relativamente" o ""reparación de Cassandra"". Si aparece 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.

Lo que necesitará

- 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 a la cuadrícula hasta que se reconstruye Cassandra 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. Póngase en contacto con el soporte técnico.

Cómo realiza la recuperación del sitio el soporte técnico

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.

1. 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 Grid topolog a**.
   c. Seleccione ***Site* nodo de almacenamiento SSM Servicios**. Compruebe que aparece el servicio Cassandra `Not Running`.
   d. Seleccione **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
```

2. Emita este comando y supervise el resultado del script: `check-cassandra-rebuild`
   - Si los servicios de almacenamiento se están ejecutando, se le solicitará que los detenga. Introduzca: **Y**
   - 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. Puede que note un resultado de script que menciona "relativamente" o ""reparación de Cassandra"". Si aparece un mensaje de error que indica que la reparación ha fallado, ejecute el comando indicado en el mensaje de error.

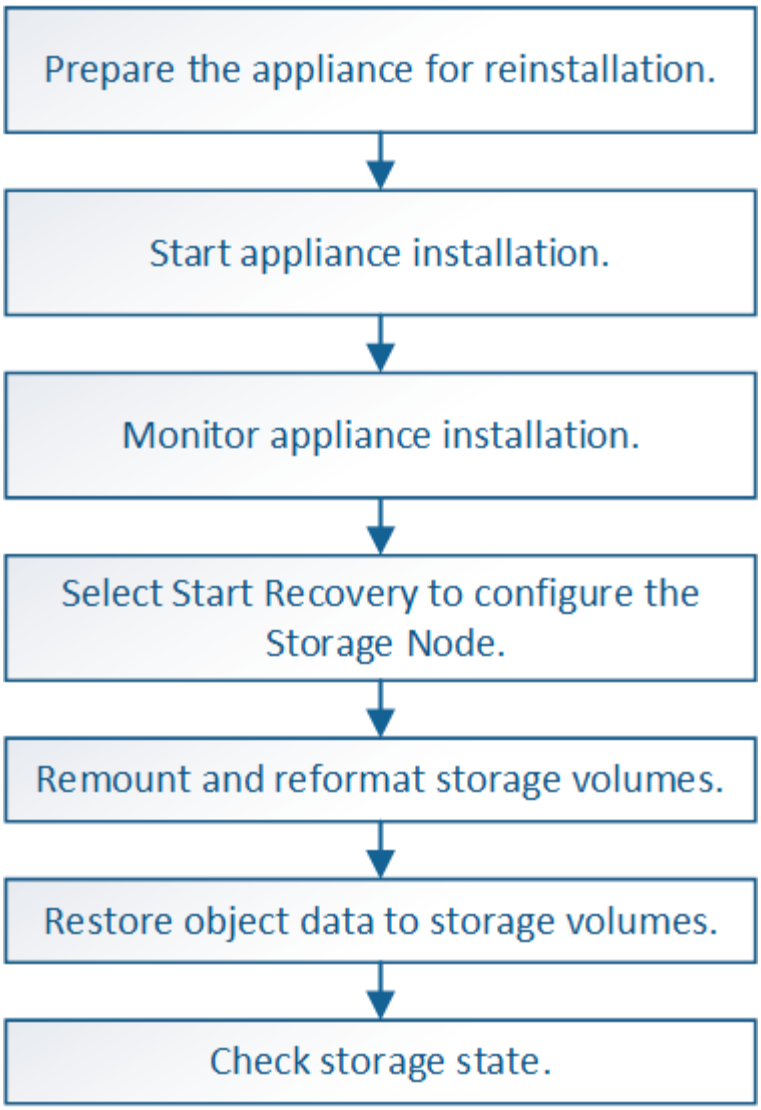
3. Una vez finalizada la reconstrucción, realice las siguientes comprobaciones:
   a. En Grid Manager, seleccione **SUPPORT Tools Grid topolog a**.
   b. Seleccione ***Site* nodo de almacenamiento recuperado SSM Servicios**.
   c. Confirme que todos los servicios están en ejecución.
   d. Seleccione **DDS almacén de datos**.
   e. Confirmar que **Estado del almacén de datos** es «'Arriba'» y que **Estado del almacén de datos** es «'normal'».

Recupere el nodo 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.

Acerca de esta tarea

Debe preparar el dispositivo y reinstalar el software, configurar el nodo para volver a unirse a la cuadrícula, volver a formatear el almacenamiento y restaurar los datos de los objetos.



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. Póngase en contacto con el soporte técnico.

Cómo realiza la recuperación del sitio el soporte técnico

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 de Servicios: Estado - Cassandra (SVST) durante la recuperación, consulte las instrucciones de supervisión y solución de problemas para recuperar la alarma reconstruyendo Cassandra. Una vez reconstruida Cassandra, las alarmas se deberían borrar. Si las alarmas no se borran, póngase en contacto con el soporte técnico.

Para obtener información sobre procedimientos de mantenimiento del hardware, como instrucciones para reemplazar un controlador o reinstalar SANtricity OS, consulte las instrucciones de instalación y mantenimiento del dispositivo de almacenamiento.

Información relacionada

Supervisión y solución de problemas

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG5600

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.

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.

   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.

Lo que necesitará

- 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 y mantenimiento de su dispositivo de almacenamiento:
  - Dispositivos de almacenamiento SG5600
  - Dispositivos de almacenamiento SG5700
  - Dispositivos de almacenamiento SG6000
- 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 administrador 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 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.

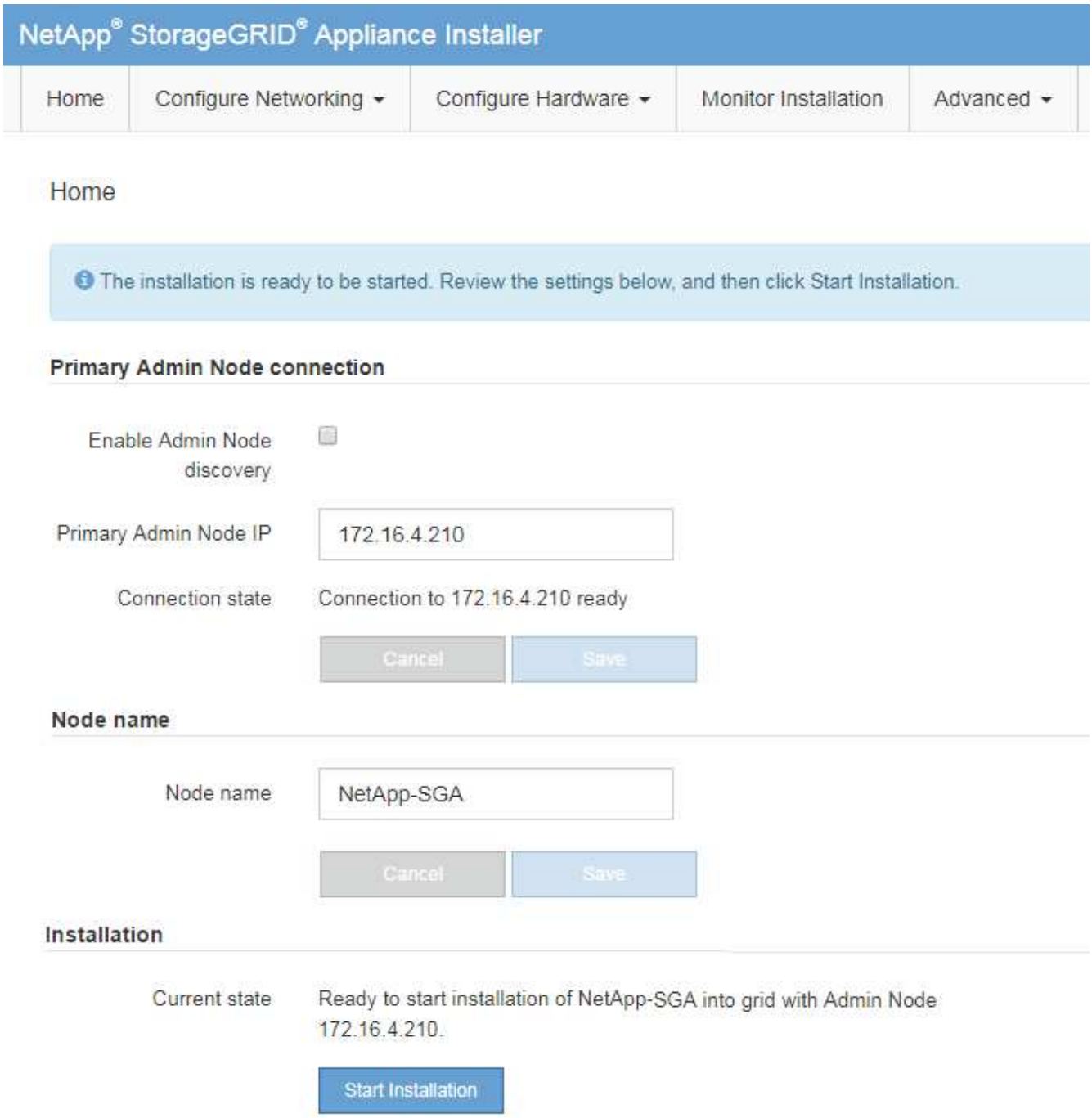
3. Si no se muestra esta dirección IP o es necesario modificarla, especifique la dirección:

Opción	Pasos
Entrada IP manual	a. Anule la selección de la casilla de verificación **Activar descubrimiento de nodo de administración**. b. Introduzca la dirección IP de forma manual. c. Haga clic en **Guardar**. d. Espere mientras el estado de conexión para la nueva dirección IP se convierte en "muy listo".
Detección automática de todos los nodos principales de administración conectados	a. Active la casilla de verificación **Activar descubrimiento de nodos de administración**. 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 mientras el estado de conexión para la nueva dirección IP se convierte en "muy listo".

4. En el campo **Nombre de nodo**, introduzca el mismo nombre 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 "'preparado para iniciar la instalación del nombre del nodo en la cuadrícula con el nodo de administración principal admin_ip'" y que el botón **Iniciar instalación** 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 instalación y mantenimiento del 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.

Información relacionada

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

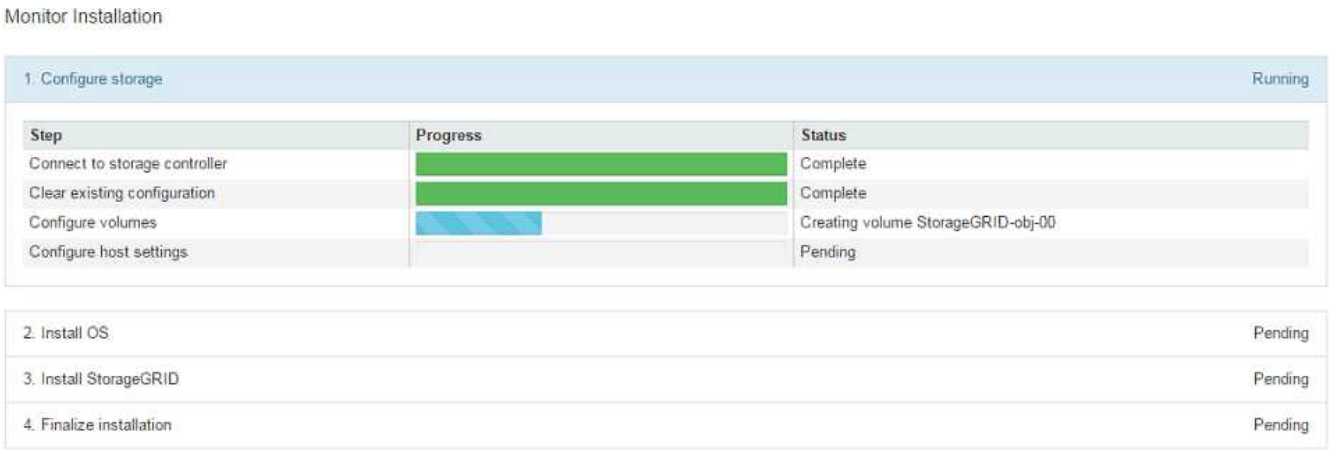
Dispositivos de almacenamiento SG5600

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.

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.

   > El instalador garantiza que no se vuelvan a ejecutar las tareas completadas en una instalación anterior. 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 de "Shided."

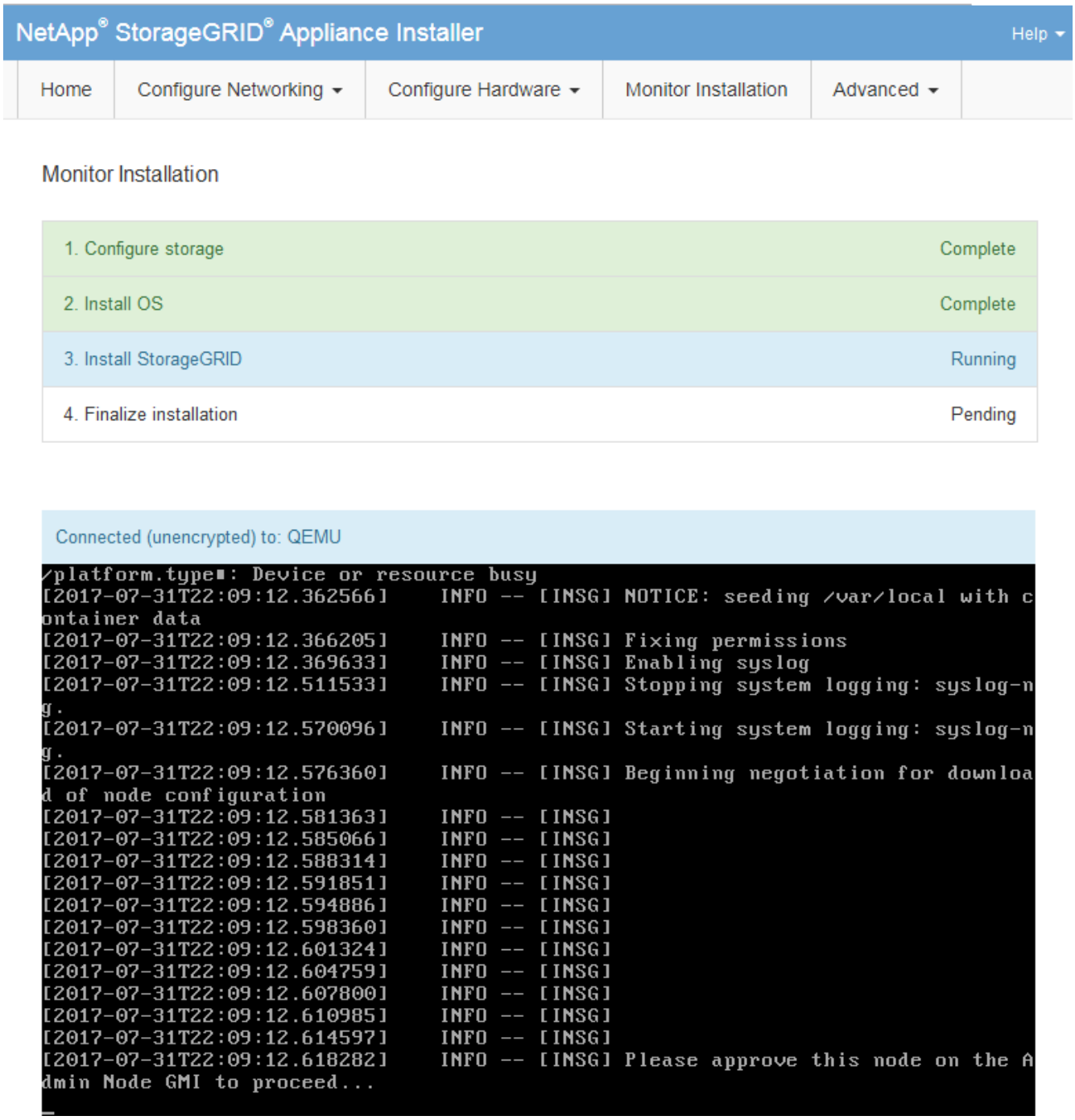
2. Revise el progreso de las dos primeras etapas de instalación.
   - **1. Configurar almacenamiento**

     Durante esta fase, el instalador se conecta al controlador de almacenamiento, borra cualquier configuración existente, se comunica con el software 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 al procedimiento 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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener los permisos de mantenimiento o acceso raíz.
- Debe tener la clave de acceso de aprovisionamiento.

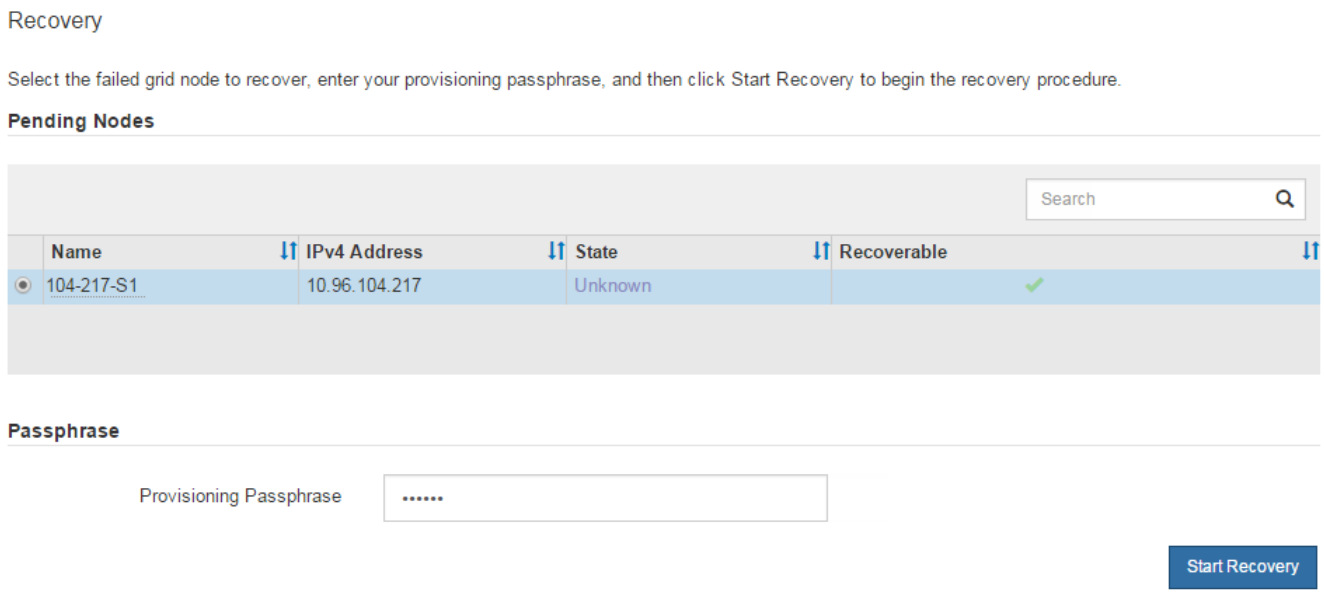
- Debe haber puesto en marcha un nodo de almacenamiento del dispositivo de recuperación.
- Debe conocer la fecha de inicio de los trabajos de reparación para los datos codificados mediante borrado.
- Debe haber verificado que el nodo de almacenamiento no se ha reconstruido en los últimos 15 días.

Pasos

1. En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **recuperación**.
2. Seleccione el nodo de cuadrícula que desea recuperar en la lista Pending Nodes.

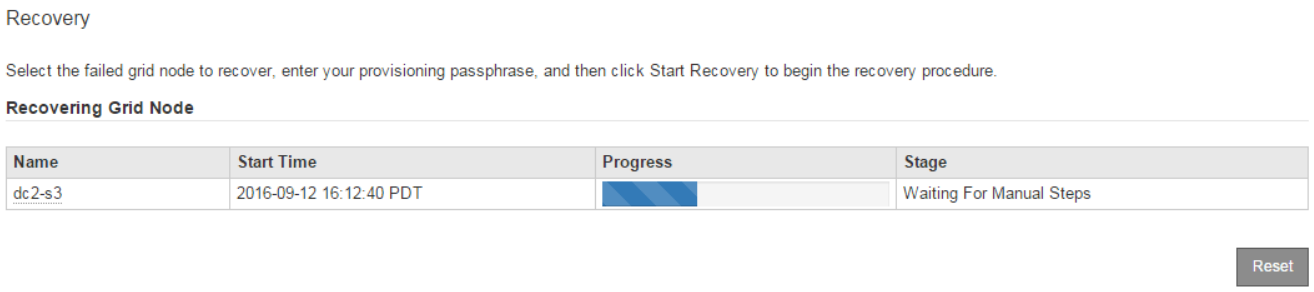
   Los nodos aparecen en la lista después de que fallan, pero no podrá seleccionar un nodo hasta que se haya vuelto a instalar y esté listo para la recuperación.

3. Introduzca la **frase de paso de aprovisionamiento**.
4. Haga clic en **Iniciar recuperación**.

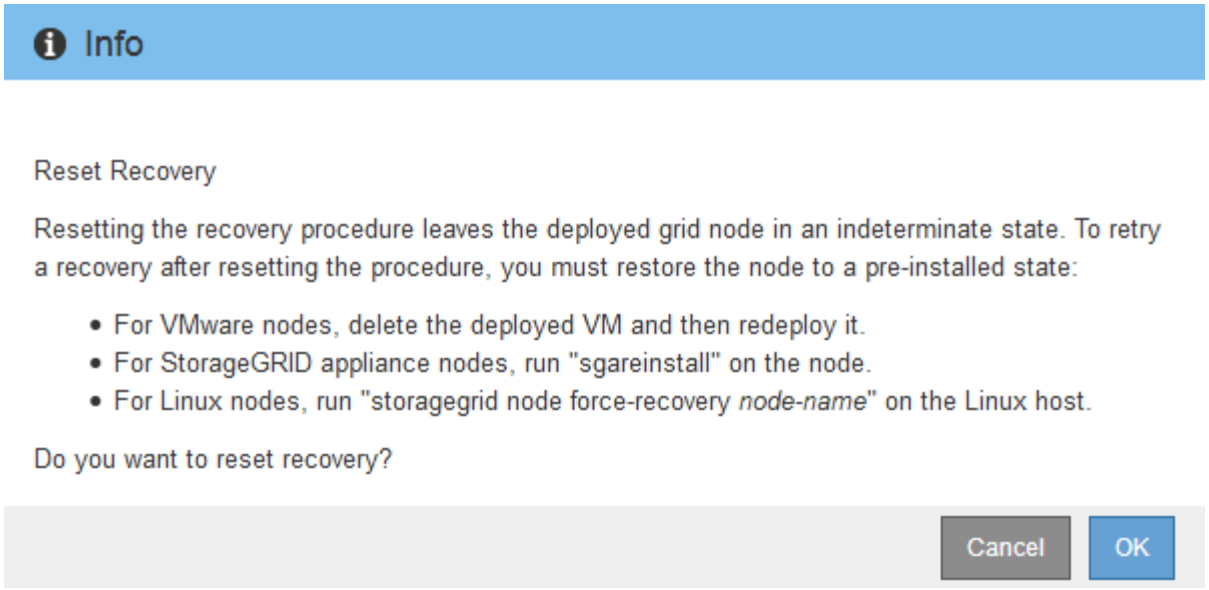


5. Supervise el progreso de la recuperación en la tabla recuperando Grid Node.

   Cuando el nodo de cuadrícula llegue a la fase «'esperando pasos manuales'», vaya al tema siguiente y realice los pasos manuales para volver a montar y formatear los volúmenes de almacenamiento de las cabinas.



> En cualquier momento durante la recuperación, puede hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparece un cuadro de diálogo Información, que indica que el nodo se quedará en 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.

Vuelva a montar y vuelva a formatear los volúmenes de almacenamiento del aparato ("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.

Lo que necesitará

- 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 ejecutarse `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 policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot 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 policy.

Do not continue to the next step if you believe that the data
remaining on this volume cannot 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 pudo montar porque el disco no estaba inicializado o el superbloque del disco estaba dañado. Cuando el script no puede montar un volumen de almacenamiento, le pregunta si desea ejecutar la comprobación de coherencia del sistema de archivos.
  - Si el volumen de almacenamiento está conectado a un nuevo disco, responda **N** al indicador. No es necesario comprobar el sistema de archivos en un nuevo disco.
  - 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 alguno de los volúmenes 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 no puede montarse un volumen de almacenamiento o tiene un formato incorrecto y 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 permanecen en un volumen de almacenamiento fallido no pueden reconstruirse desde cualquier otro lugar de la cuadrícula (por ejemplo, si la política de ILM utiliza una regla que sólo realiza 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:

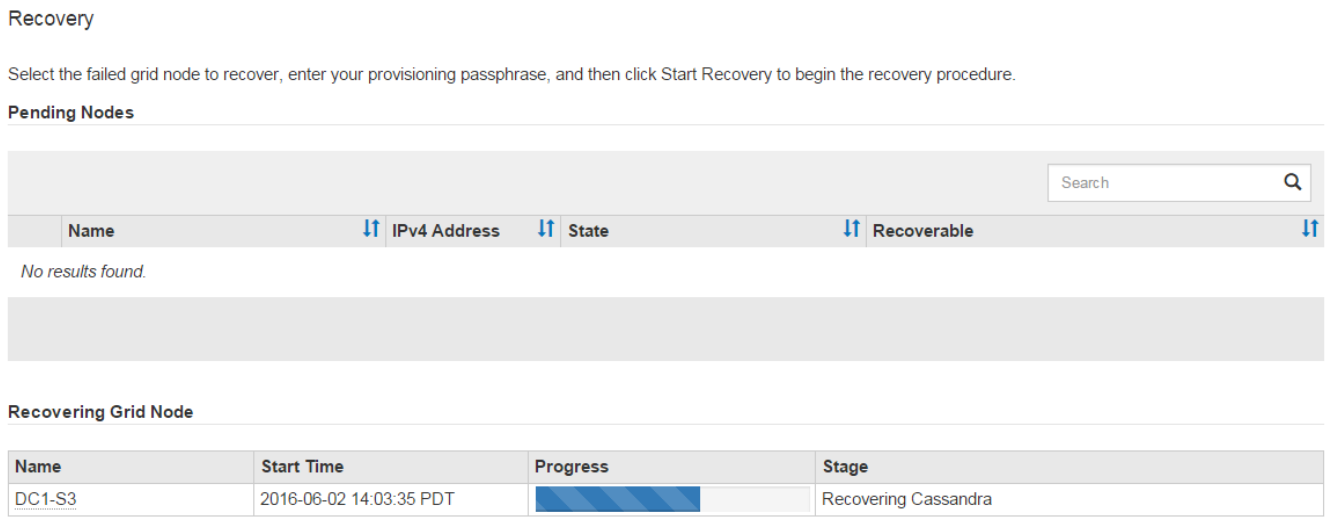
   - El script puede tardar horas en ejecutarse.
   - En general, debe dejar la sesión SSH sola mientras el script está en ejecución.
   - No pulse **Ctrl+C** mientras la sesión SSH está activa.
   - El script se ejecutará en segundo plano si se produce una interrupción de red y finaliza la sesión SSH, 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. Puede que note un resultado de script que menciona "relativamente" o ""reparación de Cassandra"". Si aparece 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.



Después del `sn-recovery-postinstall.sh` el script ha iniciado servicios en el nodo, puede restaurar datos de objeto en cualquier volumen de almacenamiento que haya formateado el script, tal y como se describe en el siguiente procedimiento.

Información relacionada

Revise las advertencias para la recuperación de la unidad del sistema del nodo de almacenamiento

Restaure datos de objetos al volumen de almacenamiento de dispositivo

Restaure datos de objetos al volumen de almacenamiento de dispositivo

Después de recuperar volúmenes de almacenamiento para el nodo de almacenamiento del dispositivo, puede restaurar los datos de objeto que se perdieron cuando falló el nodo de almacenamiento.

Lo que necesitará

- Debe haber confirmado que el nodo de almacenamiento recuperado tiene un estado de conexión de **conectado** 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.

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
```

> La `show-replicated-repair-status` Esta opción está disponible para la versión preliminar técnica de StorageGRID 11.6. Esta característica está en desarrollo y el valor devuelto puede ser incorrecto o retardado. Para determinar si una reparación está completa, utilice **esperando – todos**, **reparaciones intentadas (XRPA)** y **periodo de exploración — estimado (XSCM)** como se describe en Reparaciones del monitor.

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
```

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.

Puede realizar un seguimiento de las reparaciones de datos codificados de borrado con este comando:

```
repair-data show-ec-repair-status
```

> 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 se puede ejecutar `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 de 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, se activa la alerta **objetos perdidos** si el sistema StorageGRID no encuentra los datos del objeto 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 Supervisión y solución de problemas.

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 de 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. Es posible especificar un volumen, un rango de volúmenes o varios volúmenes que no están 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. 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, se activa la alerta **objetos perdidos** si el sistema StorageGRID no encuentra los datos del objeto 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 las instrucciones para supervisar y solucionar problemas de StorageGRID.

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. 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.

Datos replicados

- 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.

> Es posible que existan incoherencias de Cassandra y que no se realice 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 cumplan con su 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.
- Opcionalmente, para obtener un porcentaje estimado de finalización para la reparación replicada, agregue el `show-replicated-repair-status` opción del comando repair-data.

```
repair-data show-replicated-repair-status
```

> La `show-replicated-repair-status` Esta opción está disponible para la versión preliminar técnica de StorageGRID 11.6. Esta característica está en desarrollo y el valor devuelto puede ser incorrecto o retardado. Para determinar si una reparación está completa, utilice **esperando – todos**, **reparaciones intentadas (XRPA)** y **periodo de exploración — estimado (XSCM)** como se describe en Reparaciones del monitor.

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.

Lo que necesitará

- Debe iniciar 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 — corriente**.

El valor de ambos atributos debe ser en línea.

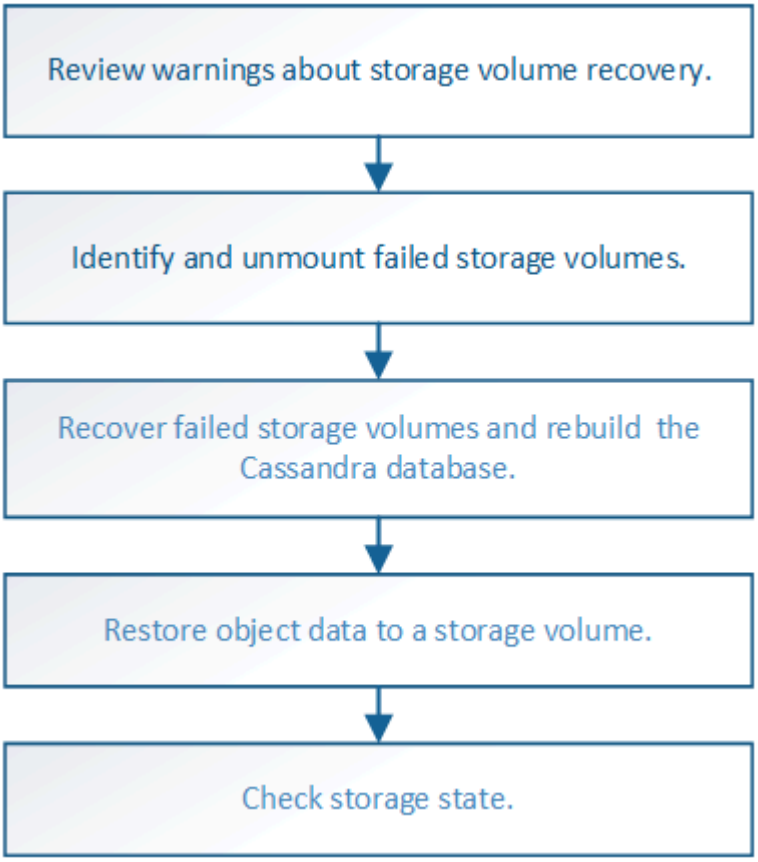
3. Si el estado de almacenamiento — deseado está establecido en sólo lectura, realice los siguientes pasos:
   a. Haga clic en la ficha **Configuración**.
   b. En la lista desplegable **Estado de almacenamiento — deseado**, seleccione **Online**.
   c. Haga clic en **aplicar cambios**.
   d. Haga clic 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

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.

Acerca de esta tarea

Este procedimiento de recuperación se aplica únicamente a los nodos de almacenamiento basados en software. Si los volúmenes de almacenamiento han fallado en un nodo de almacenamiento del dispositivo, utilice el procedimiento correspondiente a «'nodo de almacenamiento del dispositivo de recuperación».



Información relacionada

Recupere el nodo de almacenamiento del dispositivo

Revise las advertencias sobre la recuperación del volumen de almacenamiento

Antes de recuperar volúmenes de almacenamiento con fallos para un nodo de almacenamiento, debe revisar 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. Póngase en contacto con el soporte técnico.

Cómo realiza la recuperación del sitio el soporte técnico

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 de Servicios: Estado - Cassandra (SVST) durante la recuperación, consulte las instrucciones de supervisión y solución de problemas para recuperar la alarma reconstruyendo 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

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.

Lo que necesitará

Debe iniciar 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.

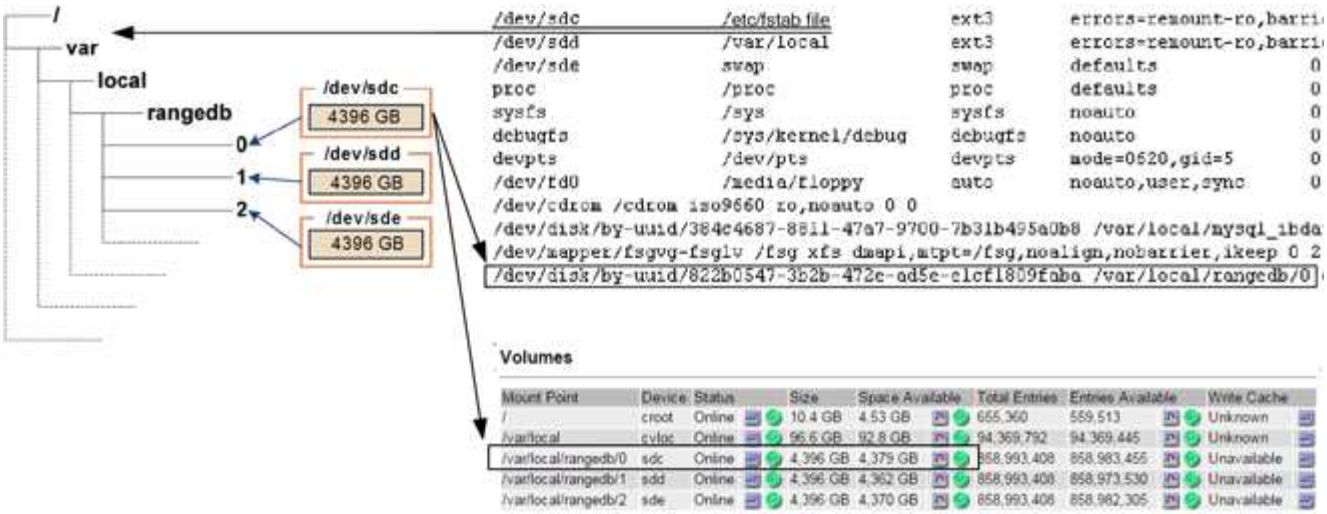
> Repare el hardware y conecte correctamente los discos antes de ejecutar el `reboot` comando.

> Identifique cuidadosamente los volúmenes de almacenamiento fallidos. Utilizará esta información para verificar qué volúmenes se deben reformatear. Una vez que un volumen se ha reformateado, 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. Seleccione **sitio nodo de almacenamiento fallido LDR almacenamiento Descripción general Principal** y busque 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 Failed Storage Node SSM Resources Overview Main**. 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 detener los servicios de almacenamiento y 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 los servicios de almacenamiento en el nodo de almacenamiento.

> Si los servicios de almacenamiento ya se han detenido, no se le solicitará. El servicio Cassandra se ha detenido solo para el volumen 0.

```
root@Storage-180:~ # sn-unmount-volume 0
Storage services (ldr, chunk, dds, cassandra) are not down.
Storage services must be stopped before running this script.
Stop storage services [y/N]? y
Shutting down storage services.
Storage services stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

En unos segundos, los servicios de almacenamiento se detienen y el volumen se desasocia. Aparecen mensajes que indican cada paso del proceso. El mensaje final indica que el volumen no está asociado.

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.

- Debe tener la `Passwords.txt` archivo.
- Las unidades del sistema del servidor deben estar intactas.
- Hay que identificar la causa del fallo y, en caso necesario, hay que adquirir hardware de almacenamiento de sustitución.
- El tamaño total del almacenamiento de reemplazo debe ser 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.

a. 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.

   Una vez que se sustituye el almacenamiento, asegúrese de volver a analizar o reiniciar para asegurarse de que el sistema operativo reconozca, pero no vuelva a montar los volúmenes. El almacenamiento se vuelve a montar y se añade a. `/etc/fstab` en un paso posterior.

b. Inicie sesión en el nodo de almacenamiento con errores:

   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 `#`.

c. 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.

d. 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`

   - Si los servicios de almacenamiento se están ejecutando, se le solicitará que los detenga. Introduzca: **Y**
   - 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. Puede que note un resultado de script que menciona "relativamente" o ""reparación de Cassandra"". Si aparece 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
Storage services must be stopped before running this script.
Stop storage services [y/N]? **y**
Shutting down storage services.
Storage services stopped.
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 c817f87f-f989-4a21-8f03-
b6f42180063f
Skipping in use device /dev/sdg
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12075630
Cassandra does not need rebuilding.
Starting services.

Reformatting done.  Now do manual steps to
restore copies of data.
```

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 está intacta, puede restaurar los datos de objetos que se perdieron cuando se produjo un error en el volumen de almacenamiento.

Lo que necesitará

- Debe haber confirmado que el nodo de almacenamiento recuperado tiene un estado de conexión de

conectado 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.

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
```

> La `show-replicated-repair-status` Esta opción está disponible para la versión preliminar técnica de StorageGRID 11.6. Esta característica está en desarrollo y el valor devuelto puede ser incorrecto o retardado. Para determinar si una reparación está completa, utilice **esperando – todos**, **reparaciones intentadas (XRPA)** y **periodo de exploración — estimado (XSCM)** como se describe en Reparaciones del monitor.

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
```

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.

Puede realizar un seguimiento de las reparaciones de datos codificados de borrado con este comando:

```
repair-data show-ec-repair-status
```

> 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 se puede ejecutar `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 de 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, se activa la alerta **objetos perdidos** si el sistema StorageGRID no encuentra los datos del objeto 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 Supervisión y solución de problemas.

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 de 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. Es posible especificar un volumen, un rango de volúmenes o varios volúmenes que no están 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. 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, se activa la alerta **objetos perdidos** si el sistema StorageGRID no encuentra los datos del objeto 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 las instrucciones para supervisar y solucionar problemas de StorageGRID.

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. 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.

Datos replicados

- 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.

> Es posible que existan incoherencias de Cassandra y que no se realice 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 cumplan con su 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.
- Opcionalmente, para obtener un porcentaje estimado de finalización para la reparación replicada, agregue el `show-replicated-repair-status` opción del comando repair-data.

```
repair-data show-replicated-repair-status
```

> La `show-replicated-repair-status` Esta opción está disponible para la versión preliminar técnica de StorageGRID 11.6. Esta característica está en desarrollo y el valor devuelto puede ser incorrecto o retardado. Para determinar si una reparación está completa, utilice **esperando – todos**, **reparaciones intentadas (XRPA)** y **periodo de exploración — estimado (XSCM)** como se describe en Reparaciones del monitor.

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.

Lo que necesitará

- Debe iniciar 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 — corriente**.

   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

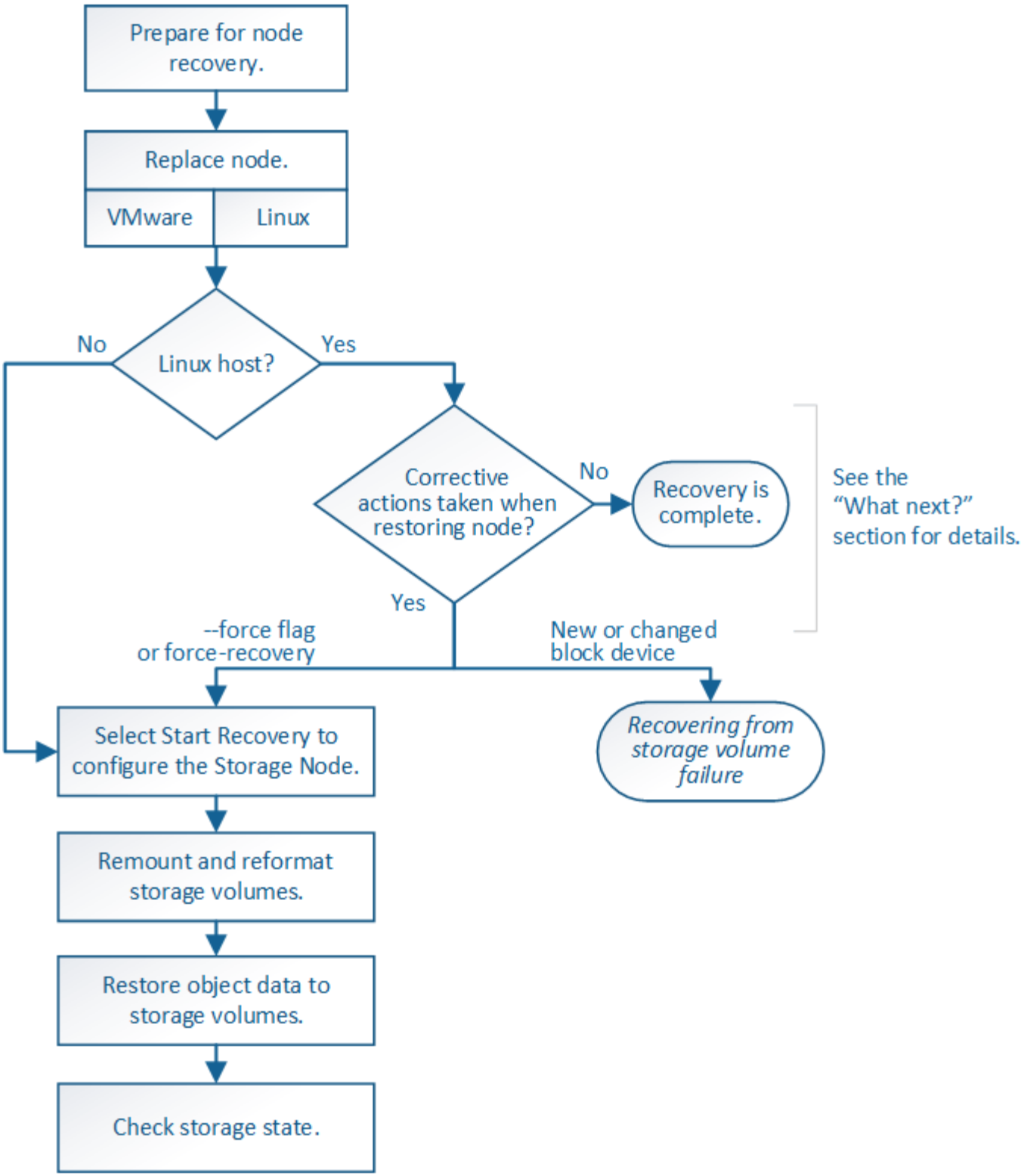
Si falló la unidad del sistema en un nodo de almacenamiento basado en software, el nodo de almacenamiento no está disponible para el sistema StorageGRID. Debe completar un conjunto específico de tareas para recuperar el sistema de un fallo de unidad.

Acerca de esta tarea

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 a seguir si alguno de los volúmenes de almacenamiento también presenta errores o no se puede volver a montar.

> Este procedimiento se aplica únicamente a nodos de almacenamiento basados en software. Debe seguir un procedimiento diferente para recuperar un nodo de almacenamiento del dispositivo.

Recupere el nodo de almacenamiento del dispositivo



Revise las advertencias para la recuperación de la unidad del sistema del nodo de almacenamiento

Antes de recuperar una unidad de sistema con errores de un nodo de almacenamiento, debe revisar las siguientes advertencias.

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. Póngase en contacto con el soporte técnico.

Cómo realiza la recuperación del sitio el soporte técnico

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 para la recuperación tras la pérdida de volúmenes de almacenamiento donde la unidad del sistema está 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 de Servicios: Estado - Cassandra (SVST) durante la recuperación, consulte las instrucciones de supervisión y solución de problemas para recuperar la alarma reconstruyendo 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

Supervisión y solución de problemas

Advertencias y consideraciones sobre los procesos de recuperación de nodos de grid

Recupérese de un fallo en el volumen de almacenamiento, donde la unidad del sistema está intacta

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 para recuperar un nodo de almacenamiento del dispositivo.

Recupere el nodo de almacenamiento del dispositivo

Linux: Si no está seguro de que su 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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener los permisos de mantenimiento o acceso raíz.
- Debe tener la clave de acceso de aprovisionamiento.
- Debe haber puesto en marcha y configurado el nodo de sustitución.
- Debe conocer la fecha de inicio de los trabajos de reparación para los datos codificados mediante borrado.
- Debe haber 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:

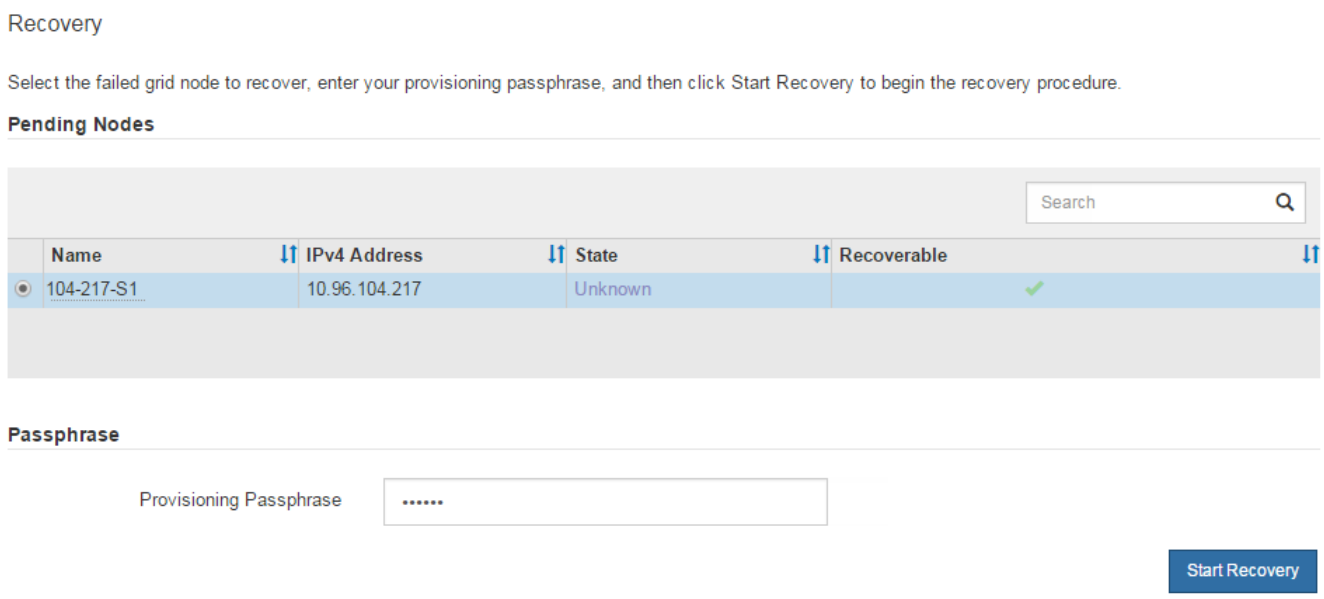
- Tenía que usar el `--force` indicador para importar el nodo o ha emitido `storagegrid node force-recovery` *`node-name`*
- Tenía que hacer una reinstalación de nodo completa o tenía que restaurar /var/local.

Pasos

1. En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **recuperación**.
2. Seleccione el nodo de cuadrícula que desea recuperar en la lista Pending Nodes.

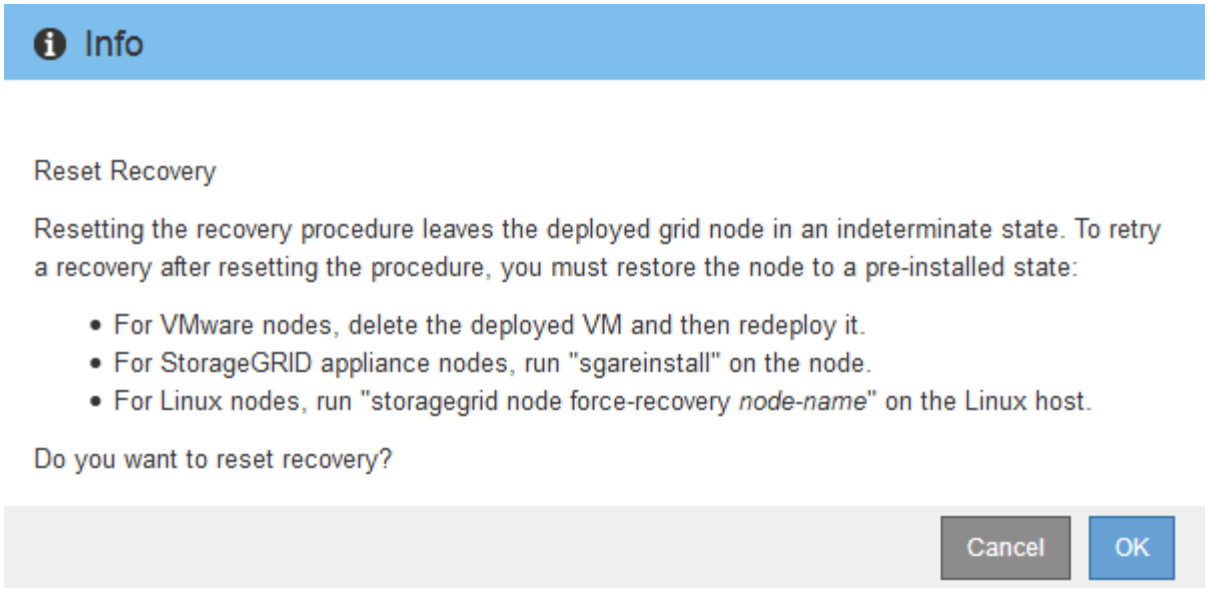
   Los nodos aparecen en la lista después de que fallan, pero no podrá seleccionar un nodo hasta que se haya vuelto a instalar y esté listo para la recuperación.

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.

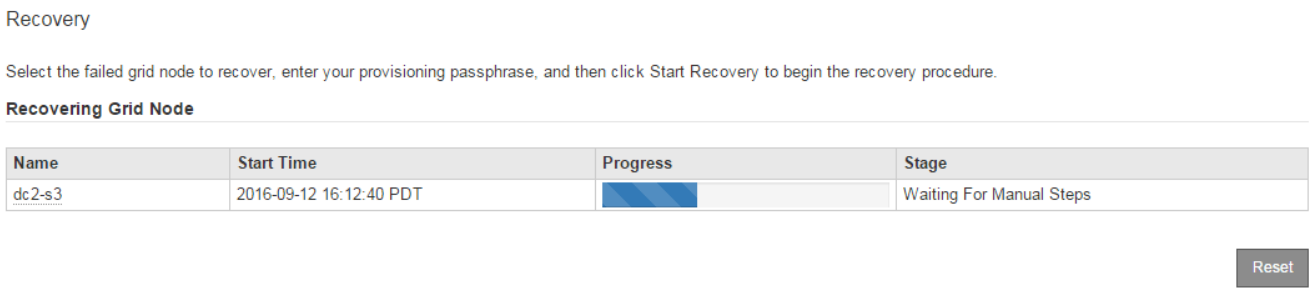
> Mientras se está ejecutando el procedimiento de recuperación, puede hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparece un cuadro de diálogo Información, que indica que el nodo se quedará en estado indeterminado si restablece el procedimiento.



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 llegue a la fase "'esperando pasos manuales'", vaya a la siguiente tarea del procedimiento de recuperación para volver a montar y formatear los volúmenes de almacenamiento.



Información relacionada

Preparar el aparato para su reinstalación (sólo sustitución de la plataforma)

Volver a montar y formatear 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.

Lo que necesitará

- 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 ejecutarse `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 policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot 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 policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot 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 pudo montar porque el disco no estaba inicializado o el superbloque del disco estaba dañado. Cuando el script no puede montar un volumen de almacenamiento, le pregunta si desea ejecutar la comprobación de coherencia del sistema de archivos.
  - Si el volumen de almacenamiento está conectado a un nuevo disco, responda **N** al indicador. No es necesario comprobar el sistema de archivos en un nuevo disco.
  - 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 alguno de los volúmenes 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 no puede montarse un volumen de almacenamiento o tiene un formato incorrecto y 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 permanecen en un volumen de almacenamiento fallido no pueden reconstruirse desde cualquier otro lugar de la cuadrícula (por ejemplo, si la política de ILM utiliza una regla que sólo realiza 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:

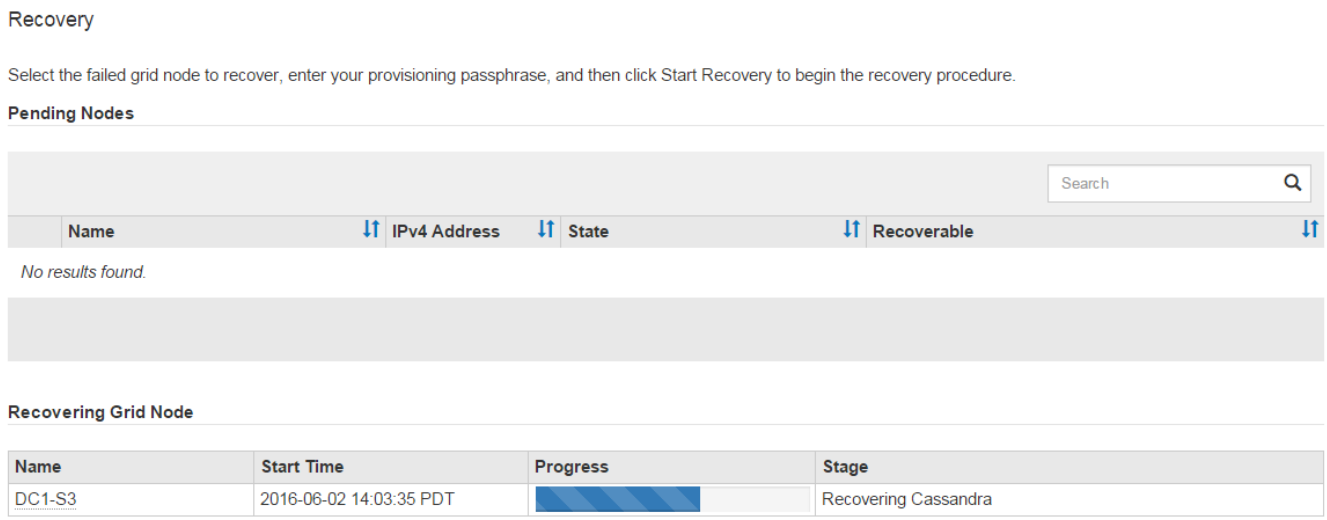
- El script puede tardar horas en ejecutarse.
- En general, debe dejar la sesión SSH sola mientras el script está en ejecución.
- No pulse **Ctrl+C** mientras la sesión SSH está activa.
- El script se ejecutará en segundo plano si se produce una interrupción de red y finaliza la sesión SSH, pero puede 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. Puede que note un resultado de script que menciona "relativamente" o ""reparación de Cassandra"". Si aparece 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.



Después del `sn-recovery-postinstall.sh` el script ha iniciado servicios en el nodo, puede restaurar datos de objeto en cualquier volumen de almacenamiento que tenga formato con el script, como se describe en ese procedimiento.

Información relacionada

Revise las advertencias para la recuperación de la unidad del sistema del nodo de almacenamiento

Restaure datos de objetos al volumen de almacenamiento, si es necesario

Restaure datos de objetos al volumen de almacenamiento, si es necesario

Si la `sn-recovery-postinstall.sh` Se necesita un script para volver a formatear uno o más volúmenes de almacenamiento con error, se deben restaurar los datos de objetos al volumen de almacenamiento con formato reformateado desde otros nodos de almacenamiento y nodos de archivado. Estos pasos no son necesarios a menos que se reformatee uno o más volúmenes de almacenamiento.

Lo que necesitará

- Debe haber confirmado que el nodo de almacenamiento recuperado tiene un estado de conexión de **conectado** 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.

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
```

> La `show-replicated-repair-status` Esta opción está disponible para la versión preliminar técnica de StorageGRID 11.6. Esta característica está en desarrollo y el valor devuelto puede ser incorrecto o retardado. Para determinar si una reparación está completa, utilice **esperando – todos**, **reparaciones intentadas (XRPA)** y **periodo de exploración — estimado (XSCM)** como se describe en Reparaciones del monitor.

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
```

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.

Puede realizar un seguimiento de las reparaciones de datos codificados de borrado con este comando:

```
repair-data show-ec-repair-status
```

> 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 se puede ejecutar `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 de 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, se activa la alerta **objetos perdidos** si el sistema StorageGRID no encuentra los datos del objeto 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 Supervisión y solución de problemas.

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 de 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. Es posible especificar un volumen, un rango de volúmenes o varios volúmenes que no están 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. 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, se activa la alerta **objetos perdidos** si el sistema StorageGRID no encuentra los datos del objeto 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 las instrucciones para supervisar y solucionar problemas de StorageGRID.

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. 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.

Datos replicados

- 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.

> Es posible que existan incoherencias de Cassandra y que no se realice 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 cumplan con su 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.
- Opcionalmente, para obtener un porcentaje estimado de finalización para la reparación replicada, agregue el `show-replicated-repair-status` opción del comando repair-data.

```
repair-data show-replicated-repair-status
```

> La `show-replicated-repair-status` Esta opción está disponible para la versión preliminar técnica de StorageGRID 11.6. Esta característica está en desarrollo y el valor devuelto puede ser incorrecto o retardado. Para determinar si una reparación está completa, utilice **esperando – todos**, **reparaciones intentadas (XRPA)** y **periodo de exploración — estimado (XSCM)** como se describe en Reparaciones del monitor.

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.

Lo que necesitará

- Debe iniciar 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 — corriente**.

El valor de ambos atributos debe ser en línea.

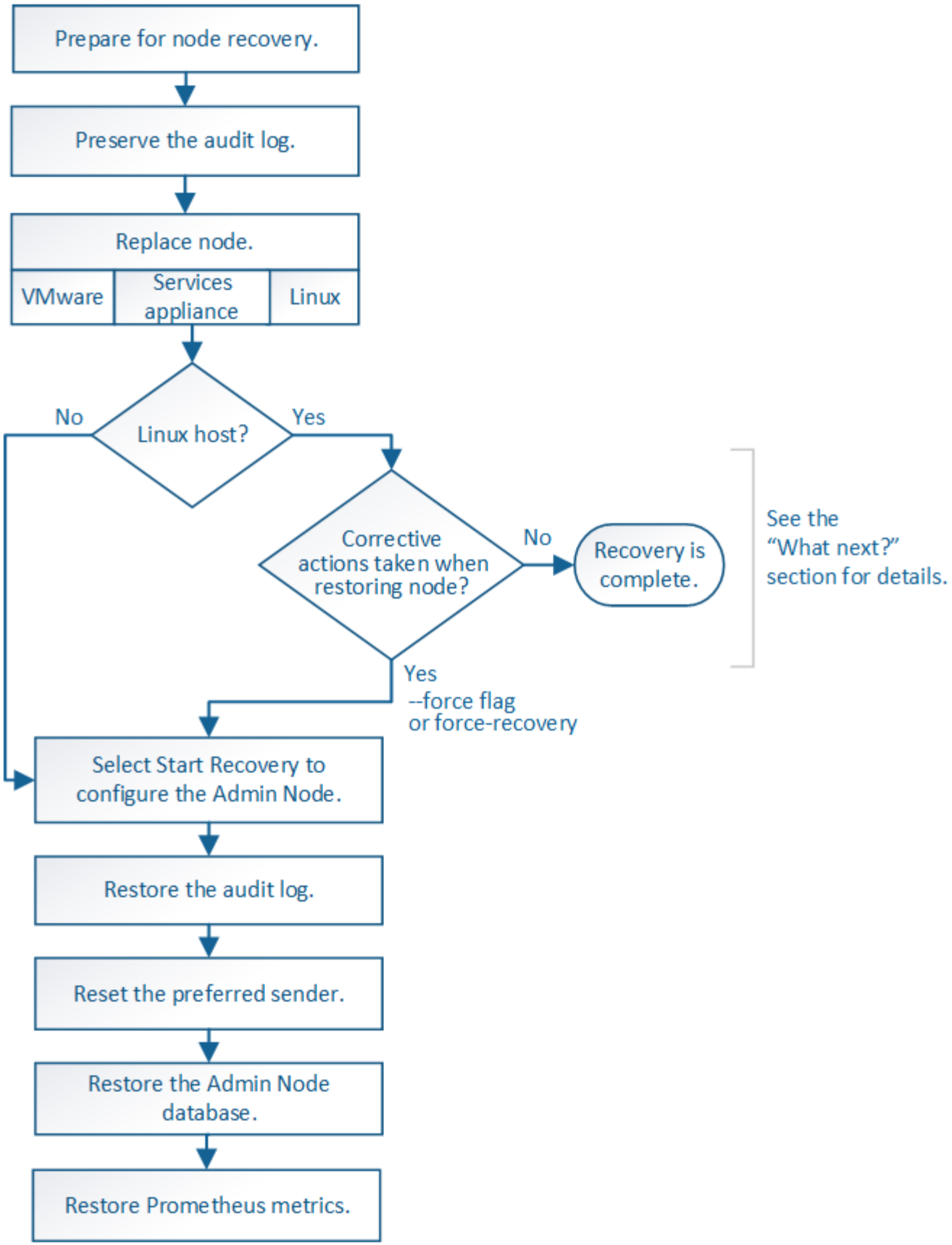
3. Si el estado de almacenamiento — deseado está establecido en sólo lectura, realice los siguientes pasos:
   a. Haga clic en la ficha **Configuración**.
   b. En la lista desplegable **Estado de almacenamiento — deseado**, seleccione **Online**.
   c. Haga clic en **aplicar cambios**.
   d. Haga clic 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 desde fallos de nodo de administrador

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.

Acerca de esta tarea

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.

Información relacionada

Servicios de aplicaciones SG100 y SG1000

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

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.

Acerca de esta tarea

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. Los objetos nuevos no se pueden procesar 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.

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 al 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 administrador con errores 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. Cambie el nombre del archivo audit.log para que no sobrescriba el archivo existente al copiarlo al nodo de administración recuperado.

   Cambie el nombre de audit.log por un nombre de archivo numerado único como aaaa-mm-dd.txt.1. Por ejemplo, puede cambiar el nombre del archivo audit.log a 2015-10-25.txt.1`cd /var/local/audit/export/`

4. Reinicie el servicio AMS: `service ams start`
5. 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.

6. Copie todos los archivos del registro de auditoría: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Cuando se lo pida, introduzca la contraseña de administrador.

7. 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

Plataforma de sustitución	Procedimiento
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.

Lo que necesitará

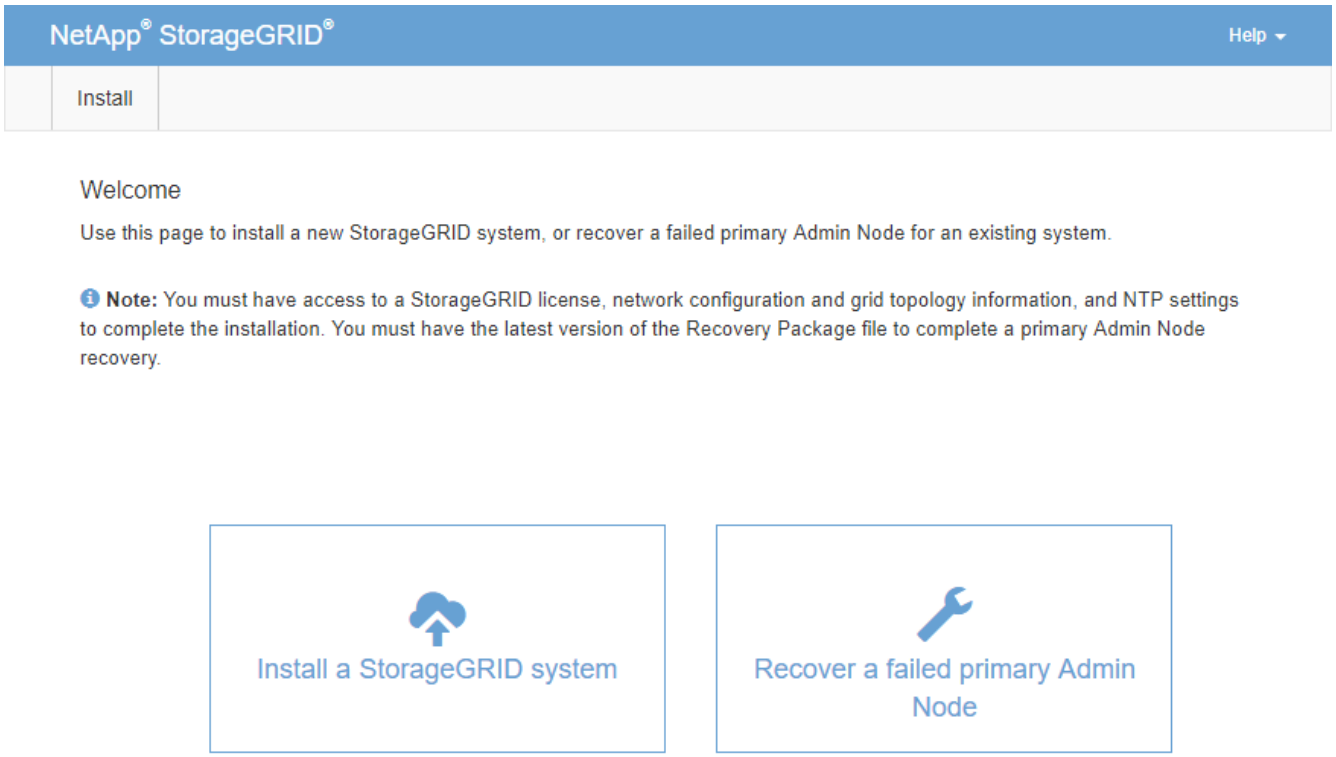
- Para los nodos de administración principales alojados en máquinas virtuales, la máquina virtual debe ponerse en marcha, encenderse e inicializarse.
- En el caso de los nodos de administrador principales alojados en un dispositivo de servicios, ha sustituido el dispositivo y ha instalado software. Consulte la guía de instalación del aparato.

  Servicios de aplicaciones SG100 y SG1000

- Debe tener el último backup del archivo de paquete de recuperación (`sgws-recovery-package-`*`id-revision`*`.zip`).
- Debe tener 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 la confianza de una parte de confianza, consulte las instrucciones para administrar StorageGRID. 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. Seleccione **NODES**.

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 mostradas en los campos **Versión de software** son las mismas, no es necesario aplicar una revisión.
- Si las versiones que aparecen en los campos **Versión de software** son diferentes, debe aplicar una revisión para actualizar el nodo de administración principal recuperado a la misma versión.

Información relacionada

Administre StorageGRID

Procedimiento de revisión de StorageGRID

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.

- El nodo de administrador recuperado debe estar instalado y en ejecución.
- Debe haber copiado los registros de auditoría en otra ubicación una vez que se produjo un error en el nodo de administración original.

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 administrador y el registro de auditoría no se puede copiar desde el nodo con errores, el nodo de administrador recuperado inicia el registro de eventos en el registro de auditoría como si la instalación es 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/audit/export`

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 las instrucciones para administrar StorageGRID.

Información relacionada

Administre StorageGRID

Restablecer el remitente preferido en el nodo de administración principal recuperado

Si el nodo de administrador principal que se está recuperando está establecido actualmente como remitente preferido de notificaciones de alerta, notificaciones de alarma y mensajes de AutoSupport, debe volver a configurar este valor.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener permisos de acceso específicos.
- El nodo de administrador recuperado debe estar instalado y en ejecución.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de pantalla**.
2. Seleccione el nodo de administración recuperado de la lista desplegable **remitente preferido**.
3. Haga clic en **aplicar cambios**.

Información relacionada

Administre StorageGRID

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.

- El nodo de administrador recuperado debe estar instalado y en ejecución.
- El sistema StorageGRID debe incluir al menos dos nodos de administración.
- Debe tener la `Passwords.txt` archivo.
- Debe tener la clave de acceso de aprovisionamiento.

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 históricos de atributos, que se utilizan en los gráficos e informes de texto disponibles en la página **SUPPORT Tools Grid topolog a**.

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 solo tiene un nodo de administrador 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.

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.

- El nodo de administrador recuperado debe estar instalado y en ejecución.
- El sistema StorageGRID debe incluir al menos dos nodos de administración.
- Debe tener la `Passwords.txt` archivo.
- Debe tener la clave de acceso de aprovisionamiento.

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 su 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.

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

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.

Información relacionada

Servicios de aplicaciones SG100 y SG1000

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 al 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 administrador con errores 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. Cambie el nombre del archivo audit.log para que no sobrescriba el archivo existente al copiarlo al nodo de administración recuperado.

   Cambie el nombre de audit.log por un nombre de archivo numerado único como aaaa-mm-dd.txt.1. Por ejemplo, puede cambiar el nombre del archivo audit.log a 2015-10-25.txt.1`cd /var/local/audit/export/`
4. Reinicie el servicio AMS: `service ams start`
5. 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.
6. Copie todos los archivos del registro de auditoría: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Cuando se lo pida, introduzca la contraseña de administrador.

7. 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.

Lo que necesitará

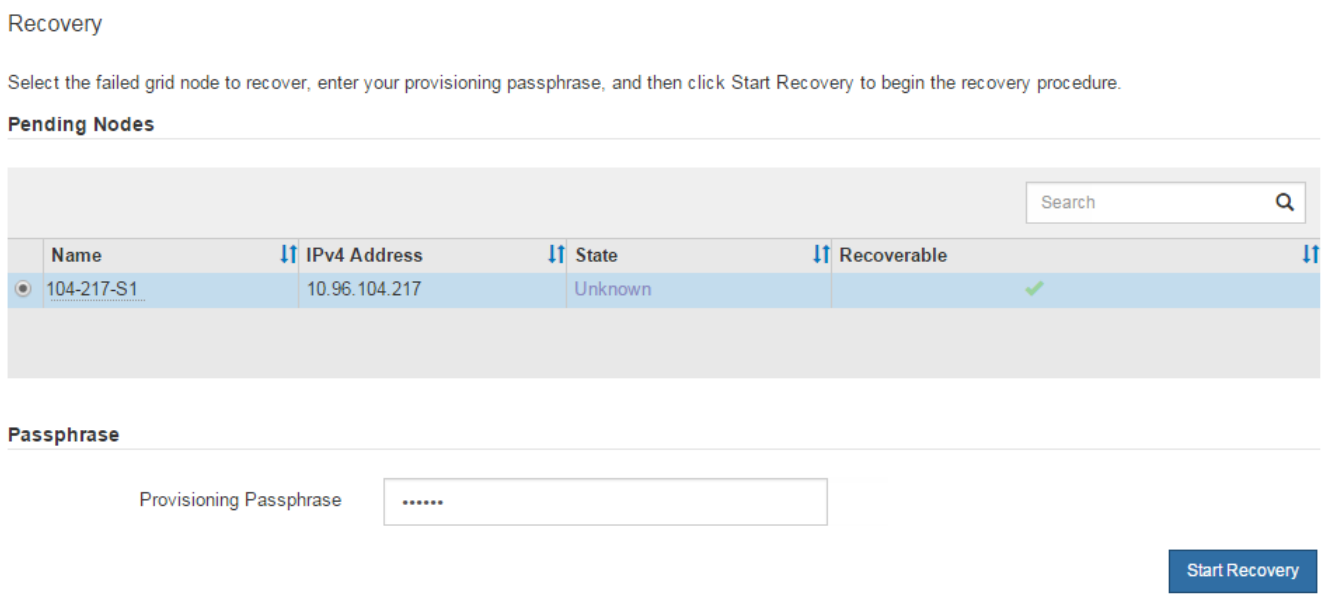
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener los permisos de mantenimiento o acceso raíz.
- Debe tener la clave de acceso de aprovisionamiento.
- Debe haber puesto en marcha y configurado el nodo de sustitución.

Pasos

1. En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **recuperación**.
2. Seleccione el nodo de cuadrícula que desea recuperar en la lista Pending Nodes.

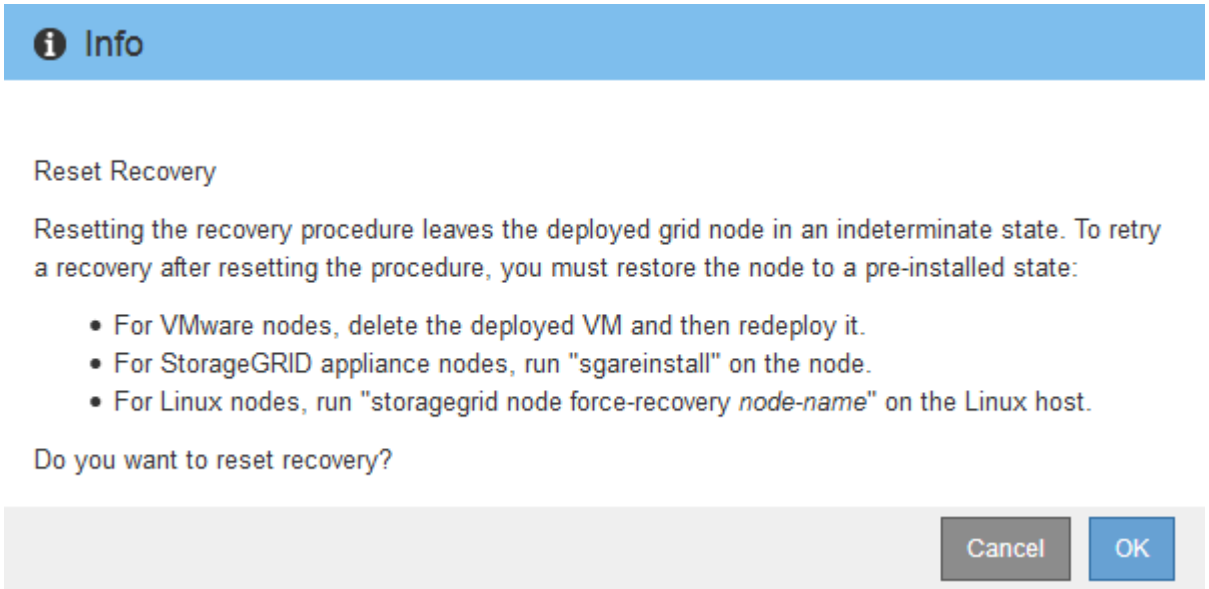
Los nodos aparecen en la lista después de que fallan, pero no podrá seleccionar un nodo hasta que se haya vuelto a instalar y esté listo para la recuperación.

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 Información, que indica que el nodo se quedará en 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.

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 la confianza de una parte de confianza, consulte las instrucciones para administrar StorageGRID. 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.

Información relacionada

Administre StorageGRID

Preparar el aparato para su reinstalación (sólo sustitución de la plataforma)

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.

- El nodo de administrador recuperado debe estar instalado y en ejecución.
- Debe haber copiado los registros de auditoría en otra ubicación una vez que se produjo un error en el nodo de administración original.

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 administrador y el registro de auditoría no se puede copiar desde el nodo con errores, el nodo de administrador recuperado inicia el registro de eventos en el registro de auditoría como si la instalación es 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/audit/export
   ```

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 las instrucciones para administrar StorageGRID.

Información relacionada

Administre StorageGRID

Restablecer el remitente preferido en el nodo de administración no primario recuperado

Si el nodo de administrador que no es principal que se está recuperando está

establecido actualmente como remitente preferido de notificaciones de alerta, notificaciones de alarma y mensajes de AutoSupport, debe volver a configurar este ajuste en el sistema StorageGRID.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener permisos de acceso específicos.
- El nodo de administrador recuperado debe estar instalado y en ejecución.

Pasos

1. Seleccione **CONFIGURACIÓN** > **sistema** > **Opciones de pantalla**.
2. Seleccione el nodo de administración recuperado de la lista desplegable **remitente preferido**.
3. Haga clic en **aplicar cambios**.

Información relacionada

Administre StorageGRID

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.

- El nodo de administrador recuperado debe estar instalado y en ejecución.
- El sistema StorageGRID debe incluir al menos dos nodos de administración.
- Debe tener la `Passwords.txt` archivo.
- Debe tener la clave de acceso de aprovisionamiento.

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 históricos de atributos, que se utilizan en los gráficos e informes de texto disponibles en la página **SUPPORT Tools Grid topolog a**.

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.

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.

- El nodo de administrador recuperado debe estar instalado y en ejecución.
- El sistema StorageGRID debe incluir al menos dos nodos de administración.
- Debe tener la `Passwords.txt` archivo.

- Debe tener la clave de acceso de aprovisionamiento.

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.

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

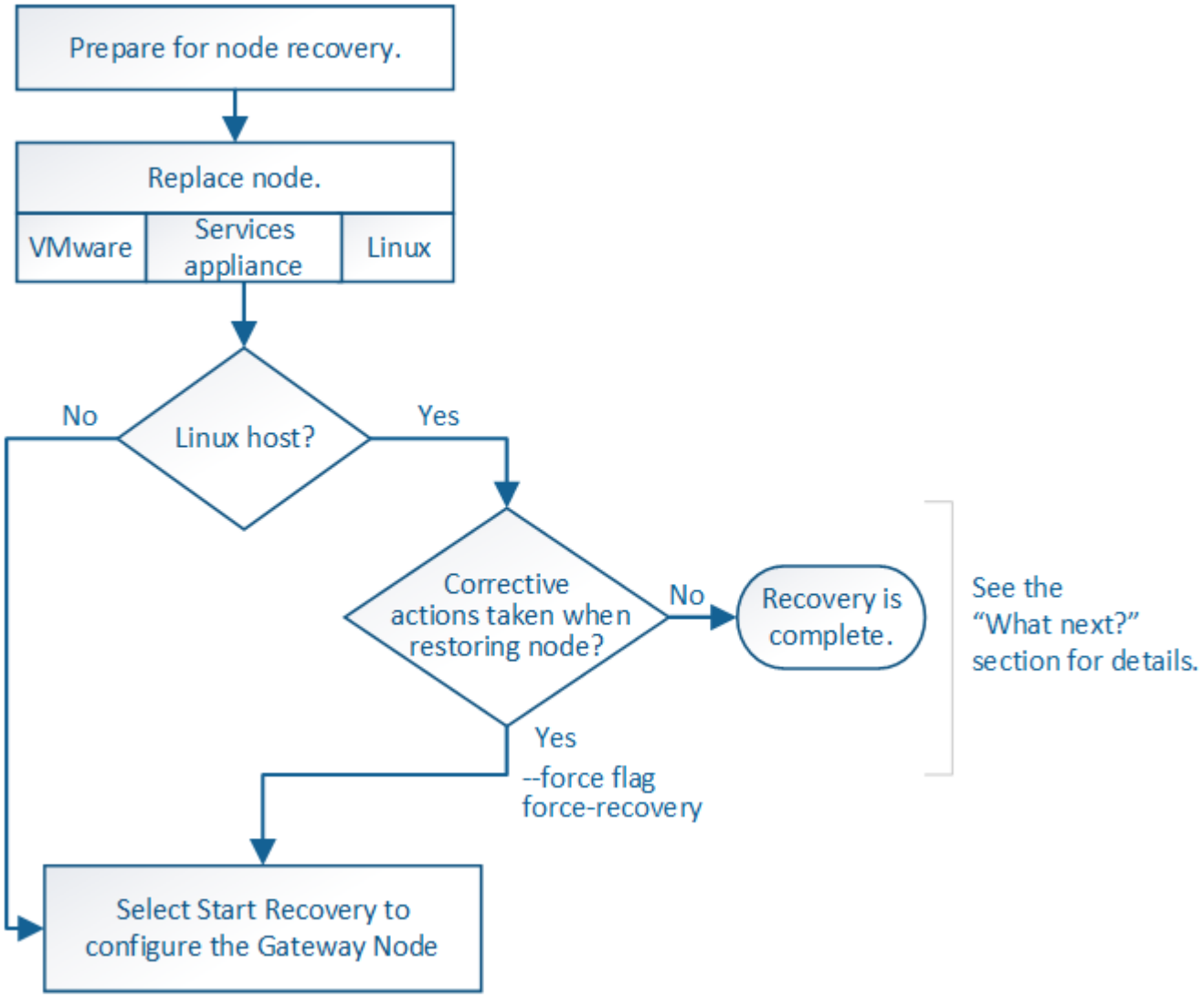
   a. Cuando ya no necesite un acceso sin contraseñas a otros servidores, quite la clave privada del agente

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

Debe completar una secuencia de tareas para poder recuperarlas de un fallo en el nodo de puerta de enlace.



Información relacionada

Servicios de aplicaciones SG100 y SG1000

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.

Lo que necesitará

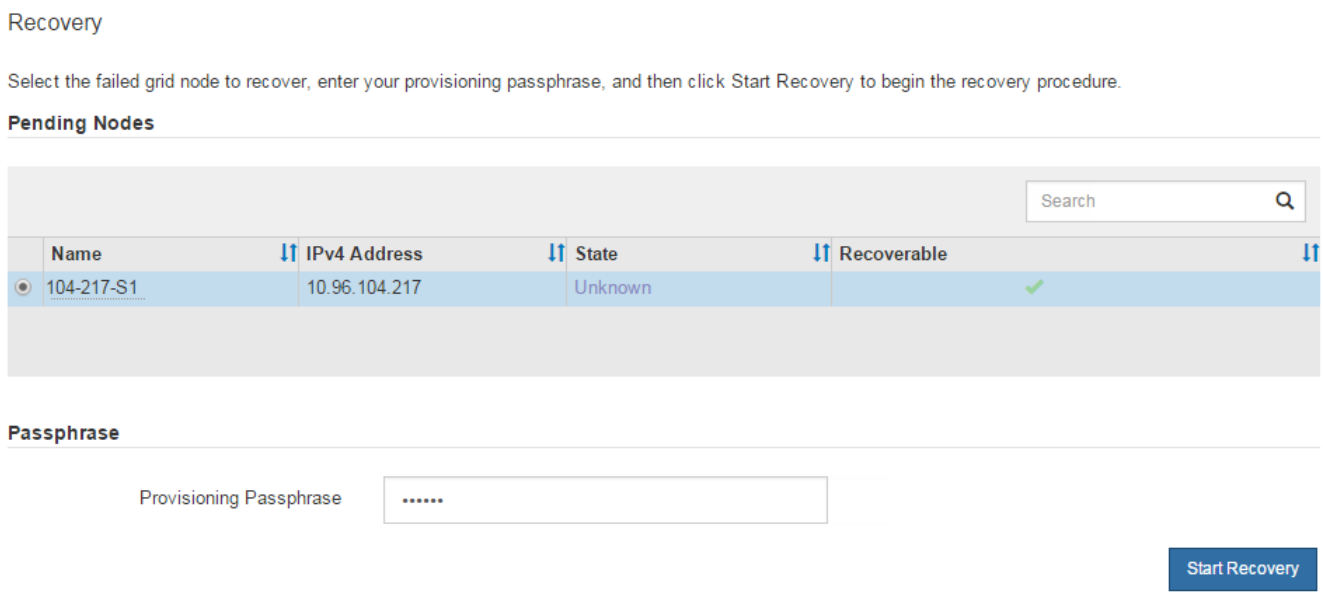
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener los permisos de mantenimiento o acceso raíz.
- Debe tener la clave de acceso de aprovisionamiento.
- Debe haber puesto en marcha y configurado el nodo de sustitución.

Pasos

1. En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **recuperación**.
2. Seleccione el nodo de cuadrícula que desea recuperar en la lista Pending Nodes.

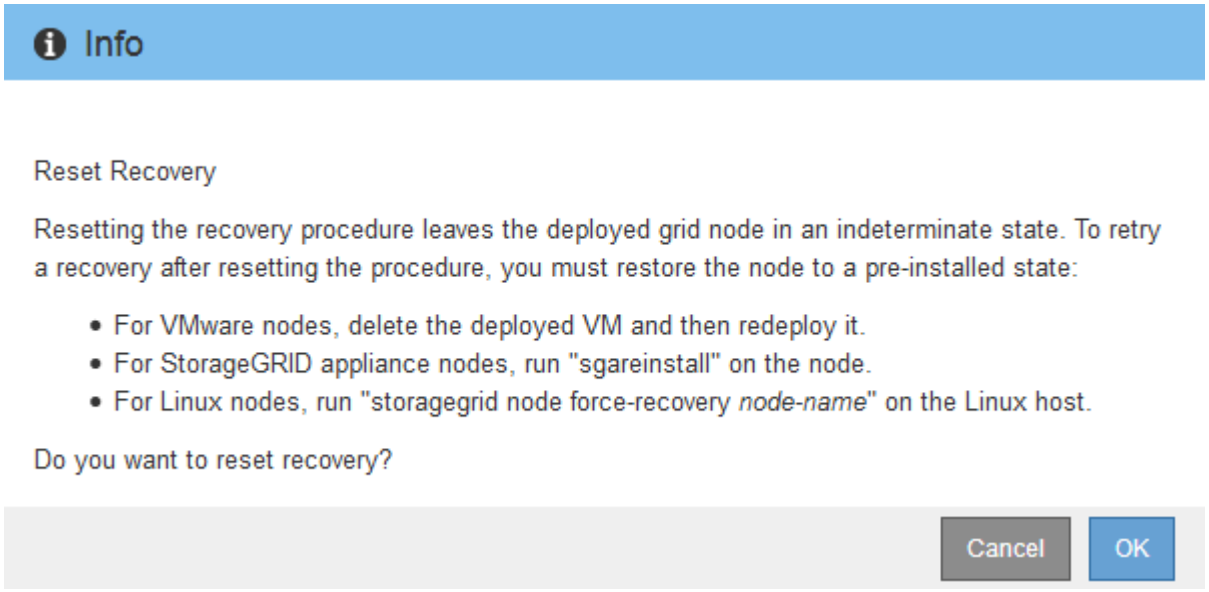
   Los nodos aparecen en la lista después de que fallan, pero no podrá seleccionar un nodo hasta que se haya vuelto a instalar y esté listo para la recuperación.

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 Información, que indica que el nodo se quedará en 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:

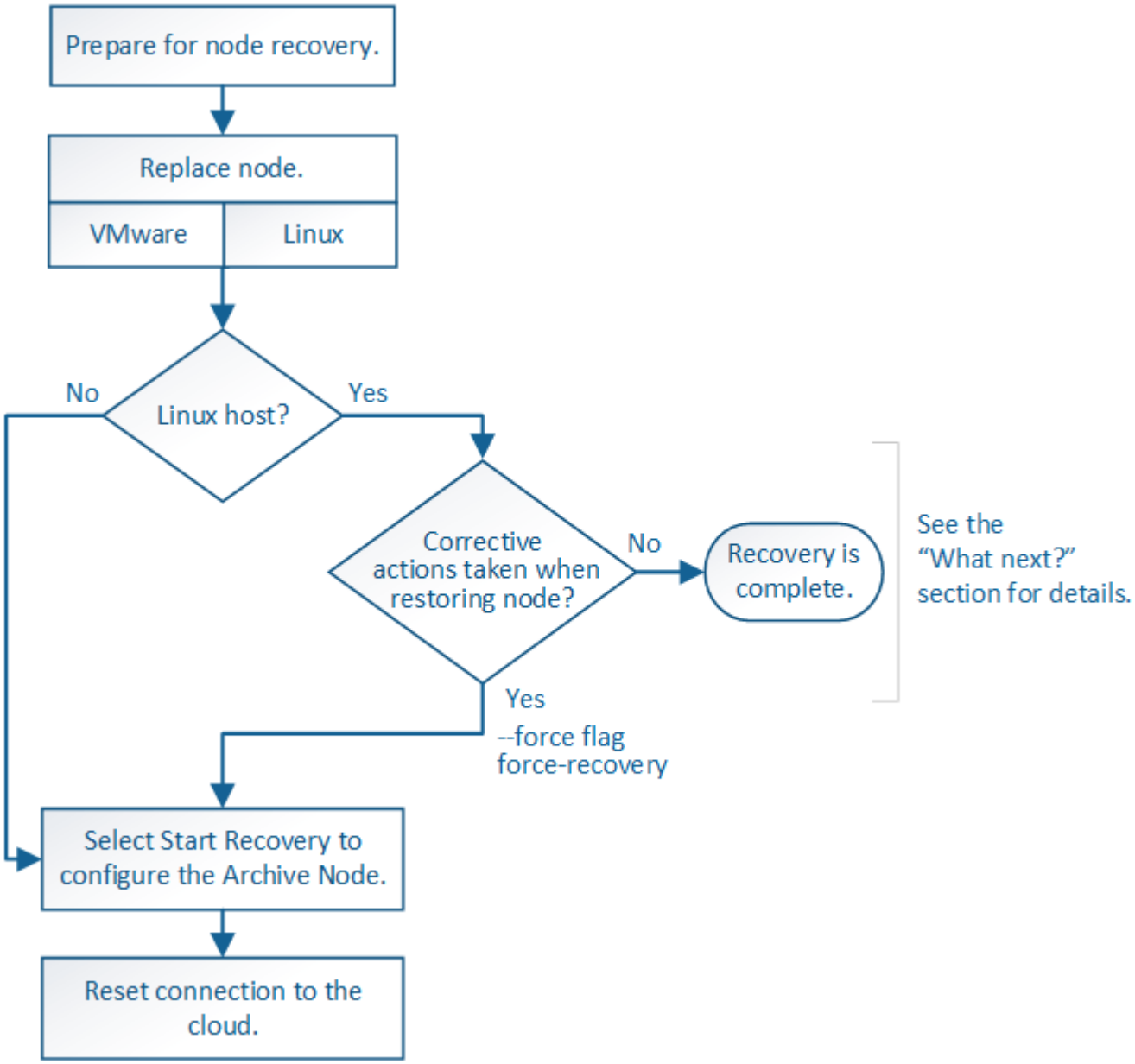
- **VMware**: Elimine el nodo de la cuadrícula virtual desplegada. A continuación, una vez que esté listo para reiniciar la recuperación, vuelva a poner el nodo en marcha.
- **Linux**: Reinicie el nodo ejecutando este comando en el host Linux: `storagegrid node force-recovery node-name`
- **Dispositivo**: 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.

Información relacionada

Preparar el aparato para su reinstalación (sólo sustitución de la plataforma)

Recupere desde errores de nodo de archivado

Debe completar una secuencia de tareas para poder recuperarlas de un fallo en el nodo de archivado.



Acerca de esta tarea

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, todos estos objetos se pierden; sin embargo, deberá seguir realizando procedimientos de recuperación para «'limpiar» su sistema StorageGRID y purgar 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.

Lo que necesitará

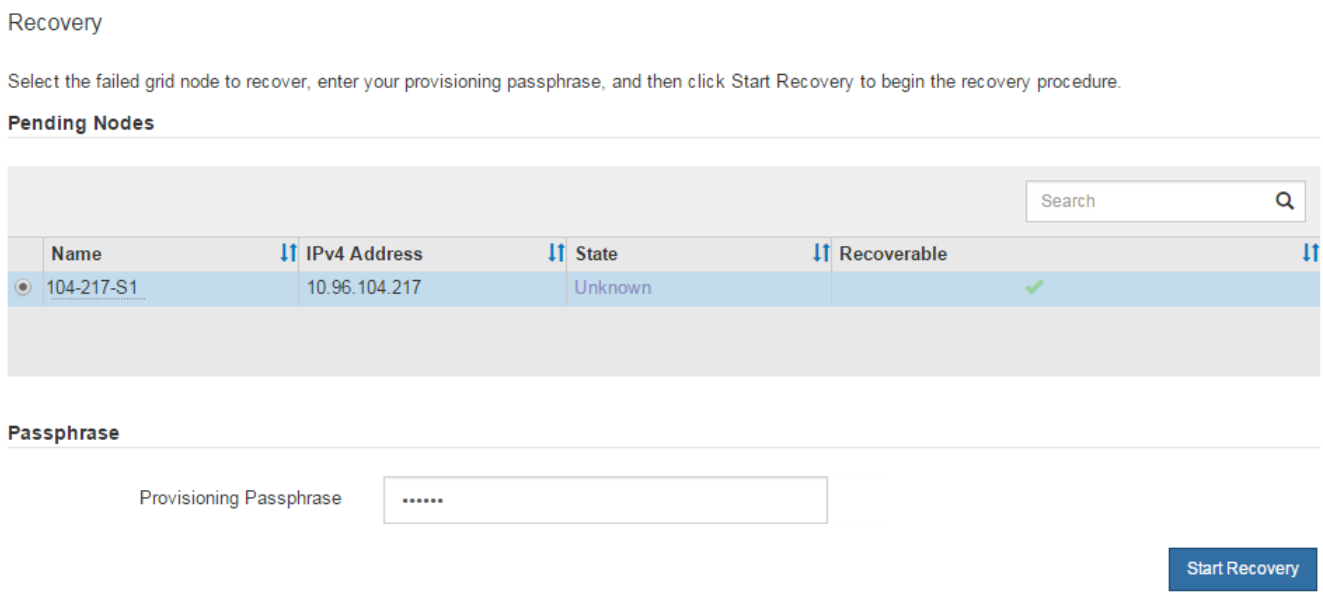
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener los permisos de mantenimiento o acceso raíz.
- Debe tener la clave de acceso de aprovisionamiento.
- Debe haber puesto en marcha y configurado el nodo de sustitución.

Pasos

1. En Grid Manager, seleccione **MANTENIMIENTO** > **tareas** > **recuperación**.
2. Seleccione el nodo de cuadrícula que desea recuperar en la lista Pending Nodes.

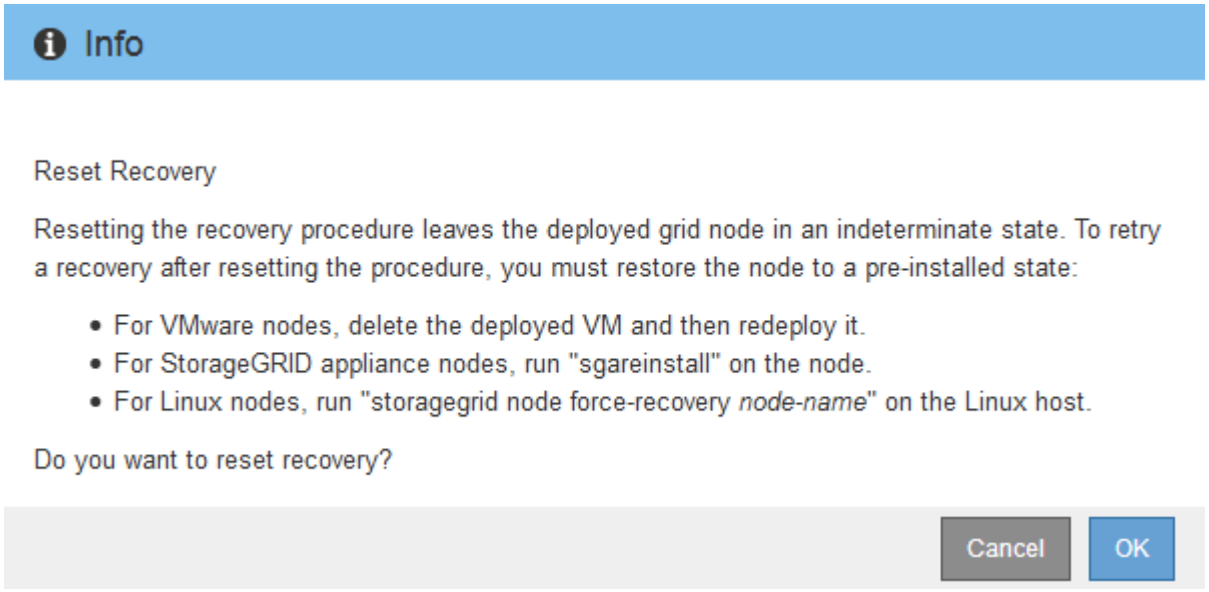
   Los nodos aparecen en la lista después de que fallan, pero no podrá seleccionar un nodo hasta que se haya vuelto a instalar y esté listo para la recuperación.

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 Información, que indica que el nodo se quedará en 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 a almacenamiento externo a través del middleware TSM, el nodo se restablece automáticamente y no necesita reconfigurar.

Lo que necesitará

Debe iniciar 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**.

Todos los tipos de nodos de grid: Sustituya el nodo VMware

Cuando recupera un nodo StorageGRID con errores que ha estado alojado en VMware, debe quitar el nodo con errores y poner en marcha un nodo de recuperación.

Lo que necesitará

Debe haber determinado que la máquina virtual no se puede restaurar y se debe reemplazar.

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.

   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.

   Para obtener instrucciones:

   Instale VMware Poner en marcha un nodo de StorageGRID como máquina virtual

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

Todos los tipos de nodos de grid: Sustituya el nodo Linux

Si un fallo requiere que se ponga en marcha uno o varios hosts físicos o virtuales nuevos o se vuelva a instalar Linux en un host existente, debe implementar y configurar el host de reemplazo para 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®, CentOS o Debian®. Utilice la herramienta matriz de interoperabilidad de NetApp para obtener una lista de las versiones compatibles.

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.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

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 del sistema operativo Linux.

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.

> Pare después de completar la tarea "'instalar el servicio de host de StorageGRID'" en las instrucciones de instalación. No inicie la tarea "D ebolling grid Nodes".

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 dar soporte a los nodos StorageGRID o ha movido algunas o todas las unidades de disco o SSD de los nodos de error a los de sustitución, debe restablecer las mismas asignaciones de almacenamiento que existían 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 desde un sistema ONTAP de NetApp, confirme que el volumen no tiene habilitada la 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.

Información relacionada

Instale Red Hat Enterprise Linux o CentOS

Instalar Ubuntu o Debian

Restaurar los nodos de grid en el host

Para restaurar un nodo de grid con errores en un nuevo host Linux, puede restaurar el archivo de configuración del nodo con los comandos correspondientes.

Cuando se realiza una instalación nueva, se crea un archivo de configuración de nodos para cada nodo de

grid que se instala 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.

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.

Pasos

- Restaurar y validar nodos de grid
- Inicie el servicio de host StorageGRID
- Recupere los nodos que no se inician normalmente

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 los archivos de configuración de grid.

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 de `/var/local` volumen para un nodo.

Pasos

1. En la línea de comandos del host recuperado, se enumeran todos los nodos de grid 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 no aparecen algunos o todos los nodos de grid que deben configurarse en el host, debe restaurar los nodos de grid 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` volumen, vuelva a crear el archivo de configuración del nodo para restaurarlo al host.

   Siga las instrucciones de la sección ""Crear archivos de configuración de nodos"" en las instrucciones de instalación.

   > 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 vaya a volver a crear el archivo de configuración de un nodo, asegúrese de seguir todas 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.

Información relacionada

Instale Red Hat Enterprise Linux o CentOS

Instalar Ubuntu o Debian

Corrija los errores de interfaz de red que faltan

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` para el nodo *node-name*…'
`ERROR: *node-name*: GRID_NETWORK_TARGET = *host-interface-name*' *Node-name*: La interfaz '*host-interface-name*' no existe'

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* no existe'

Significa eso `/etc/storagegrid/nodes/node-name.conf` Asigna el dispositivo de bloque utilizado por *node-name* CON EL PROPÓSITO del nombre de ruta de acceso dado 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.

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 del tamaño y categoría de almacenamiento adecuados y editar el archivo de configuración del nodo para cambiar el valor de BLOCK_DEVICE_PURPOSE para que apunte al nuevo archivo especial del dispositivo de bloque.

Determine el tamaño y la categoría de almacenamiento adecuados de las tablas de la sección «requisitos de almacenamiento» de las instrucciones de instalación del sistema operativo Linux. Revise las recomendaciones que se indican en «"Configuración del almacenamiento host"» antes de proceder con la sustitución del dispositivo de bloque.

> 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.

PRECAUCIÓN:

Ejecute el siguiente comando solo para nuevos dispositivos de almacenamiento en bloques. No ejecute este comando si cree que el almacenamiento en bloque sigue contiene datos válidos para el nodo que se va a recuperar, ya que se perderán todos los datos del dispositivo.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

Información relacionada

Instale Red Hat Enterprise Linux o CentOS

Instalar Ubuntu o Debian

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.

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`

   Para los nodos que devuelven el estado sin ejecución o detenido, ejecute el siguiente comando:

   `sudo storagegrid node start node-name`

3. 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 vuelve a unirse a la cuadrícula con normalidad y no se muestra como recuperable, puede dañarse. Puede forzar el nodo en el modo de recuperación.

Para forzar el nodo en el modo de recuperación:

`sudo storagegrid node force-recovery node-name`

> Antes de emitir este comando, confirme que la configuración de red del nodo es correcta; es posible que no haya podido volver a unirse a la cuadrícula debido a asignaciones de interfaz de red incorrectas o a una dirección IP o puerta de enlace de red de red incorrecta.

> Después de emitir el `storagegrid node force-recovery node-name` debe realizar pasos de recuperación adicionales para *node-name*.

Información relacionada

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 un nodo, es posible que haya que realizar una de estas 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 con fallos por el dispositivo de servicios

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.

Lo que necesitará

- Debe haber 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.
- Debe asegurarse de que la versión de instalador de dispositivos de StorageGRID en el dispositivo de servicios coincida con la versión de software del sistema StorageGRID, como se describe en instalación y mantenimiento de hardware para verificar y actualizar la versión de instalador de dispositivos de StorageGRID.

  Servicios de aplicaciones SG100 y SG1000

> No instale un SG100 ni un dispositivo de servicio 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 que ha fallado se hospedó en VMware o Linux (cambio de plataforma).
- El nodo con errores se hospedó en un dispositivo de servicios (reemplazo de plataforma)

Instalar el dispositivo de servicios (sólo cambio de plataforma)

Cuando recupere un nodo de red fallido alojado en VMware o un host Linux y utilice un dispositivo de servicios SG100 o SG1000 para el nodo de sustitución, primero debe instalar el hardware de la nueva aplicación con el mismo nombre de nodo que el nodo fallido.

Debe tener 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.
- **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.

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.

1. Siga las instrucciones para instalar un nuevo dispositivo de servicios SG100 o SG1000.
2. Cuando se le solicite el nombre de un nodo, utilice el nombre del nodo con errores.

Información relacionada

Servicios de aplicaciones SG100 y SG1000

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 estuvo alojado originalmente en un host VMware o Linux.

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.

Lo que necesitará

- El dispositivo debe estar instalado en un rack, conectado a las redes y encendido.
- Los enlaces de red y las direcciones IP deben configurarse 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 cuadrícula que aparecen en la página Configuración de IP del instalador de dispositivos StorageGRID deben estar definidas en la lista de subredes de red de cuadrícula del nodo de administración principal.

Para obtener instrucciones sobre cómo completar estas tareas de requisitos previos, consulte las instrucciones de instalación y mantenimiento de un dispositivo de servicios SG100 o SG1000.

- Debe usar un navegador web compatible.
- Debe conocer 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 precargada del software coincide con la versión que se está utilizando 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:

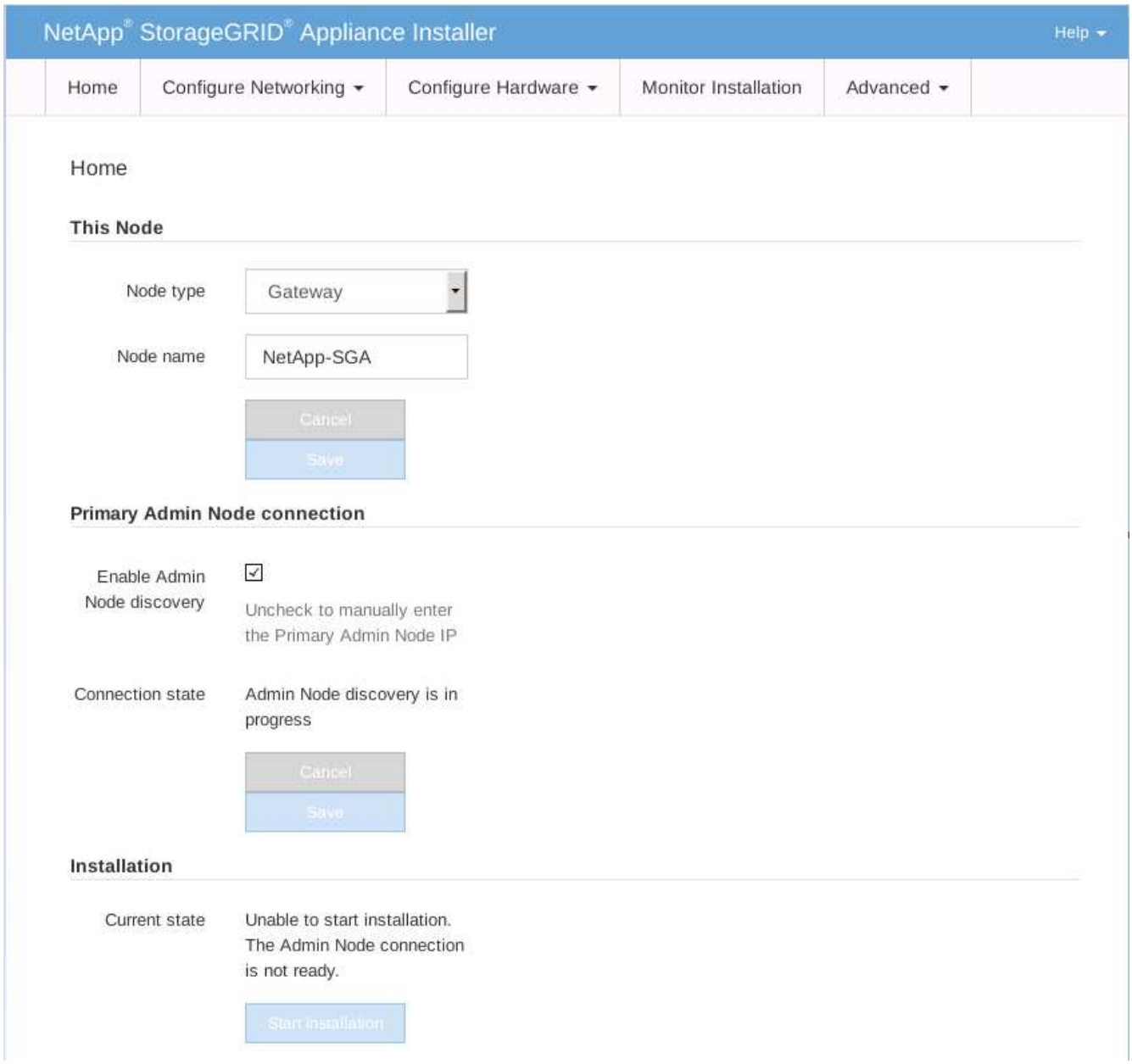
- Para un nodo de administración principal, debe especificar el nombre del nodo y luego cargar los paquetes de software adecuados (si es necesario).
- En el caso de un nodo de administrador que no sea primario o un nodo de puerta de enlace, debe especificar o confirmar la dirección IP del nodo de administración 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**.

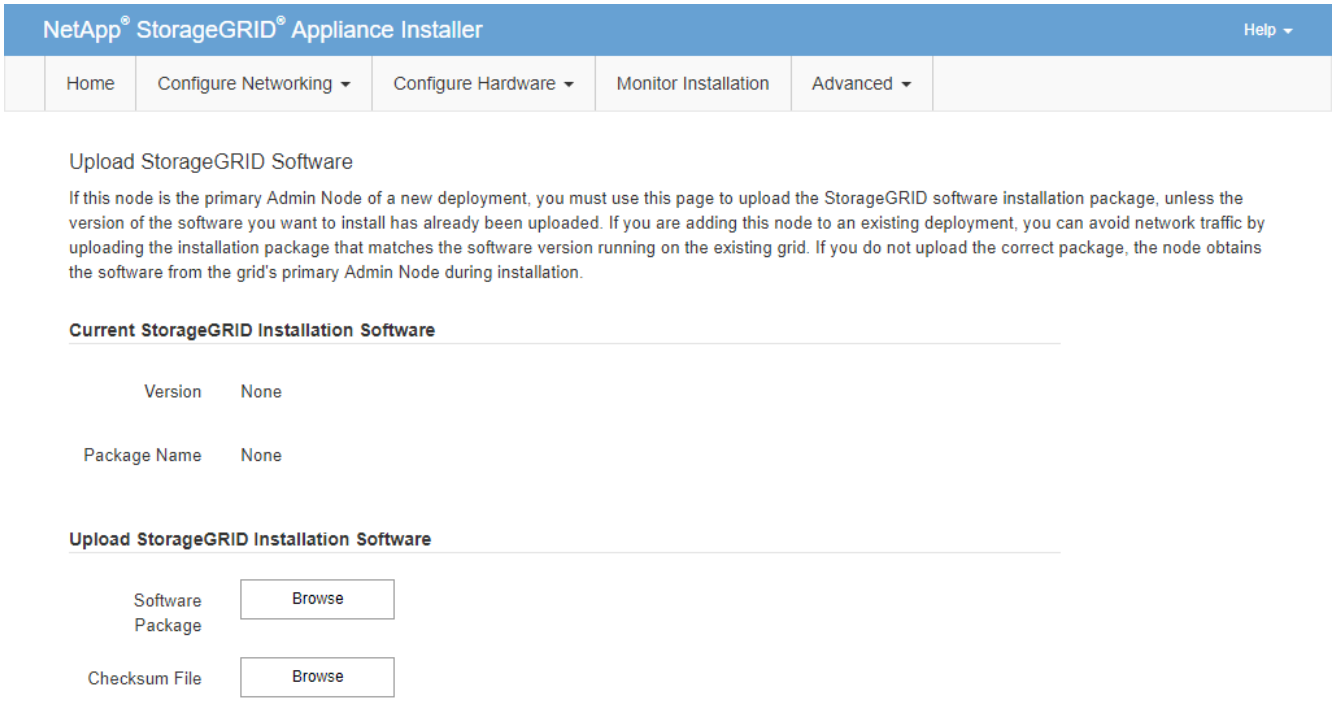
   b. En el campo **Nombre de nodo**, introduzca el mismo nombre que se utilizó para el nodo que está recuperando y haga clic en **Guardar**.

   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. Anule la selección de la casilla de verificación **Activar descubrimiento de nodo de administración**. b. Introduzca la dirección IP de forma manual. c. Haga clic en **Guardar**. d. Espere mientras el estado de conexión para la nueva dirección IP se convierte en "muy listo".

Opción	Descripción
Detección automática de todos los nodos principales de administración conectados	a. Active la casilla de verificación **Activar descubrimiento de nodos de administración**. 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 mientras el estado de conexión para la nueva dirección IP se convierte en "muy 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 instalación y mantenimiento del 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.

Información relacionada

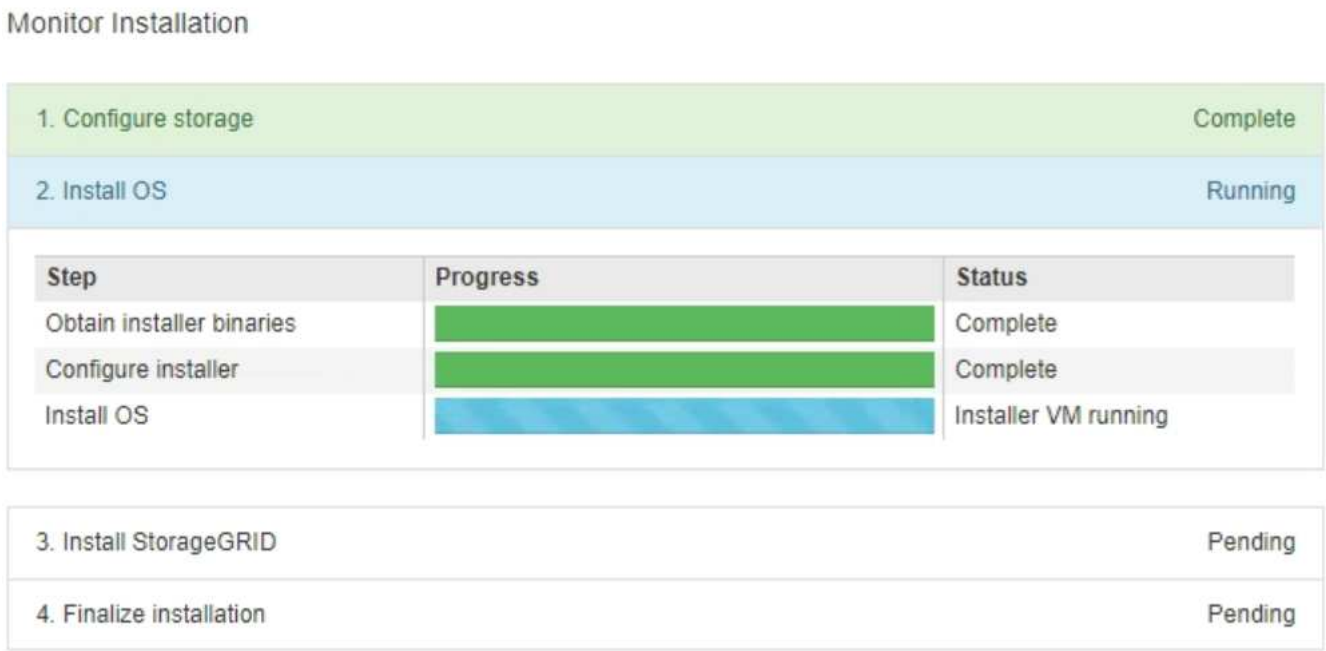
Servicios de aplicaciones SG100 y SG1000

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.

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.

> El instalador garantiza que no se vuelvan a ejecutar las tareas completadas en una instalación anterior. 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 de "Shided."

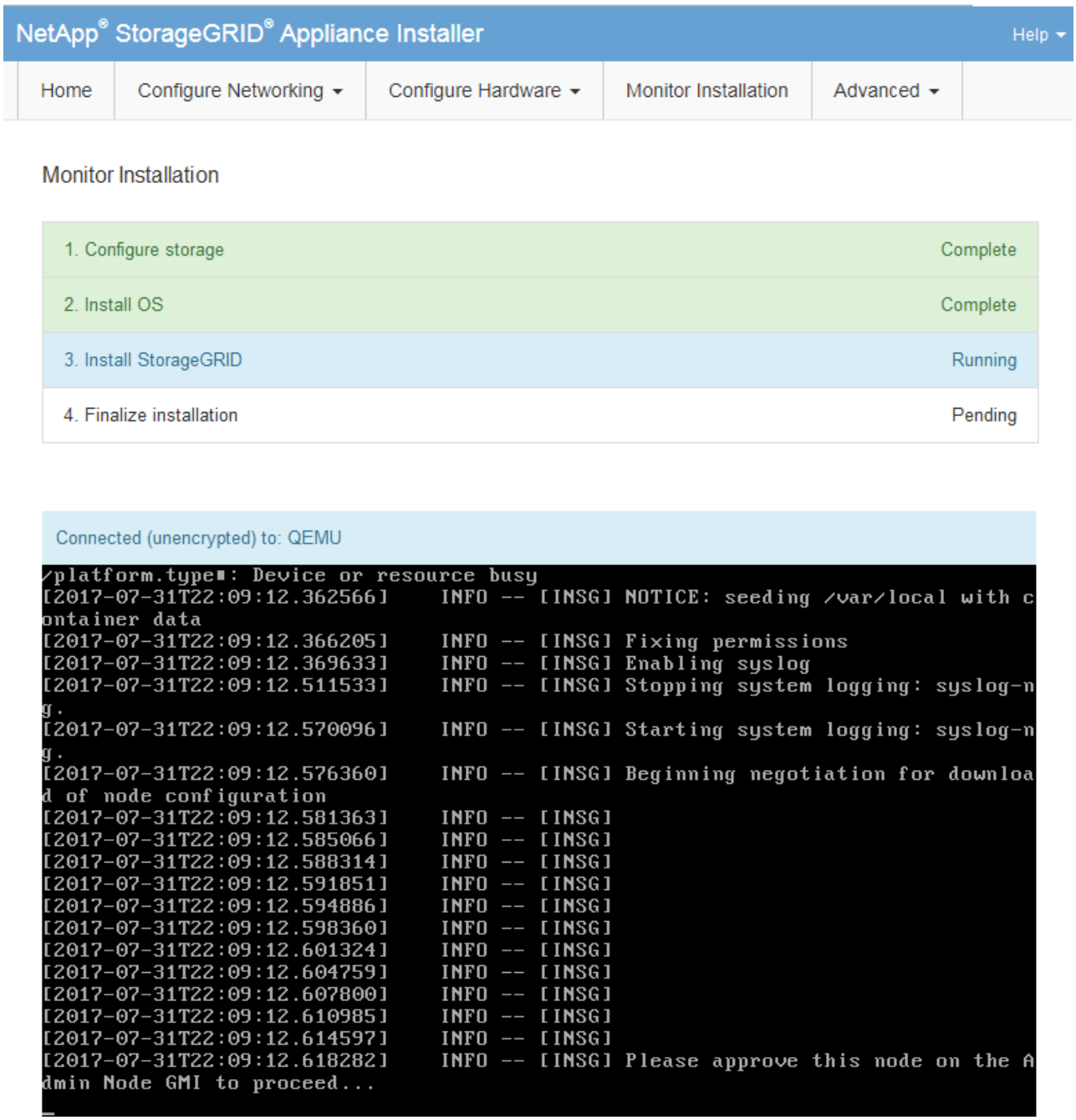
2. Revise el progreso de las dos primeras etapas de instalación.
   - **1. Configurar almacenamiento**

     Durante esta fase, el instalador borra toda la configuración existente de las unidades y configura la configuración del host.

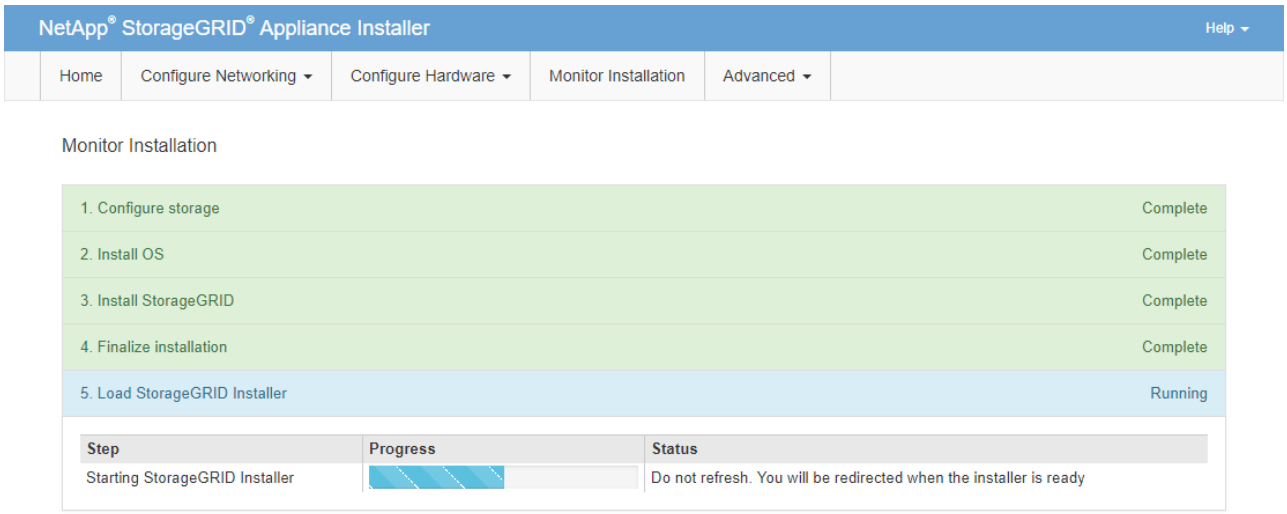
   - **2. Instalar OS**

     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. Continúe con el siguiente paso del proceso de recuperación del tipo de nodo de grid de 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 realiza la recuperación del sitio el soporte técnico

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 error**: Antes de comenzar una recuperación del sitio, es importante establecer si alguno de los nodos en el sitio fallido está intacto o si alguno de los nodos de almacenamiento contiene

objetos recuperables. Si reconstruye nodos o volúmenes de almacenamiento que contienen datos válidos, podría producirse una pérdida de datos innecesaria.

- **Política de ILM activa**: El número, el tipo y la ubicación de las copias de objetos de la cuadrícula está controlado por su política de ILM activa. Los detalles específicos de su política de ILM pueden afectar la cantidad de datos recuperables, así como las técnicas específicas necesarias para la recuperación.

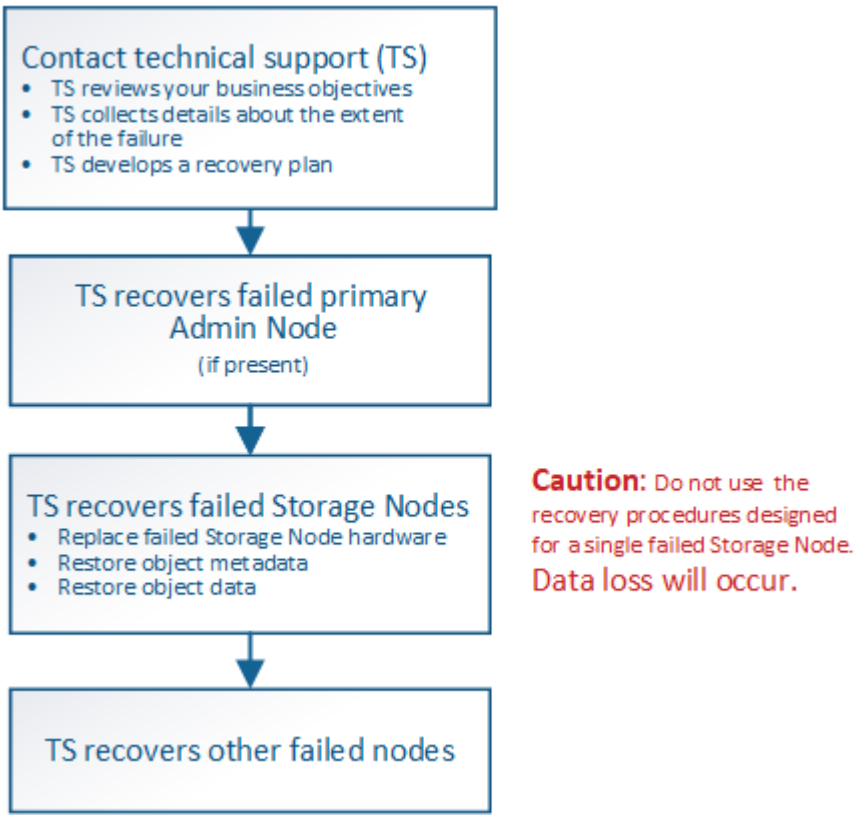
  Si un sitio contiene la única copia de un objeto y el sitio se pierde, el objeto se pierde.

- **Consistencia de bloque (o contenedor)**: El nivel de consistencia aplicado a un cubo (o contenedor) afecta si StorageGRID replica completamente los metadatos de objeto a todos los nodos y sitios antes de decirle a un cliente que la ingesta de objeto fue correcta. Si el nivel de consistencia permite eventualmente la consistencia, es posible que se hayan perdido algunos metadatos de objetos en el fallo del sitio. Esto puede afectar a la cantidad de datos recuperables y a los detalles del procedimiento de recuperación.
- * Historia de los cambios recientes*: Los detalles de su procedimiento de recuperación pueden verse afectados por si algún procedimiento de mantenimiento estaba en curso en el momento del fallo o si se han realizado cambios recientes en su política 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.

Descripción general de la recuperación del sitio

Esta es una descripción general del proceso que utiliza el soporte técnico para recuperar un sitio con errores.

Solo el soporte técnico puede realizar la recuperación del sitio.



1. Póngase en contacto con el soporte técnico.

   El soporte técnico realiza una evaluación detallada del error y trabaja con usted para revisar sus objetivos empresariales. A partir de esta información, el soporte técnico desarrolla un plan de recuperación

adaptado a su situación.

2. El soporte técnico recupera el nodo de administración principal si se ha producido un error.
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 un sitio entero, se necesitan comandos especializados para restaurar correctamente los objetos y los metadatos de objetos.

4. El soporte técnico recupera otros nodos con errores.

   Una vez recuperados los metadatos y los datos de objetos, los nodos de puerta de enlace con error, los nodos de administrador que no son primarios y los nodos de archivado pueden recuperarse mediante procedimientos estándar.

Información relacionada

Retirada de sitios

Procedimiento de retirada

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 de **nodo** para eliminar uno o más nodos, que pueden estar en uno o más sitios. Los nodos que quita pueden estar en línea y conectados al sistema StorageGRID, o bien pueden estar desconectados y desconectados.
- Realice una retirada de **sitio conectado** para eliminar un sitio en el que todos los nodos estén conectados a StorageGRID.
- Realice una retirada de sitio * desconectado* para eliminar un sitio en el que todos los nodos estén desconectados de StorageGRID.

> Antes de retirar un 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.

Si un sitio contiene una mezcla de conectado ( ) y nodos desconectados (o.), debe volver a conectar todos los nodos sin conexión.

Si necesita realizar un segundo procedimiento de mantenimiento, puede hacerlo Detenga el procedimiento de retirada 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.

Información relacionada

Retirada del nodo de grid

Retirada de sitios

Retirada del nodo de grid

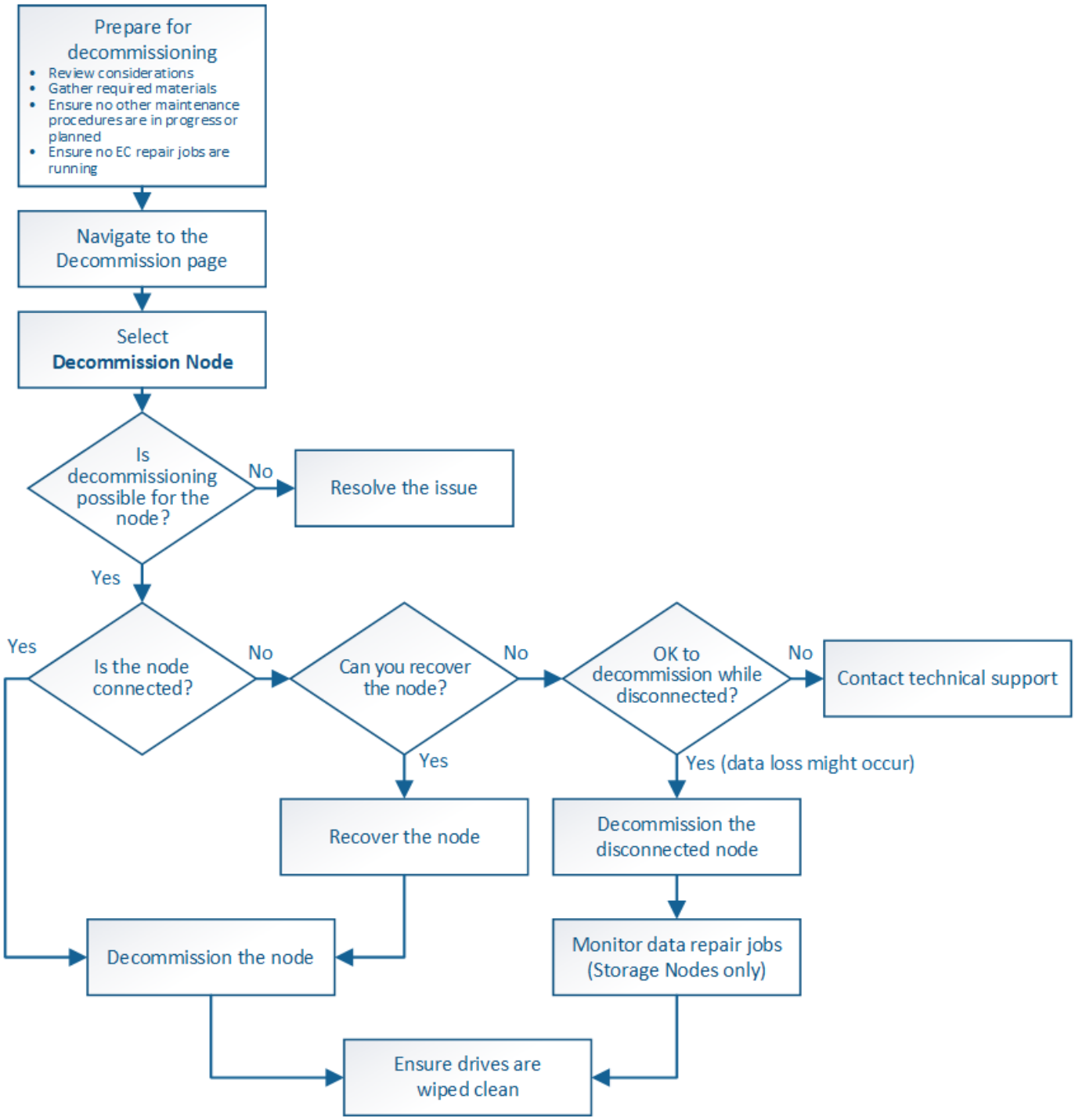
Puede usar el procedimiento de retirada de nodos para quitar uno o varios nodos de almacenamiento, nodos de puerta de enlace o nodos de administración no primarios en uno o más sitios. No puede retirar el nodo administrador principal ni un nodo de archivado.

En general, debe retirar los nodos de red solo mientras están conectados al sistema StorageGRID y todos los nodos tienen un estado normal (tienen iconos verdes en las páginas **NODOS** y en la página **nodos de misión**). Sin embargo, si es necesario, puede retirar un nodo de grid desconectado. Antes de quitar un nodo desconectado, asegúrese de comprender las implicaciones y restricciones de ese proceso.

Usar el procedimiento de retirada del nodo cuando se cumple alguna de las siguientes condiciones:

- Añadió un nodo de almacenamiento de mayor tamaño al sistema y desea quitar uno o más nodos de almacenamiento más pequeños mientras conserva los objetos al mismo tiempo.
- 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 diagrama de flujo muestra los pasos de alto nivel para retirar los nodos de la cuadrícula.



Prepare la retirada de nodos de grid

Debe revisar las consideraciones que se deben tener en cuenta al eliminar los nodos de cuadrícula y confirmar que no haya ninguna tarea de reparación activa para los datos codificados de borrado.

Consideraciones para la retirada del nodo de grid

Antes de iniciar este procedimiento para retirar uno o más nodos, debe comprender las implicaciones que tendría la eliminación de cada tipo de nodo. Una vez que el decomisionado correcto de un nodo, sus servicios se deshabilitarán y el nodo se apagará

automáticamente.

No puede retirar un nodo si lo hace dejará a StorageGRID en estado no válido. Se aplican las siguientes reglas:

- No se puede retirar el nodo de administrador principal.
- No se pueden retirar nodos de archivado.
- No puede retirar un nodo de administrador ni un nodo de puerta de enlace si una de sus interfaces de red forma parte de un grupo de alta disponibilidad (ha).
- No puede retirar un nodo de almacenamiento si su eliminación afectaría al quórum de ADC.
- No puede retirar un nodo de almacenamiento si se requiere para la política de ILM activa.
- No debe retirar más de 10 nodos de almacenamiento en un único procedimiento de nodo de retirada.
- No puede decomisionar un nodo conectado si el grid incluye nodos desconectados (nodos cuyo estado es desconocido o inactivo administrativamente). Primero, debe decomisionar o recuperar los nodos desconectados.
- 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.
- Si no se puede quitar un nodo desconectado (por ejemplo, un nodo de almacenamiento necesario para el quórum de ADC), no se puede quitar ningún otro nodo desconectado.
- Si desea sustituir un aparato antiguo por otro más nuevo, tenga en cuenta clonar el nodo del dispositivo en lugar de retirar el nodo antiguo y añadir el nuevo nodo en una ampliación.

> No quite la máquina virtual de un nodo de grid ni otros recursos hasta que se le indique hacerlo en procedimientos de retirada.

Consideraciones para la retirada del nodo de administración o del nodo de puerta de enlace

Revise las siguientes consideraciones antes de retirar un nodo de administración o un nodo de puerta de enlace.

- El procedimiento de retirada del servicio requiere acceso exclusivo a algunos recursos del sistema, por lo que debe confirmar que no se están ejecutando otros procedimientos de mantenimiento.
- No se puede retirar el nodo de administrador principal.
- No puede retirar un nodo de administrador ni 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 administrar StorageGRID.
- Según sea necesario, puede cambiar con seguridad la política de ILM mientras decomisiona un nodo de puerta de enlace o 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).

Información relacionada

Administre StorageGRID

Consideraciones para la retirada del nodo de almacenamiento

Si va a retirar un nodo de almacenamiento, debe comprender cómo StorageGRID gestiona los datos de objeto y los metadatos de ese nodo.

Se aplican las siguientes consideraciones y restricciones al decomisionar nodos de almacenamiento:

- El sistema debe, en todo momento, incluir suficientes nodos de almacenamiento para satisfacer los requisitos operativos, incluidos el quórum de ADC y la normativa de ILM activa. 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.
- Si el nodo de almacenamiento se desconecta durante su retirada, el sistema debe reconstruir los datos mediante datos de los nodos de almacenamiento conectados, lo que puede producir la pérdida de datos.
- Cuando se quita un nodo de almacenamiento, se deben transferir grandes volúmenes de datos de objeto a través de la red. Si bien 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.
- Los procedimientos de retirada que implican a los nodos de almacenamiento se pueden pausar durante ciertas fases para permitir que se ejecuten otros procedimientos de mantenimiento en caso de que sean necesarios y luego se reanuden una vez completadas.
- No se pueden ejecutar operaciones de reparación de datos en ningún nodo de cuadrícula cuando se está ejecutando una tarea de retirada.
- No debe realizar ningún cambio en la política de ILM mientras se decomisione un nodo de almacenamiento.
- Cuando quita un nodo de almacenamiento, los datos del nodo se migran a otros nodos de grid; sin embargo, estos datos no se eliminan completamente del nodo de cuadrícula dado de servicio. Para eliminar datos de forma permanente y segura, debe borrar las unidades del nodo de cuadrícula dado de baja una vez completado el procedimiento de retirada.
- Al decomisionar un nodo de almacenamiento, es posible que se eliminen las siguientes alertas y alarmas y que se puedan recibir las notificaciones SNMP y por correo electrónico relacionadas:
  - **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.

Información relacionada

Restaure datos de objetos al volumen de almacenamiento, si es necesario

Comprender el quórum de ADC

Es posible que no pueda retirar ciertos nodos de almacenamiento en un sitio de centro de datos si después del decomisionado permanecerán demasiados servicios de controlador de dominio administrativo (ADC). Este servicio, que se encuentra en algunos nodos de almacenamiento, mantiene información de topología de grid y proporciona servicios de configuración al grid. 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 se quita el nodo se haría que el quórum de ADC ya no se cumpliera. Para satisfacer el quórum de ADC durante un decomisionado, un mínimo de tres nodos de almacenamiento en cada sitio del centro de datos debe tener el servicio ADC. Si un sitio de un centro de datos tiene más de tres nodos de almacenamiento con el servicio ADC, la mayoría simple de esos nodos debe permanecer disponible después de la retirada ((0.5 * `Storage Nodes with ADC`) + 1).

Por ejemplo, supongamos que el sitio de un centro de datos incluye actualmente seis nodos de almacenamiento con servicios ADC y 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 del servicio, debe asegurarse de que cuatro nodos de almacenamiento con servicios ADC permanecen disponibles ((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 ahora sólo requiere que tres servicios ADC permanezcan disponibles ((0.5 * 4) + 1).

Si necesita retirar un nodo de almacenamiento pero no puede debido al requisito de quórum de ADC, debe agregar un nodo de almacenamiento nuevo en una expansión y especificar que debe tener un servicio ADC. A continuación, puede retirar el nodo de almacenamiento existente.

Información relacionada

Amplíe su grid

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 la política de gestión de vida útil activa para garantizar que el sistema StorageGRID siga teniendo la capacidad suficiente del tipo correcto y en las ubicaciones correctas para poder acomodar el desmantelamiento 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, Debe agregar 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.
- ¿El sistema, en todo momento, incluirá suficientes nodos de almacenamiento como para satisfacer la política activa de ILM?

> Una política de ILM que no se pueda satisfacer provocaría retrasos y alarmas, además de detener el funcionamiento del sistema StorageGRID.

Compruebe que la topología propuesta que será el resultado del proceso de decomisionado cumpla la política de ILM al evaluar los factores indicados en la tabla.

Área a evaluar	Notas
Capacidad disponible	¿Habrá suficiente capacidad de almacenamiento para acomodar todos los datos de objetos almacenados en el sistema StorageGRID? Incluir las copias permanentes de datos de objetos almacenados actualmente en el nodo de almacenamiento para ser dado de baja. ¿Habrá suficiente capacidad para gestionar el crecimiento previsto de los datos de objetos almacenados por un intervalo de tiempo razonable una vez completado 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 dictar que el contenido se puede mover de un tipo de almacenamiento a otro a medida que el contenido envejece. De ser así, debe asegurarse de que la configuración final del sistema StorageGRID dispone de suficiente almacenamiento del tipo adecuado.

Información relacionada

Gestión de objetos con ILM

Amplíe su grid

Retire nodos de almacenamiento desconectados

Debe comprender qué puede suceder si decomisiona un nodo de almacenamiento mientras está desconectado (el estado es desconocido o inactivo administrativamente).

Al decomisionar un nodo de almacenamiento desconectado del grid, StorageGRID utiliza datos de otros nodos de almacenamiento para reconstruir los datos de objetos y los metadatos que se encuentran en el nodo desconectado. Para ello, inicia automáticamente los trabajos de reparación de datos al final del proceso de retirada del servicio.

Antes de retirar un nodo de almacenamiento desconectado, tenga en cuenta lo siguiente:

- Nunca debe decomisionar un nodo desconectado a menos que esté seguro de que no se puede conectar ni recuperar.

> No realice este procedimiento si cree que podría recuperar datos de objeto del nodo. En su lugar, póngase en contacto con el soporte técnico para determinar si es posible la recuperación del nodo.

- Si un nodo de almacenamiento desconectado contiene la única copia de un objeto, se perderá ese objeto al retirar el nodo. 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.
- 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 se supervisan mediante el procedimiento de retirada. Debe supervisar manualmente estos trabajos y reiniciarlos según sea necesario. Consulte Compruebe los trabajos de reparación de datos.
- Si decomisiona más de un nodo de almacenamiento desconectado a la vez, se podrían perder datos. Es posible que el sistema no pueda reconstruir los datos si hay muy pocas copias disponibles de datos de objetos, metadatos o fragmentos codificados para borrado.

> Si tiene más de un nodo de almacenamiento desconectado que no se puede recuperar, póngase en contacto con el soporte técnico para determinar el mejor curso de acción.

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 nodos de almacenamiento, se amplía el sistema StorageGRID para añadir nodos de almacenamiento nuevos con mayor capacidad y, luego, decomisionar los nodos de almacenamiento antiguos y 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 o pequeños con modelos nuevos o dispositivos de mayor capacidad, muchos deben usar la función de clonado de nodos o el procedimiento de clonado de nodos y el procedimiento de retirada si no va a realizar 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.

Información relacionada

Amplíe su grid

Retire nodos de almacenamiento múltiples

Si necesita quitar más de un nodo de almacenamiento, puede decomisionar secuencialmente o en paralelo

- 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 resultar en una situación en la que todas las copias permanentes de un archivo se marquen como «sólo en términos de lectura», desactivando temporalmente la eliminación en cuadrículas en las que esta función está activada.

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.

Si necesita retirar un nodo de almacenamiento desconectado, también completará estos pasos una vez completado el procedimiento de retirada para garantizar que el trabajo de reparación de datos se ha 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.

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

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

   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. 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. Vaya al paso siguiente.

```
root@DC1-ADM1:~ # repair-data show-ec-repair-status

Repair ID Scope Start Time End Time State Est/Affected Bytes Repaired
Retry Repair
=========================================================================
===========
949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success 17359
17359 No
949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure 17359 0
Yes
949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure 17359 0
Yes
949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure 17359 0
Yes
```

3. Si el Estado para todas las reparaciones es `Success`, no es necesario reiniciar ningún trabajo de reparación.
4. Si el estado para cualquier reparación es `Failure`, 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 `Success`.

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.

Elemento	Notas
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.

Lo que necesitará

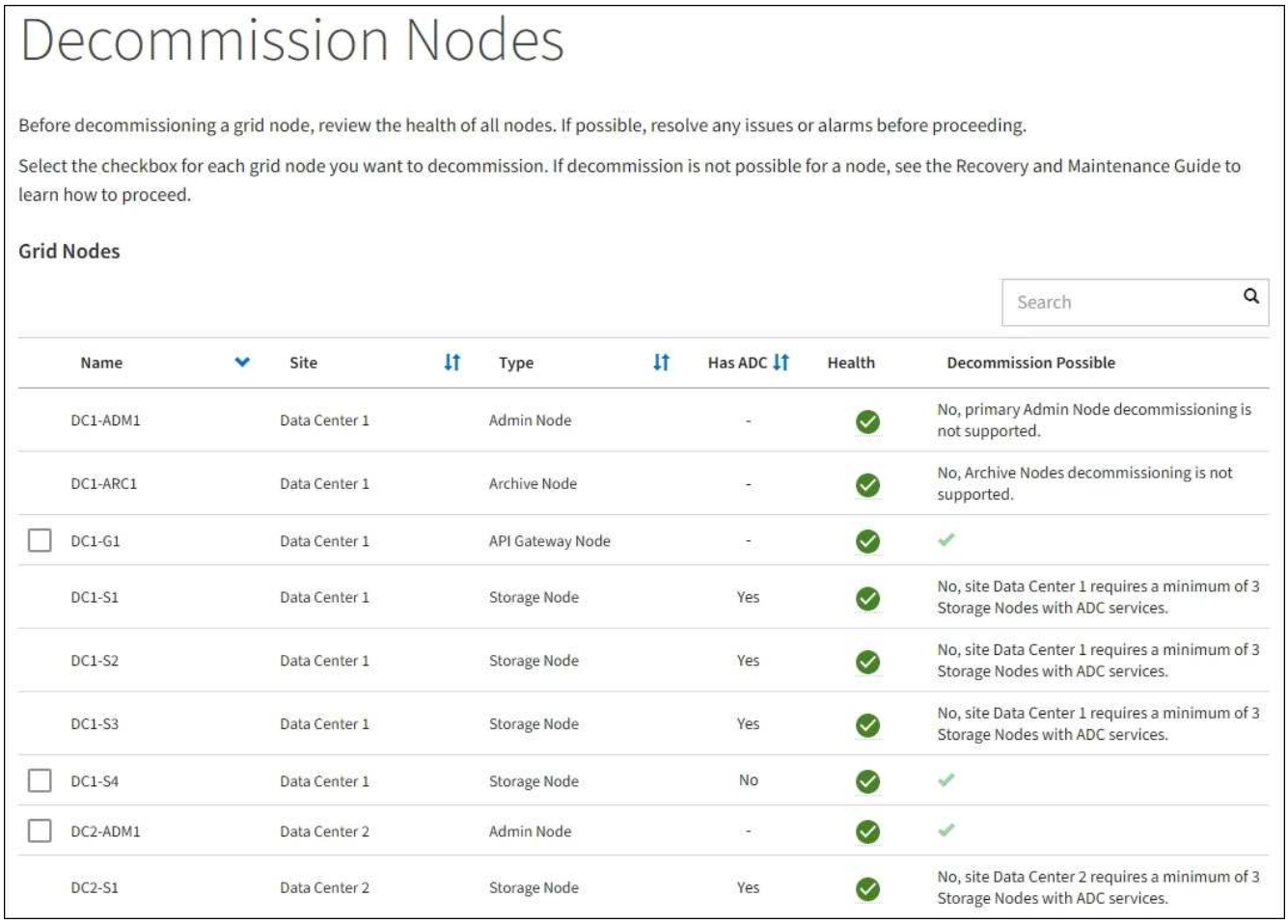
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener los permisos de mantenimiento o acceso raíz.

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. Por ejemplo, esta página muestra nodos de cuadrícula en dos centros de datos. La columna Decommission posible indica que puede retirar el nodo de puerta de enlace, uno de los cinco nodos de almacenamiento y el nodo de administración no primario.



3. Revise la columna **DECOMmission possible** para cada nodo que desee retirar.

   Si se puede retirar el servicio de un nodo de cuadrícula, esta columna incluye una Marca de verificación verde y la columna situada más a la izquierda incluye una casilla de verificación. Si un nodo no puede retirarse, esta columna describe el problema. Si hay más de una razón por la que un nodo no puede ser retirado, se muestra el motivo más crítico.

Razón posible de retirada	Descripción	Pasos a resolver
No, el tipo de nodo decomisionado no es compatible.	No puede retirar el nodo administrador principal ni un nodo de archivado.	Ninguno.

Razón posible de retirada	Descripción	Pasos a resolver
No, al menos un nodo de grid está desconectado. **Nota:** este mensaje sólo se muestra para los nodos de red conectados.	No puede retirar 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	Vaya a la paso que enumera las opciones de procedimiento de retirada de servicio.
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 red desconectado si también se desconecta uno o más nodos necesarios (por ejemplo, un nodo de almacenamiento necesario para el quórum de ADC).	a. Revise los mensajes de DECOMmission posibles para todos los nodos desconectados. b. Determine qué nodos no se pueden retirar del servicio 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 alta disponibilidad: *X*. Antes de poder retirar este nodo, debe quitarlo de todos los grupos de alta disponibilidad.	No puede retirar un nodo de administrador ni un nodo de puerta de enlace si una interfaz de nodo pertenece a un grupo de alta disponibilidad.	Edite el grupo de alta disponibilidad para quitar la interfaz del nodo o eliminar todo el grupo de alta disponibilidad. Consulte las instrucciones para administrar StorageGRID.
No, el sitio *x* requiere un mínimo de *n* nodos de almacenamiento con servicios ADC.	**Sólo nodos de almacenamiento.** no puede retirar un nodo de almacenamiento si no quedan nodos suficientes en el sitio para admitir los requisitos de quórum de ADC.	Realice una expansión. Agregue un nodo de almacenamiento nuevo al sitio y especifique que debe tener un servicio ADC. Consulte la información sobre el quórum de ADC.

Razón posible de retirada	Descripción	Pasos a resolver
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.	**Sólo nodos de almacenamiento.** no puede retirar un nodo de almacenamiento a menos que queden suficientes nodos para los perfiles de código de borrado existentes. Por ejemplo, si existe un perfil de código de borrado para la codificación de borrado 4+2, deben permanecer 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 la política activa de ILM**: Realizar una expansión. Añada suficientes nodos de almacenamiento nuevos para permitir que continúe la codificación de borrado. Consulte las instrucciones para ampliar StorageGRID. • **Utilizado en una regla de ILM pero no en la política de ILM activa**: Edite o elimine la regla y, a continuación, desactive el perfil de código de borrado. • **No se utiliza en ninguna regla ILM**: Desactiva el perfil de código de borrado. **Nota:** aparece un mensaje de error si intenta desactivar un perfil de código de borrado y los datos de objeto siguen asociados con el perfil. Es posible que deba esperar varias semanas antes de volver a intentar el proceso de desactivación. Obtenga información sobre cómo desactivar un perfil de código de borrado en las instrucciones para gestionar objetos con la gestión del ciclo de vida de la información.

4. Si es posible la retirada del servicio para el nodo, determine qué procedimiento debe realizar:

Si la cuadrícula incluye…	Vaya a…
Todos los nodos de grid desconectados	Retirada de nodos de red desconectados
Solo nodos de grid conectados	Retirada de nodos de grid conectados

Información relacionada

Compruebe los trabajos de reparación de datos

Comprender el quórum de ADC

Gestión de objetos con ILM

Amplíe su grid

Administre StorageGRID

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).

Lo que necesitará

- Usted entiende los requisitos y. consideraciones sobre el decomisionado de los nodos de cuadrícula.
- 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.
- Debe tener 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 almacenamiento denominado DC1-S4 está desconectado; todos los demás nodos están conectados.

Decommission Nodes

Before decommissioning a grid node, review the health of all nodes. If possible, resolve any issues or alarms before proceeding.

A grid node is disconnected (has a blue or gray health icon). Try to bring it back online or recover it. Data loss might occur if you decommission a node that is disconnected.

See the Recovery and Maintenance Guide for details. Contact Support if you cannot recover a node and do not want to decommission it.

Select the checkbox for each grid node you want to decommission. If decommission is not possible for a node, see the Recovery and Maintenance Guide to learn how to proceed.

Grid Nodes

Search

	Name	Site	Type	Has ADC	Health	Decommission Possible
	DC1-ADM1	Data Center 1	Admin Node	-		No, primary Admin Node decommissioning is not supported.
	DC1-ADM2	Data Center 1	Admin Node	-		No, at least one grid node is disconnected.
	DC1-G1	Data Center 1	API Gateway Node	-		No, at least one grid node is disconnected.
	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		✔

Passphrase

Provisioning Passphrase

Start Decommission

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.

> Tenga mucho cuidado al retirar más de un nodo de grid desconectado a la vez, especialmente si selecciona varios nodos de almacenamiento desconectados.

- Si no se puede quitar un nodo desconectado (por ejemplo, un nodo de almacenamiento necesario para el quórum de ADC), no se puede quitar ningún otro nodo desconectado.

Antes de retirar un **nodo de almacenamiento** desconectado, tenga en cuenta lo siguiente

- Nunca debe decomisionar un nodo de almacenamiento desconectado a menos que esté seguro de que no se puede conectar ni recuperar.

> Si cree que los datos de objeto todavía se pueden recuperar del nodo, no realice este procedimiento. En su lugar, póngase en contacto con el soporte técnico para determinar si es posible la recuperación del nodo.

- Si decomisiona más de un nodo de almacenamiento desconectado, se podrían perder datos. 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.

  > Si tiene más de un nodo de almacenamiento desconectado que no se 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 se supervisan mediante el procedimiento de retirada. 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.

Antes de retirar un nodo **Admin** o **Gateway Node** desconectado, tenga en cuenta lo siguiente:

- 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.
- Puede retirar un nodo de puerta de enlace de forma segura mientras está desconectado.

Pasos

1. Intente volver a conectar los nodos de grid desconectados o para recuperarlos.

   Consulte los procedimientos de recuperación para obtener instrucciones.

2. Si no puede recuperar un nodo de cuadrícula desconectado y desea decomisionar mientras está desconectado, seleccione la casilla de comprobación 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.

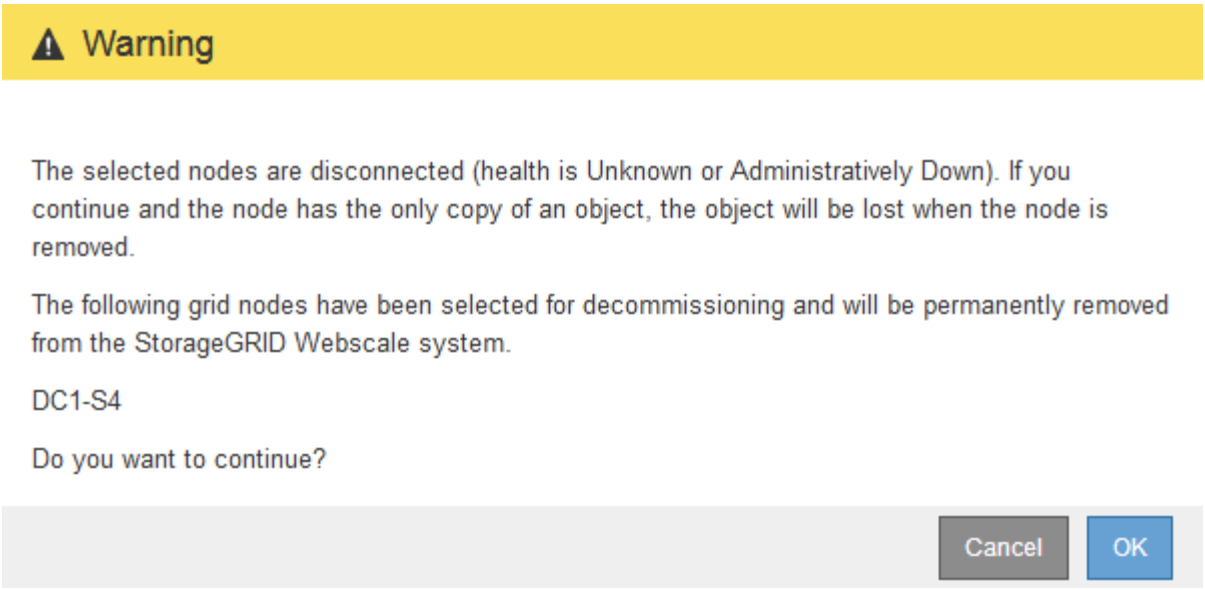
   > Tenga mucho cuidado al elegir retirar más de un nodo de grid desconectado a la vez, especialmente si selecciona varios nodos de almacenamiento desconectados. Si tiene más de un nodo de almacenamiento desconectado que no se puede recuperar, póngase en contacto con el soporte técnico para determinar el mejor curso de acción.

3. Introduzca la clave de acceso de aprovisionamiento.

   El botón **Iniciar misión** está activado.

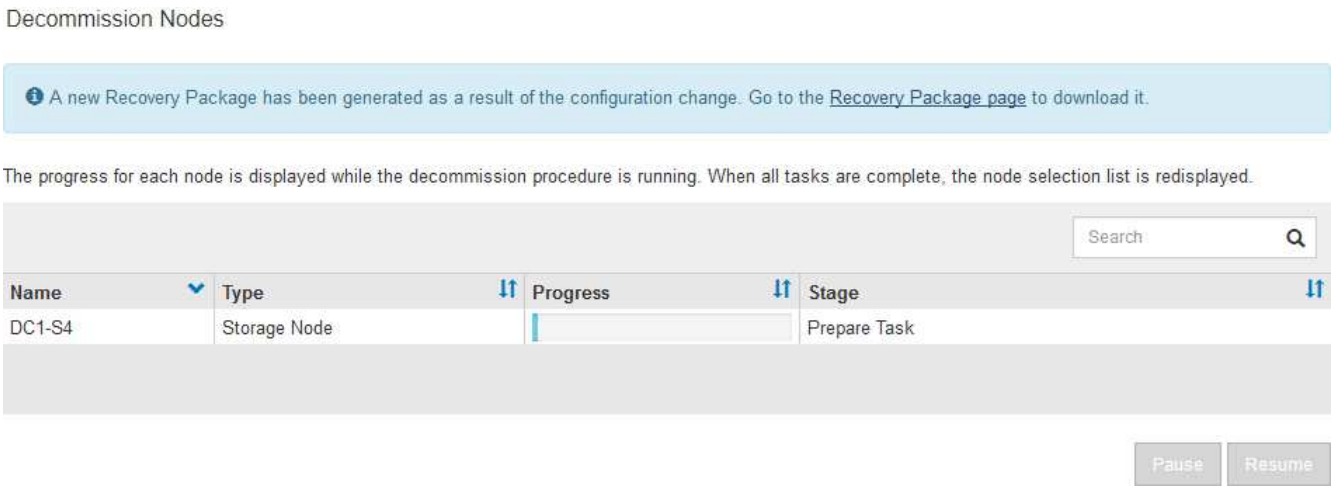
4. Haga clic en **Iniciar misión**.

   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. Tan pronto como 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.

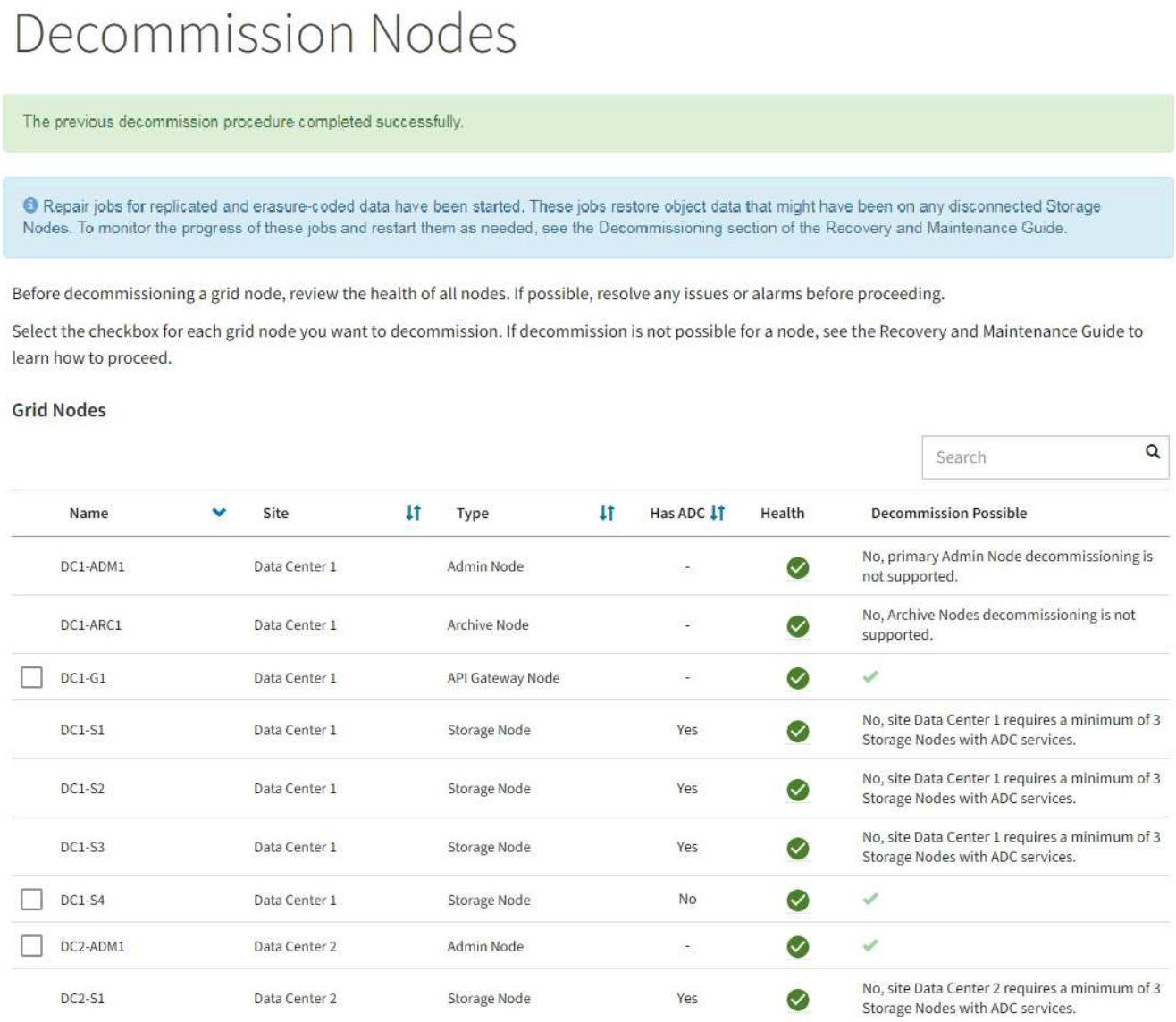
   > Descargue el Lo antes posible. del paquete de recuperación para asegurarse de que puede recuperar la red si hay algún problema durante el procedimiento de retirada de servicio.

   > 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 ejecute 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 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.

> Es posible que existan incoherencias de Cassandra y que no se realice 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 cumplan con su 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.
- Opcionalmente, para obtener un porcentaje estimado de finalización para la reparación replicada, agregue el `show-replicated-repair-status` opción del comando repair-data.

```
repair-data show-replicated-repair-status
```

> La `show-replicated-repair-status` Esta opción está disponible para la versión preliminar técnica de StorageGRID 11.6. Esta característica está en desarrollo y el valor devuelto puede ser incorrecto o retardado. Para determinar si una reparación está completa, utilice **esperando – todos**, **reparaciones intentadas (XRPA)** y **periodo de exploración — estimado (XSCM)** como se describe en Reparaciones del monitor.

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.
  - Servicios de aplicaciones SG100 y SG1000
  - Dispositivos de almacenamiento SG5600
  - Dispositivos de almacenamiento SG5700
  - Dispositivos de almacenamiento SG6000

Información relacionada

Procedimientos de recuperación de nodos de grid

Retirada de nodos de grid conectados

Puede retirar y eliminar permanentemente los nodos conectados a la cuadrícula.

- Debe comprender los requisitos y. consideraciones sobre el decomisionado de los nodos de cuadrícula.
- Usted debe haber reunido todos los materiales requeridos.
- Debe haberse asegurado de que no hay ningún trabajo de reparación de datos activo.
- Debe haber 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.
- Debe haber asegurado 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.
- Debe tener la clave de acceso de aprovisionamiento.
- Los nodos de grid están conectados.
- La columna **retirada posible** para el nodo o los nodos que desea retirar debe incluir una Marca de verificación verde.
- Todos los nodos de grid deben tener 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.

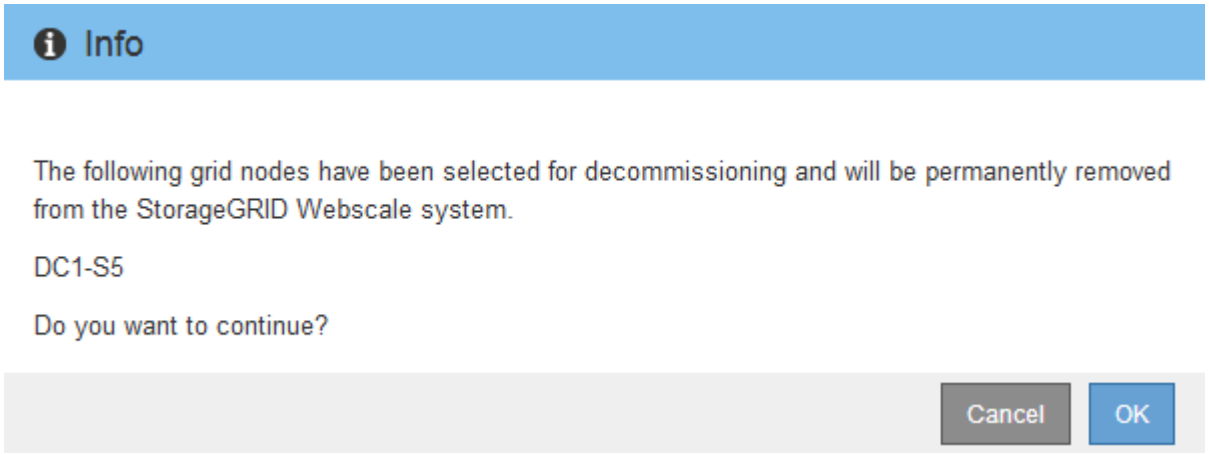
> No quite la máquina virtual de un nodo de grid ni otros recursos hasta que se le indique hacerlo en este procedimiento.

1. En la página nodos de misión de retirada, seleccione la casilla de verificación de cada nodo de cuadrícula que desee retirar.
2. Introduzca la clave de acceso de aprovisionamiento.

El botón **Iniciar misión** está activado.

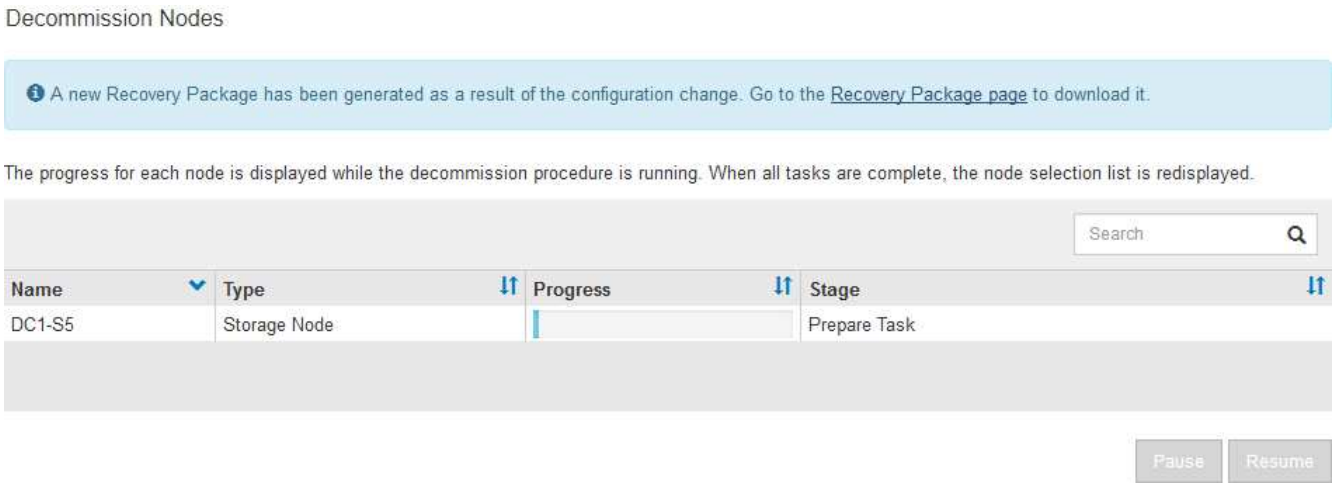
3. Haga clic en **Iniciar misión**.

   Se muestra un cuadro de diálogo de confirmación.



4. Revise la lista de nodos seleccionados y haga clic en **Aceptar**.

   Se inicia el procedimiento de retirada del nodo y se muestra el progreso de cada nodo. Durante el procedimiento, se genera un nuevo paquete de recuperación para mostrar el cambio de configuración de la cuadrícula.



> No desconecte un nodo de almacenamiento una vez que se haya iniciado el procedimiento de retirada del servicio. El cambio de estado puede provocar que parte del contenido no se copie en otras ubicaciones.

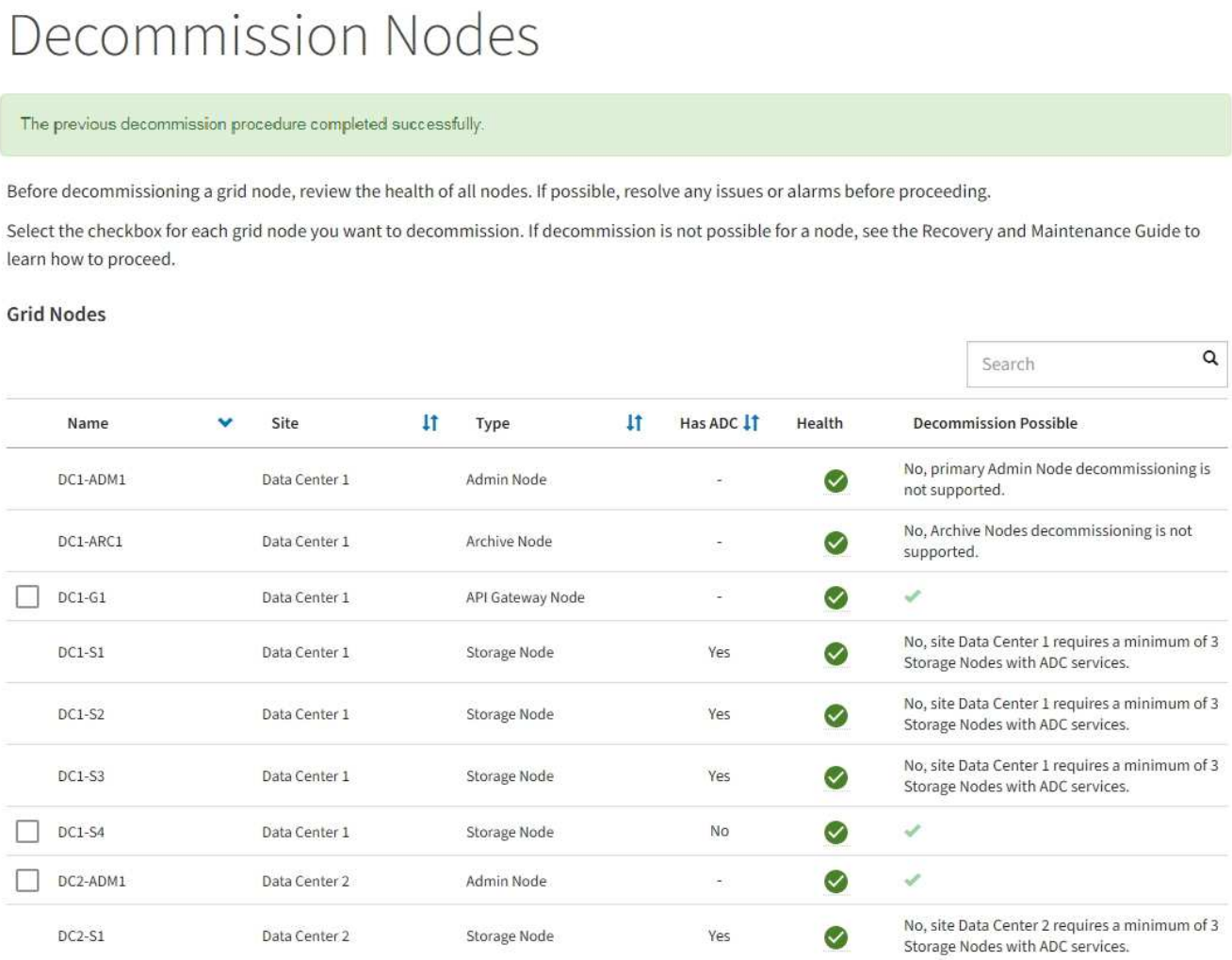
5. Tan pronto como el nuevo paquete de recuperación esté disponible, haga clic en el enlace o seleccione **MANTENIMIENTO sistema paquete de recuperación** para acceder a la página paquete de recuperación. A continuación, descargue la `.zip` archivo.

   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.

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.



7. 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.
   - **VMware**: Es posible que desee utilizar la opción "Borrar desde disco" de vCenter 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.

Complete estos pasos después de completar el procedimiento de retirada del nodo:

- 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 utilizar el dispositivo en otra cuadrícula.

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG5600

Dispositivos de almacenamiento SG5700

Dispositivos de almacenamiento SG6000

Información relacionada

Instale Red Hat Enterprise Linux o CentOS

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.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener los permisos de mantenimiento o acceso raíz.

Pasos

1. Seleccione **MANTENIMIENTO** > **tareas** > **misión**.

   Aparece la página de retirada.

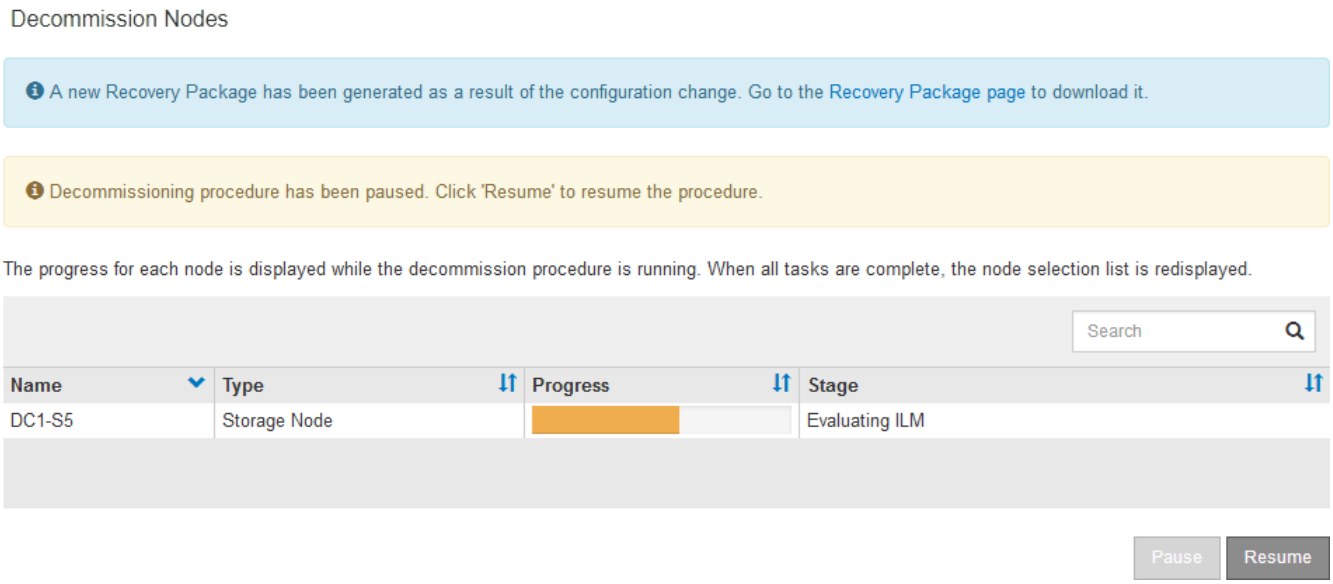
2. Seleccione **nodos de misión**.

   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
   - Datos codificados de borrado decomisionado

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.

Lo que necesitará

Debe iniciar 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 la cuadrícula de decomisionado 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.

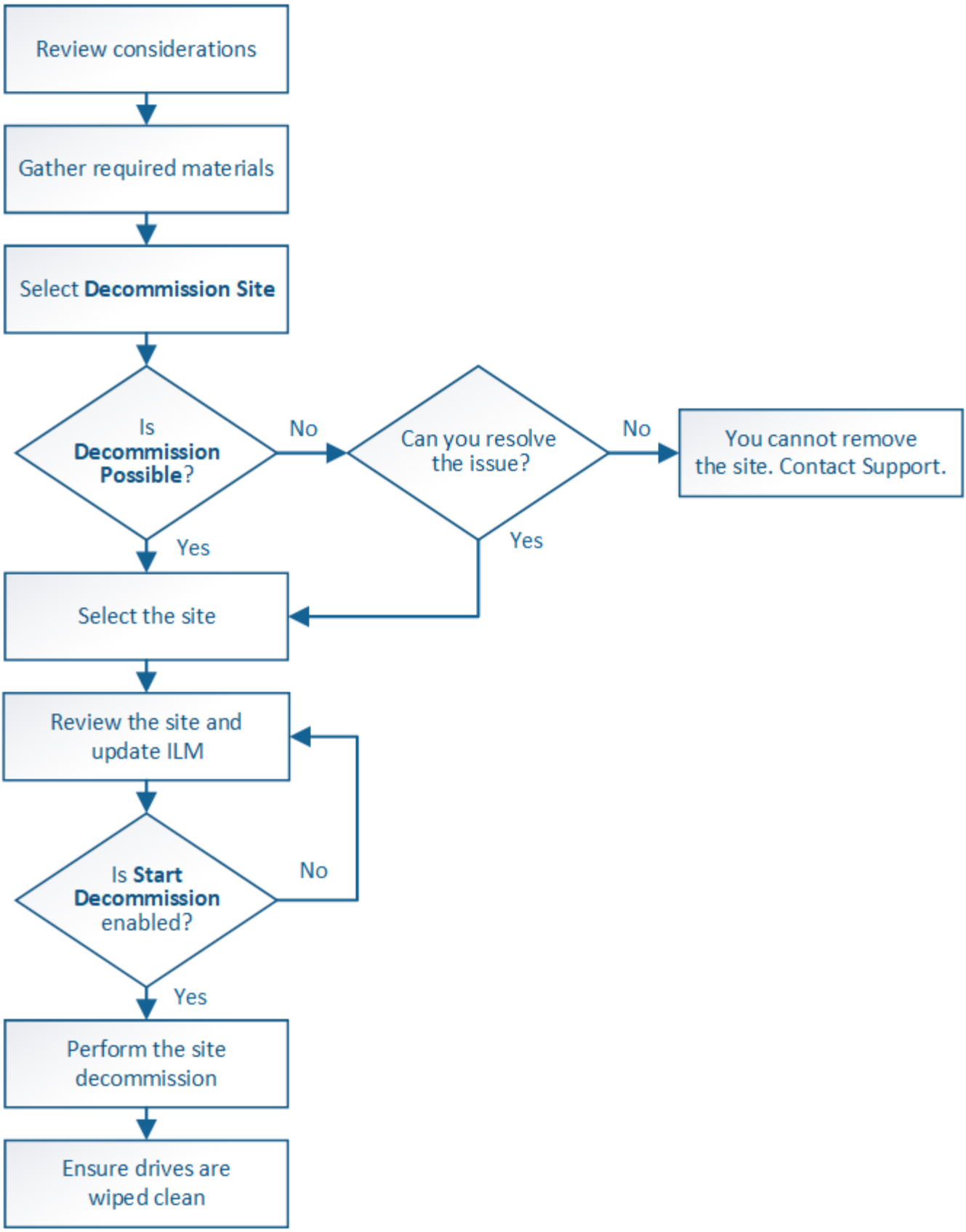
El servicio CMN debe estar conectado a al menos un servicio ADC y la mayoría (el 50 por ciento más uno) de los servicios ADC del sistema StorageGRID debe estar disponible para que una tarea de cuadrícula pueda moverse de una fase de desmantelamiento a otra y terminar.

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.

Retirada de sitios

Es posible que deba eliminar un sitio de centro de datos del sistema StorageGRID. Para quitar un sitio, debe retirarlo.

El diagrama de flujo muestra los pasos de alto nivel para retirar un sitio.



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 es posible utilizar pools de almacenamiento ni perfiles de código de borrado a los que se hace referencia en el sitio. Cuando StorageGRID descompone 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 pertenece a un grupo de alta disponibilidad (ha). 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 se puede iniciar el procedimiento de retirada del sitio si hay una operación de reparación de 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 puede crear reglas de ILM que hagan referencia al sitio que se va a retirar del servicio. Tampoco puede editar una regla de ILM existente para hacer referencia al sitio.
  - No puede realizar otros procedimientos de mantenimiento, como expansión o 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:

- La política de ILM activa no remite al sitio. Si lo está, debe crear y activar una nueva política de ILM con nuevas reglas de ILM.
- No existe ninguna política de ILM propuesta. Si tiene una política propuesta, debe eliminarla.
- No se hace referencia a ninguna regla de ILM al sitio, aunque estas reglas no se utilicen en la política activa o propuesta. Debe eliminar o editar todas las reglas que hacen referencia al sitio.

Cuando StorageGRID destransfiere el sitio, desactiva automáticamente todos los perfiles de código de borrado que no se utilicen y hacen referencia al sitio, y elimina automáticamente todos los pools de almacenamiento no utilizados que hacen referencia al sitio. El pool de almacenamiento predeterminado del sistema todos los nodos de almacenamiento 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. Estas instrucciones dan por sentado que conoce bien cómo funciona ILM y que está familiarizado con la creación de pools de almacenamiento, perfiles de código de borrado, reglas de ILM y la simulación y activación de una política de ILM. Consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

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 la política de ILM, debe revisar la capacidad de 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 suficiente disponible, es posible que deba añadir volúmenes de almacenamiento o nodos de almacenamiento a un sitio existente o añadir un sitio nuevo antes de realizar este procedimiento. Consulte las instrucciones para ampliar un sistema StorageGRID.

- 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 va a quitar contiene un nodo de puerta de enlace o un nodo de administración que se utiliza para el equilibrio de carga, es posible que deba realizar un procedimiento de expansión para agregar un nodo nuevo 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 retirada hasta que elimine estos nodos de todos los grupos de alta disponibilidad. 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 objeto que se mueva debido a los cambios realizados en la política de ILM activa. En algunos casos, es posible que deba expandir el sistema StorageGRID añadiendo nodos de almacenamiento, volúmenes de almacenamiento o nuevos sitios antes de poder completar un decomiso 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.

- Todos los nodos del sitio deben tener el estado de conexión de uno de los siguientes:
  - **Desconocido** ( ): El nodo no está conectado a la cuadrícula por una razón desconocida. Por ejemplo, se ha perdido la conexión de red entre los nodos o se ha apagado el suministro eléctrico.
  - **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 sobre los controles de consistencia cuando se quita un sitio

El nivel de coherencia de un bloque de S3 o un contenedor Swift determina si StorageGRID replica por completo los metadatos de objetos en todos los nodos y sitios antes de indicar a un cliente que la ingesta de objetos se ha realizado correctamente. Los controles de consistencia proporcionan 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 el nivel de coherencia de cada bloque 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.

Información relacionada

Cómo realiza la recuperación del sitio el soporte técnico

Gestión de objetos con ILM

Amplíe su grid

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.
`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

Descargue el paquete de recuperación

Paso 1: Seleccione Sitio

Para determinar si un sitio se puede retirar del servicio, comience por acceder al asistente del sitio de retirada.

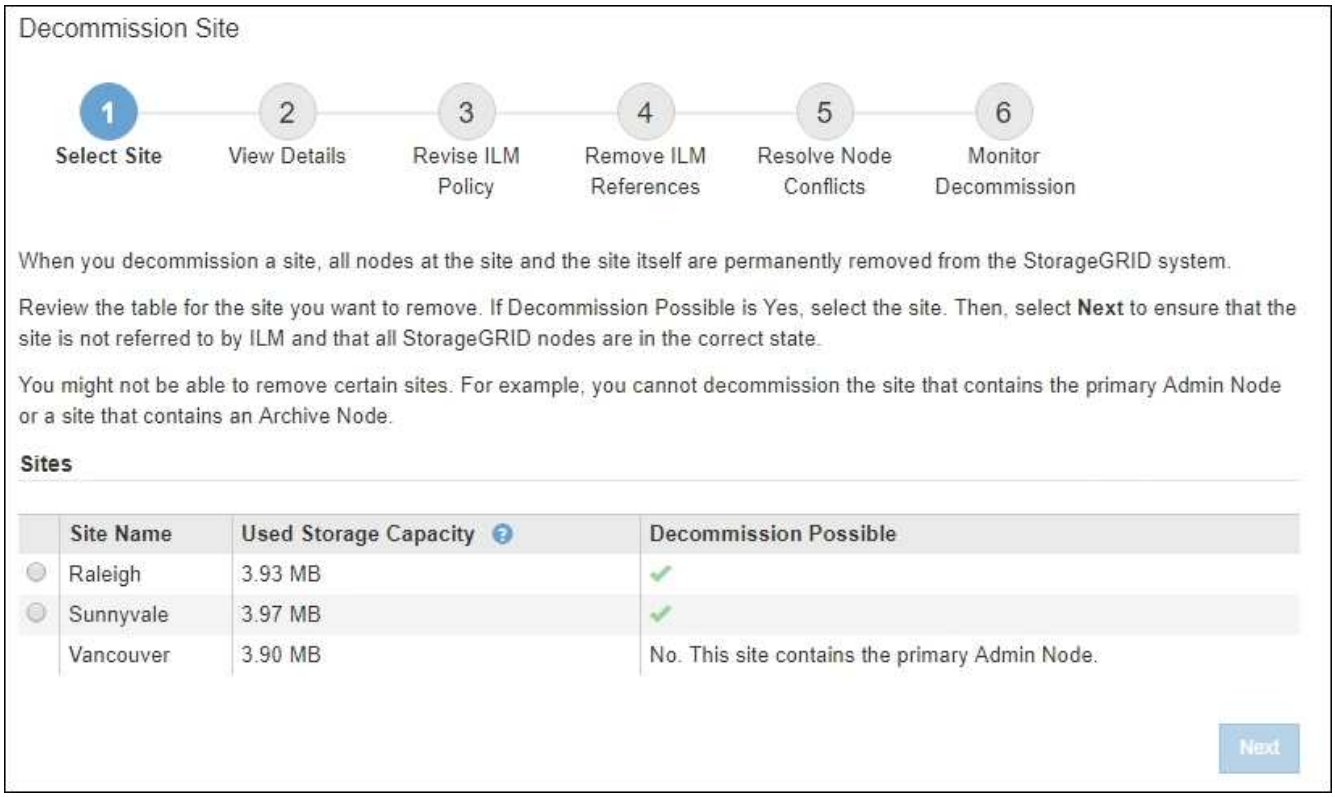
Lo que necesitará

- Usted debe haber obtenido todos los materiales requeridos.
- Debe haber revisado las consideraciones para quitar un centro.
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener los permisos de acceso raíz o Mantenimiento de la información y gestión del ciclo de vida de la información.

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 retirado, 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.

Razón posible de retirada	Descripción	Paso siguiente
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 la retirada de un 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.

Lo que necesitará

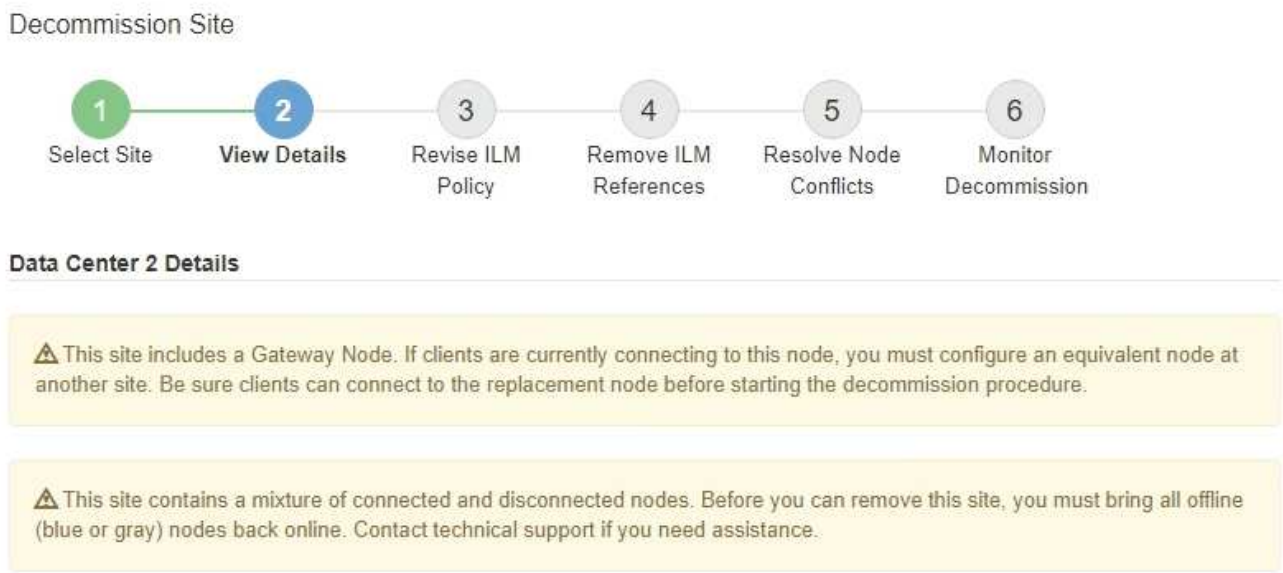
Antes de retirar un sitio, debe revisar la cantidad de datos de objeto que hay en el sitio.

- 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 de sitios desconectado, ILM no puede 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.

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.

Decommission Site

1 Select Site — 2 View Details — 3 Revise ILM Policy — 4 Remove ILM References — 5 Resolve Node Conflicts — 6 Monitor Decommission

Raleigh Details

Number of Nodes: 3
Free Space: 475.38 GB
Used Space: 3.93 MB
Site Capacity: 475.38 GB

Node Name	Node Type	Connnection State	Details
RAL-S1-101-196	Storage Node	✔	1.30 MB used space
RAL-S2-101-197	Storage Node	✔	1.30 MB used space
RAL-S3-101-198	Storage Node	✔	1.34 MB used space

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**

Previous Next

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 la retirada, debe editar grupos de alta disponibilidad para quitar todos los nodos del sitio. O bien, puede quitar el grupo de alta disponibilidad si solo incluye nodos de este sitio.

  Administre StorageGRID

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).

Información relacionada

Gestión de objetos con ILM

Paso 3: Revisar la política de ILM

En el paso 3 (revisar la política ILM) del asistente de sitio de retirada, puede determinar si la política de ILM activa hace referencia al sitio.

Lo que necesitará

Conoce el funcionamiento de ILM y está familiarizado con la creación de pools de almacenamiento, perfiles de código de borrado, reglas de ILM y la simulación y activación de una política de ILM.

Gestión de objetos con ILM

Acerca de esta tarea

StorageGRID no puede decomisionar un sitio si dicho sitio se conoce mediante cualquier regla de ILM de la

política de ILM activa.

Si su política actual de ILM hace referencia al sitio que desea quitar, debe activar una nueva política de ILM que cumpla con ciertos requisitos. En concreto, la nueva política de ILM:

- No se puede utilizar una agrupación de almacenamiento que haga referencia al sitio.
- No se puede utilizar un perfil de código de borrado que haga referencia al sitio.
- No se puede utilizar el grupo de almacenamiento * todos los nodos de almacenamiento* predeterminado o el sitio * todos los sitios* predeterminado.
- No se puede utilizar la regla de existencias **hacer 2 copias**.
- Debe estar diseñado para proteger completamente todos los datos de objetos.

> 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 un *sitio conectado Decomisión*, debe considerar cómo StorageGRID debe administrar los datos del objeto actualmente en el sitio que desea eliminar. En función de los requisitos de protección de datos, las nuevas reglas pueden mover los datos de objetos existentes a diferentes sitios o pueden eliminar las copias de objetos adicionales que ya no sean necesarias.

Póngase en contacto con el soporte técnico si necesita ayuda para diseñar la nueva política.

Pasos

1. En el paso 3 (revisar la política de ILM), determinar si alguna regla de ILM de la política activa de ILM se refiere al sitio que seleccionó para quitar.

Decommission Site

1 Select Site — 2 View Details — 3 **Revise ILM Policy** — 4 Remove ILM References — 5 Resolve Node Conflicts — 6 Monitor Decommission

If your current ILM policy refers to the site, you must activate a new policy before you can go to the next step.

The new ILM policy:

- Cannot use a storage pool that refers to the site.
- Cannot use an Erasure Coding profile that refers to the site.
- Cannot use the default **All Storage Nodes** storage pool or the default **All Sites** site.
- Cannot use the **Make 2 Copies** rule.
- Must be designed to fully protect all object data after one site is removed.

Contact technical support if you need assistance in designing the new policy.

If you are performing a connected site decommission, StorageGRID will begin to remove object data from the site as soon as you activate the new ILM policy. Moving or deleting all object copies might take weeks, but you can safely start a site decommission while object data still exists at the site.

Rules Referring to Raleigh in the Active ILM Policy

The table lists the ILM rules in the active ILM policy that refer to the site.

- If no ILM rules are listed, the active ILM policy does not refer to the site. Select **Next** to go to Step 4 (Remove ILM References).
- If one or more ILM rules are listed, you must create and activate a new policy that does not use these rules.

Active Policy Name: Data Protection for Three Sites

The active ILM policy refers to Raleigh. Before you can remove this site, you must propose and activate a new policy.

Name	EC Profiles	Storage Pools
3 copies for S3 tenant	—	Raleigh storage pool
2 copy 2 sites for smaller objects	—	Raleigh storage pool
EC for larger objects	three site EC profile	All 3 Sites

Previous Next

2. Si no aparece ninguna regla, seleccione **Siguiente** para ir al paso 4 (Eliminar referencias de ILM)

Paso 4: Eliminar referencias de ILM

3. Si una o más reglas de ILM aparecen en la tabla, seleccione el vínculo situado junto a **Nombre de directiva activa**.

   La página ILM Policies aparece en una nueva pestaña del navegador. Utilice esta pestaña para actualizar ILM. La página Sitio de retirada permanecerá abierta en la pestaña otros.

   a. Si es necesario, seleccione **ILM agrupaciones de almacenamiento** para crear una o más agrupaciones de almacenamiento que no hagan referencia al sitio.

> Para obtener más detalles, consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

b. Si planea utilizar la codificación de borrado, seleccione **ILM codificación de borrado** para crear uno o más perfiles de codificación de borrado.

   Debe seleccionar grupos de almacenamiento que no hagan referencia al sitio.

> No utilice el pool de almacenamiento **todos los nodos de almacenamiento** en los perfiles de código de borrado.

4. Seleccione **ILM Reglas** y clone cada una de las reglas enumeradas en la tabla para el paso 3 (revisar política ILM).

> Para obtener más detalles, consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

   a. Utilice nombres que facilitan la selección de estas reglas en una directiva nueva.
   b. Actualice las instrucciones de colocación.

      Quite todos los pools de almacenamiento o los perfiles de código de borrado que hagan referencia al sitio y reemplacen por nuevos pools de almacenamiento o perfiles de código de borrado.

> No utilice el pool de almacenamiento **todos los nodos de almacenamiento** en las nuevas reglas.

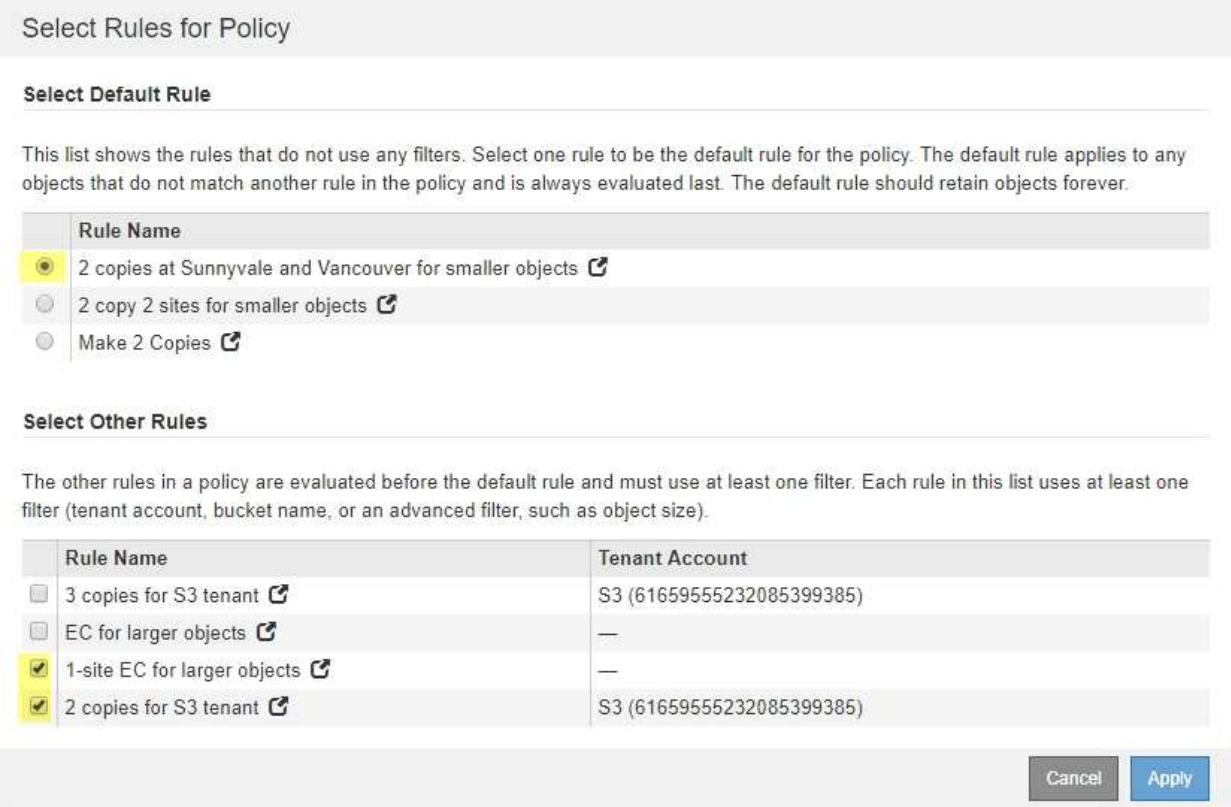
5. Seleccione **ILM políticas** y cree una nueva directiva que utilice las nuevas reglas.

> Para obtener más detalles, consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

   a. Seleccione la directiva activa y seleccione **Clonar**.
   b. Escriba un nombre de política y un motivo para el cambio.
   c. Seleccione reglas para la política clonada.
      - Deseleccione todas las reglas enumeradas para el paso 3 (revisar la política de ILM) de la página Sitio de retirada.
      - Seleccione una regla predeterminada que no haga referencia al sitio.

> No seleccione la regla **hacer 2 copias** porque esa regla utiliza el pool de almacenamiento **todos los nodos de almacenamiento**, que no está permitido.

      - Seleccione las demás reglas de reemplazo que ha creado. Estas reglas no deben referirse al sitio.



d. Seleccione **aplicar**.

e. Arrastre y suelte las filas para reordenar las reglas de la directiva.

No se puede mover la regla predeterminada.

> 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.

a. Guarde la directiva propuesta.

6. Procese objetos de prueba y simule la política propuesta para garantizar 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.

7. Activar la nueva política.

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).

8. Vuelva a **Paso 3 (revisar la política de ILM)** para asegurarse de que no haya reglas de ILM en la nueva política activa. Consulte el sitio y el botón **Siguiente** esté activado.

> Si aparece alguna regla en la lista, debe crear y activar una nueva política de ILM para poder continuar.

9. Si no aparece ninguna regla, 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 desmisión, puede quitar la directiva propuesta si existe y eliminar o editar las reglas de ILM que todavía no se utilicen en el sitio.

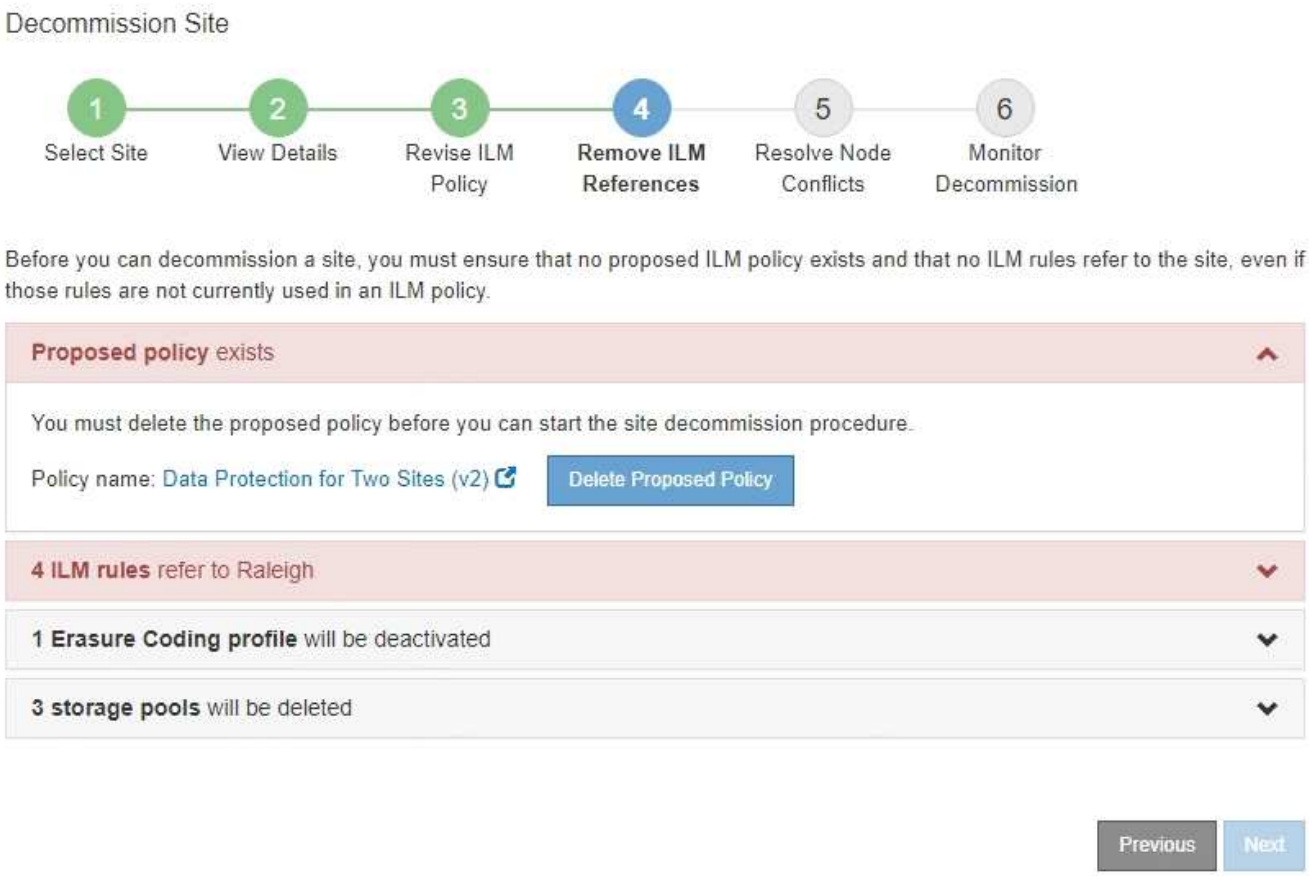
Acerca de esta tarea

Se le impide iniciar el procedimiento de retirada de instalaciones en estos casos:

- Existe una política de ILM propuesta. Si tiene una política propuesta, debe eliminarla.
- Cualquier regla de ILM se refiere al sitio, incluso si esa regla no se usa en ninguna política de ILM. Debe eliminar o editar todas las reglas que hacen referencia al sitio.

Pasos

1. Si aparece una directiva propuesta, elimínela.



a. Seleccione **Eliminar directiva propuesta**.

b. Seleccione **Aceptar** en el cuadro de diálogo de confirmación.

2. Determine si alguna regla de ILM sin usar se refiere al sitio.

Decommission Site

1 Select Site — 2 View Details — 3 Revise ILM Policy — 4 **Remove ILM References** — 5 Resolve Node Conflicts — 6 Monitor Decommission

Before you can decommission a site, you must ensure that no proposed ILM policy exists and that no ILM rules refer to the site, even if those rules are not currently used in an ILM policy.

No proposed policy exists

4 ILM rules refer to Data Center 3

This table lists the unused ILM rules that still refer to the site. For each rule listed, you must do one of the following:

- Edit the rule to remove the Erasure Coding profile or storage pool from the placement instructions.
- Delete the rule.

Go to the ILM Rules page

Name	EC Profiles	Storage Pools	Delete
Make 2 Copies	—	All Storage Nodes	
3 copies for S3 tenant	—	Raleigh storage pool	
2 copies 2 sites for smaller objects	—	Raleigh storage pool	
EC larger objects	three site EC profile	All 3 Sites	

1 Erasure Coding profile will be deactivated

3 storage pools will be deleted

Cualquier regla de ILM que se enumera sigue haciendo referencia al sitio, pero no se utiliza en ninguna política. En el ejemplo:

- La regla de stock **hacer 2 copias** utiliza la agrupación de almacenamiento predeterminada del sistema **todos los nodos de almacenamiento**, que utiliza el sitio todos los sitios.
- La regla **3 copias no utilizadas para el inquilino S3** se refiere a la piscina de almacenamiento **Raleigh**.
- La norma **2 Copy 2 no utilizada para objetos más pequeños** se refiere a la piscina de almacenamiento **Raleigh**.
- Las reglas **EC más grandes** no utilizadas utilizan el sitio de Raleigh en el perfil de codificación de borrado **todos los 3 sitios**.
- Si no aparece ninguna regla de ILM, seleccione **Siguiente** para ir a **Paso 5 (resolver conflictos de nodos)**.

Paso 5: Resolver conflictos de nodos (e iniciar retirada)

> Cuando StorageGRID destransfiere el sitio, desactiva automáticamente todos los perfiles de código de borrado que no se utilicen y hacen referencia al sitio, y elimina automáticamente todos los pools de almacenamiento no utilizados que hacen referencia al sitio. El pool de almacenamiento predeterminado del sistema todos los nodos de almacenamiento se elimina porque utiliza el sitio todos los sitios.

- Si aparece una o varias reglas de ILM, vaya al paso siguiente.

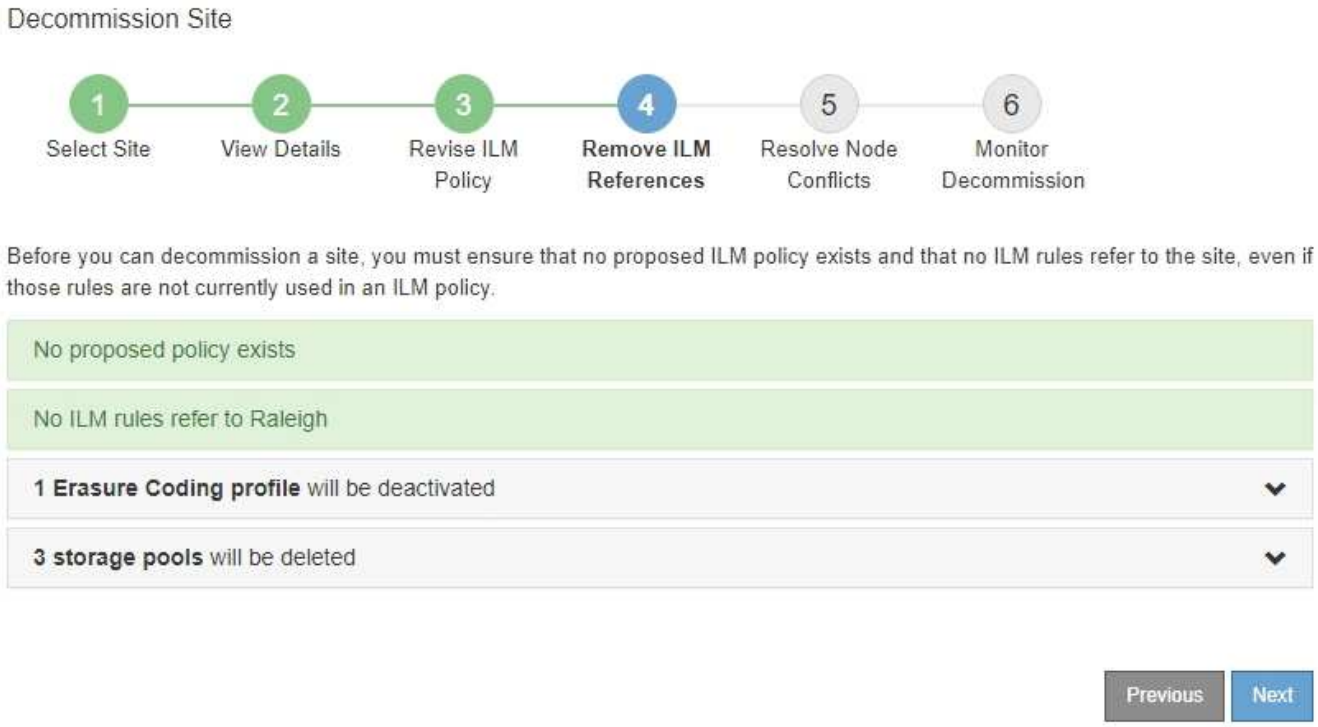
3. Edite o elimine cada regla no utilizada:
   - Para editar una regla, vaya a la página ILM Rules y actualice todas las ubicaciones que utilizan un perfil de código de borrado o un pool de almacenamiento que hace referencia al sitio. A continuación, vuelva a **Paso 4 (Eliminar referencias de ILM)**.

     > Para obtener más detalles, consulte las instrucciones para gestionar objetos con gestión del ciclo de vida de la información.

   - Para eliminar una regla, seleccione el icono de papelera Y seleccione **OK**.

     > Debe eliminar la regla de stock **hacer 2 copias** antes de poder retirar un sitio.

4. Confirme que no existe ninguna política de ILM propuesta, que no haya reglas de ILM sin usar consulte el sitio y que el botón **Siguiente** esté activado.



5. Seleccione **Siguiente**.

> Los pools de almacenamiento restantes y los perfiles de código de borrado que hacen referencia al sitio no serán válidos cuando se elimine el sitio. Cuando StorageGRID destransfiere el sitio, desactiva automáticamente todos los perfiles de código de borrado que no se utilicen y hacen referencia al sitio, y elimina automáticamente todos los pools de almacenamiento no utilizados que hacen referencia al sitio. El pool de almacenamiento predeterminado del sistema todos los nodos de almacenamiento 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.

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.

- Ningún nodo del sitio que va a quitar puede tener una interfaz que pertenezca a un grupo de alta disponibilidad.

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.

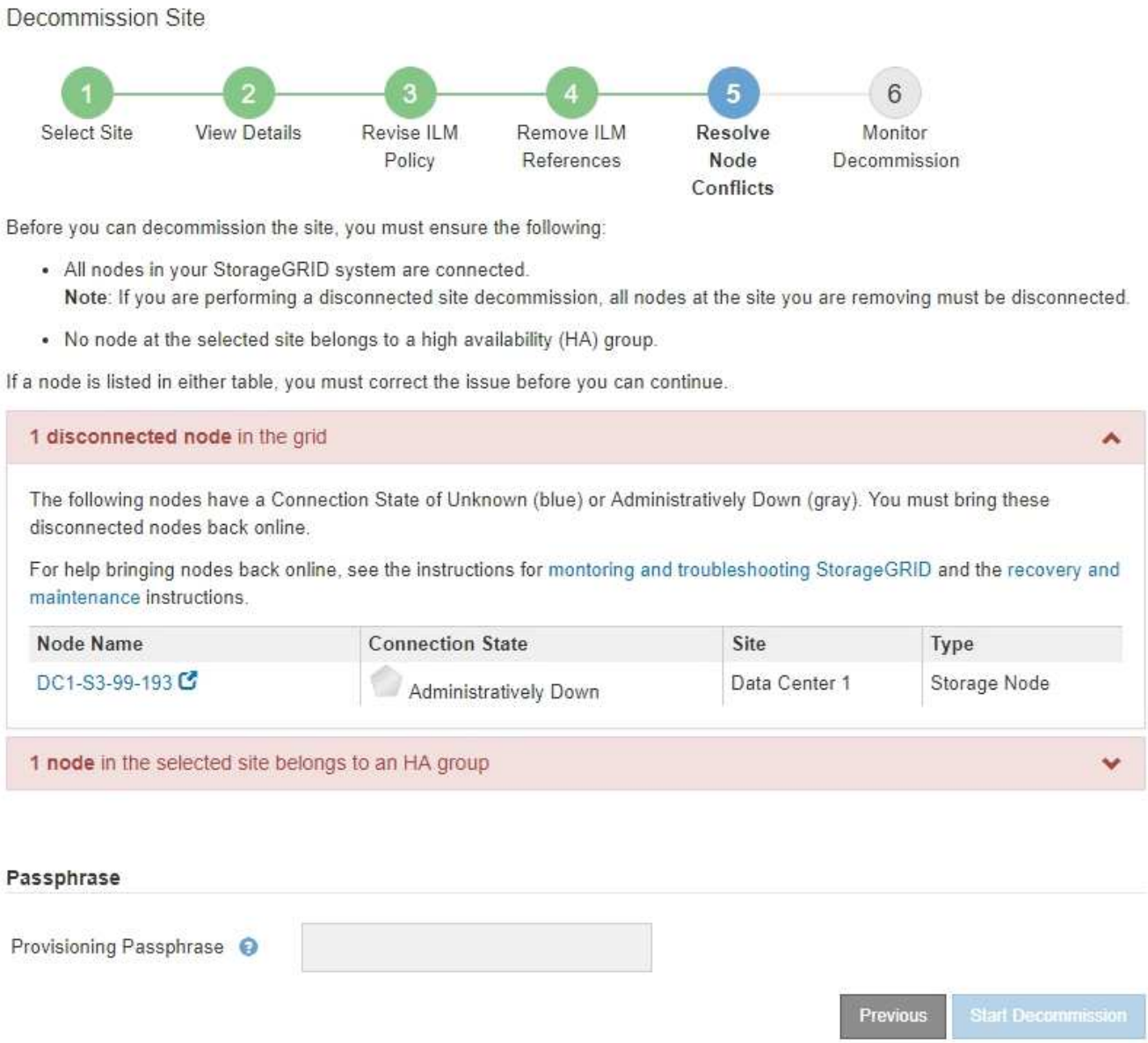
- Mientras se está ejecutando el procedimiento de retirada de instalaciones:
  - No puede crear reglas de ILM que hagan referencia al sitio que se va a retirar del servicio. Tampoco puede editar una regla de ILM existente para hacer referencia al sitio.
  - No puede realizar otros procedimientos de mantenimiento, como expansión o 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** se activa durante la fase "datos replicados y codificados 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 ( ).

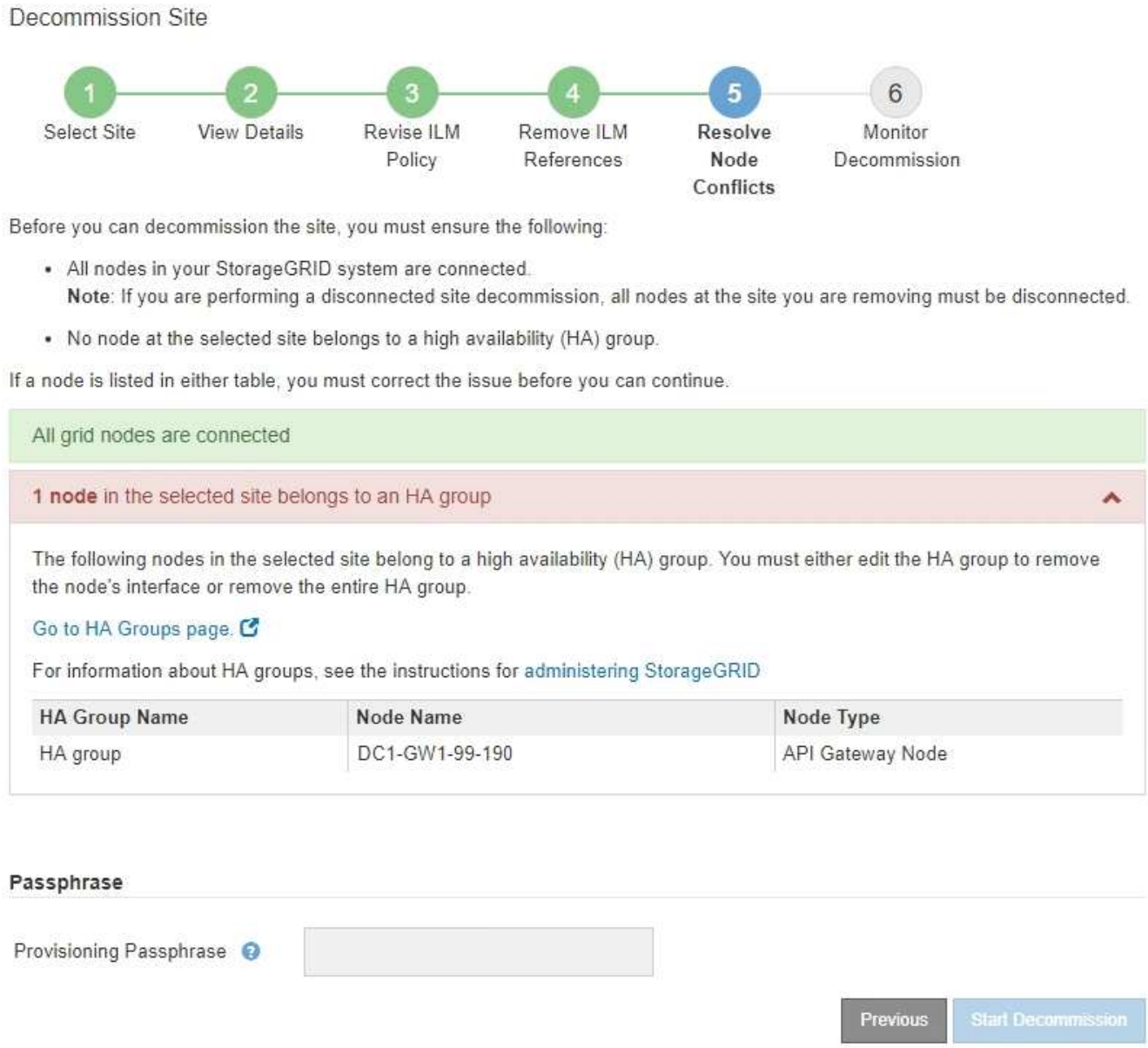


2. Si alguno de los nodos está desconectado, vuelva a ponerlos en línea.

   Consulte las instrucciones para supervisar y solucionar los problemas de StorageGRID y los procedimientos de los nodos de grid. 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.



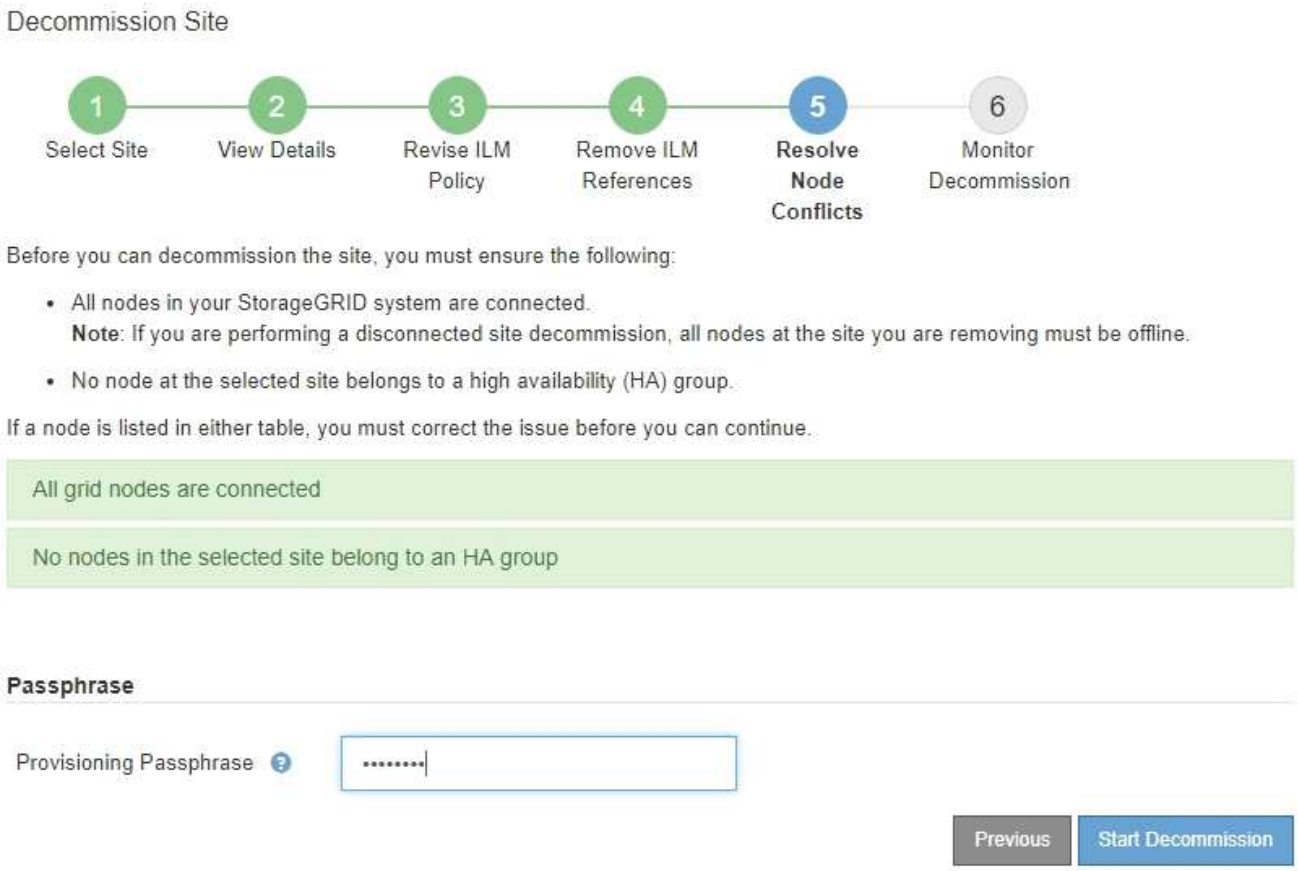
4. Si aparece algún nodo, realice una de las siguientes acciones:

   - 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.

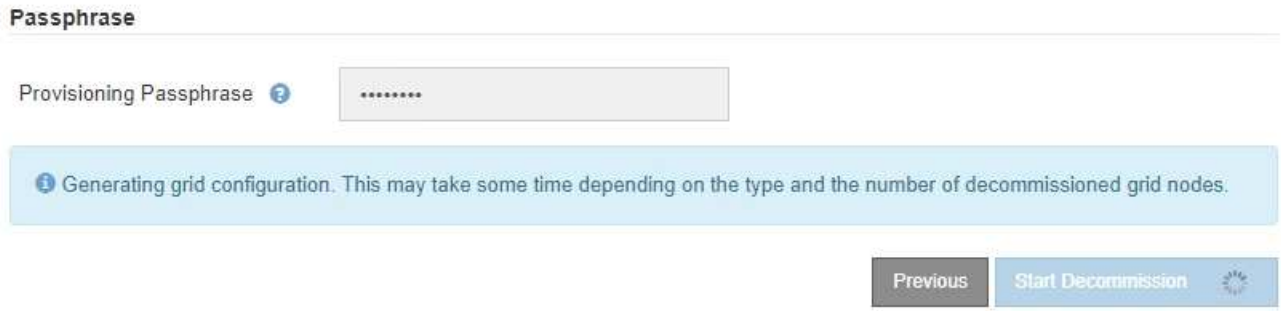


6. Si está listo para iniciar el procedimiento de retirada del sitio, seleccione **Iniciar misión**.

   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.

Información relacionada

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 vínculo en el mensaje o seleccione **MANTENIMIENTO sistema paquete de recuperación**.

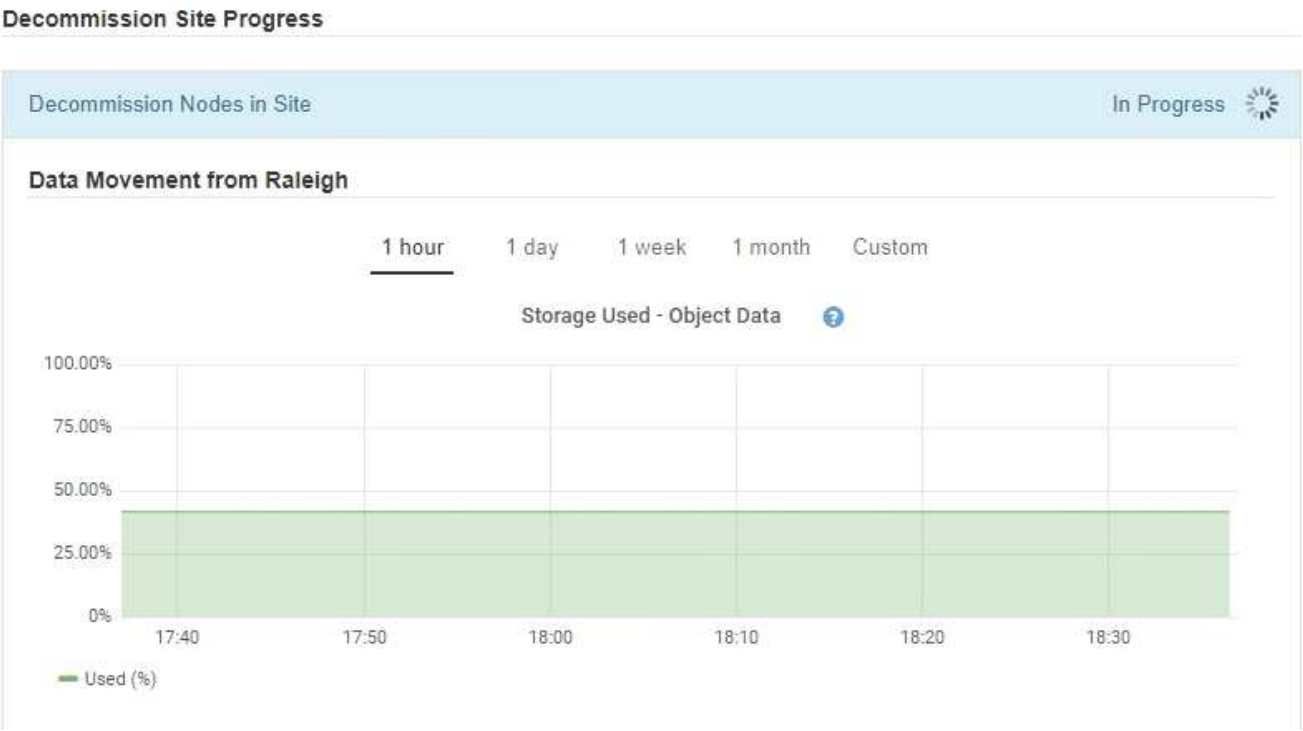
b. Descargue el `.zip` archivo.

   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.

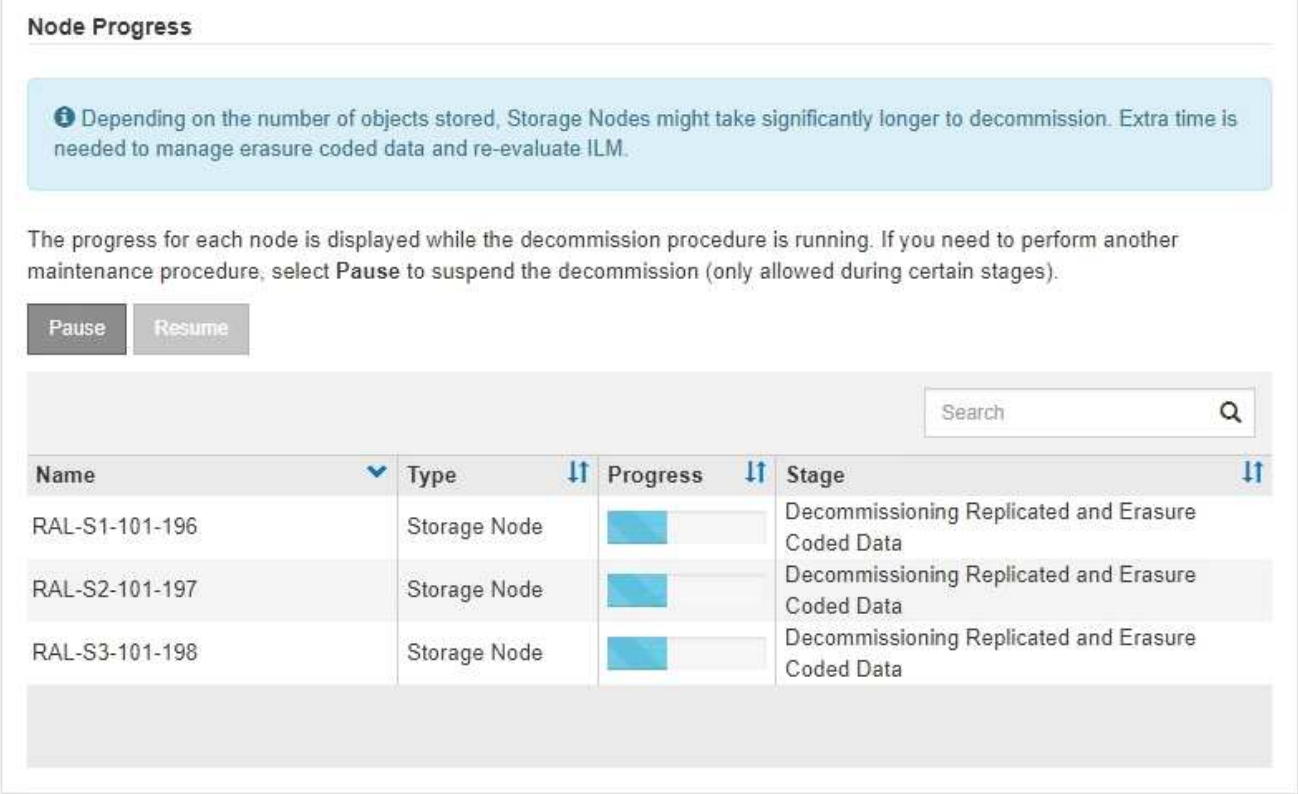
2. Con el gráfico de movimiento de datos, supervise el movimiento de datos de objetos desde este sitio a otros sitios.

   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.



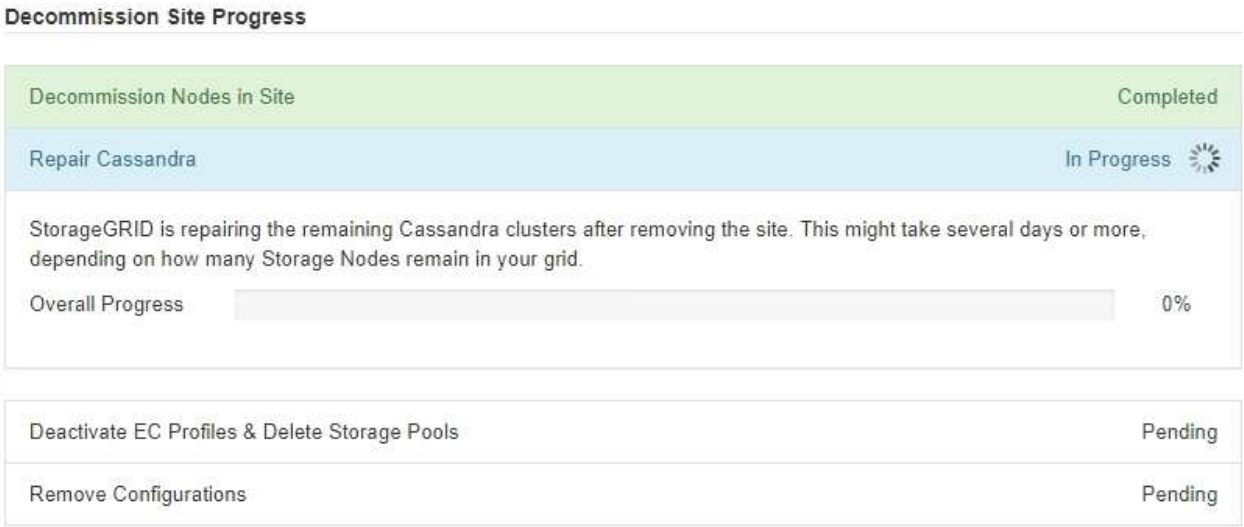
Si va a supervisar el progreso de una retirada de sitios conectados, consulte esta tabla para comprender las etapas de retirada de un nodo de almacenamiento:

Etapa	Duración estimada
Pendiente	Minuto o menos
Espere a que se bloqueen	Minutos
Preparar tarea	Minuto o menos
Marcado de LDR retirado	Minutos
Decomisionado de datos replicados y 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.

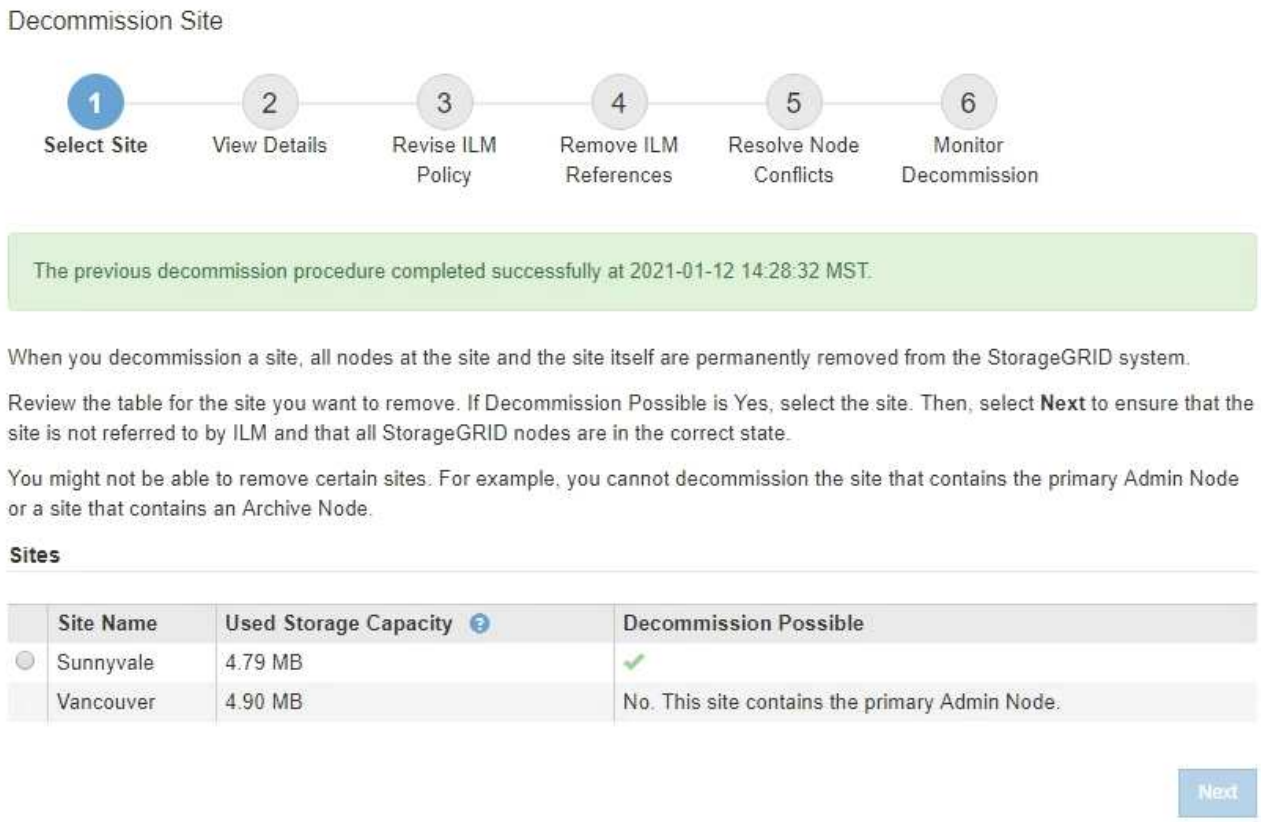


   - Durante el paso **Desactivar perfiles de EC Eliminar agrupaciones de almacenamiento**, se realizan los siguientes cambios de ILM:
     - Los perfiles de código de borrado que hacen referencia a la planta se desactivan.
     - Los pools de almacenamiento a los que se hace referencia el sitio se eliminan.

> El pool de almacenamiento predeterminado del sistema All Storage Nodes también se quita porque utiliza el sitio All Sites.

- 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.

Procedimientos de mantenimiento 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.

Lo que necesitará

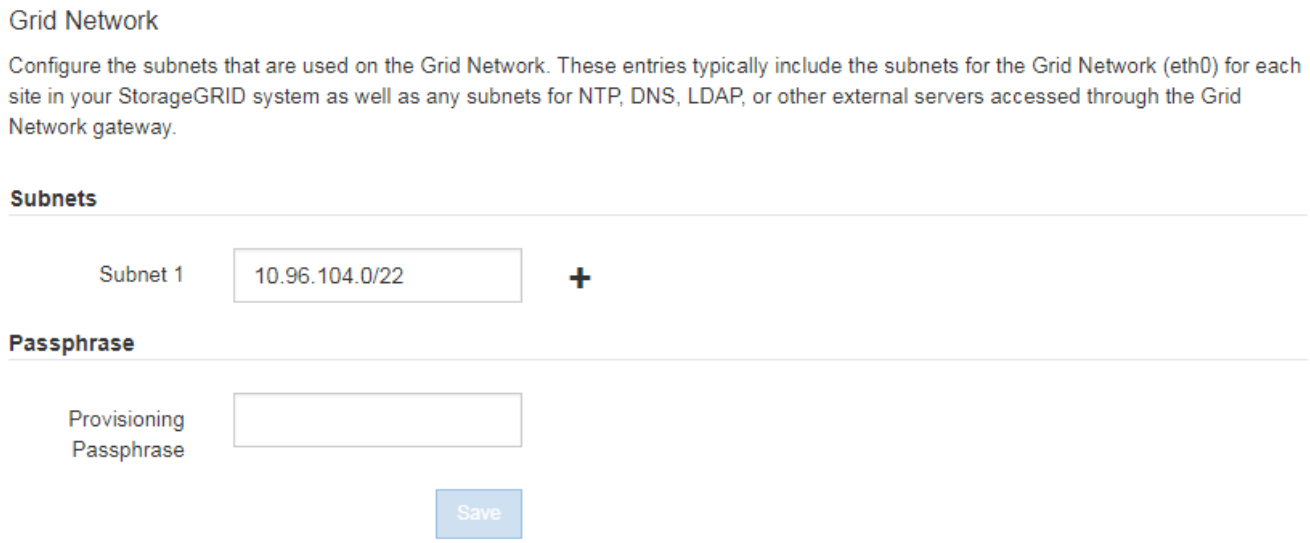
- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener los permisos de mantenimiento o acceso raíz.
- Debe tener la clave de acceso de aprovisionamiento.
- Debe tener las direcciones de red, en notación CIDR, de las subredes que desea configurar.

Acerca de esta tarea

Si está realizando una actividad de expansión que incluye la adición de una nueva subred, debe agregar la nueva subred de cuadrícula antes de iniciar el procedimiento de expansión.

Pasos

1. Seleccione **MANTENIMIENTO** > **Red** > **Red de red**.



2. En la lista subredes, haga clic en el signo más para añadir una nueva subred en notación CIDR.

   Por ejemplo, introduzca `10.96.104.0/22`.

3. Introduzca la frase de acceso de aprovisionamiento y haga clic en **Guardar**.

   Las subredes que ha especificado se configuran automáticamente para el sistema StorageGRID.

4. Descargue un nuevo paquete de recuperación desde Grid Manager.
   a. Seleccione **MANTENIMIENTO** > **sistema** > **paquete de recuperación**.
   b. Introduzca la clave de acceso de aprovisionamiento.

Configurar las direcciones IP

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.

> 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.

> 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.

> 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.

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 ficha **SSM Recursos** puede mostrar la dirección IP de red de cliente, administrador y cuadrícula asignada a otras interfaces además de eth0, eth1 o eth2.

DHCP

DHCP solo puede configurarse durante la fase de implementación. No es posible 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 incluida en un grupo ha, no puede cambiar la dirección IP de red del cliente para esa interfaz a una dirección que esté fuera de la subred configurada para el grupo ha.
- No puede cambiar la dirección IP de la red de cliente por el valor de una dirección IP virtual existente asignada a un grupo ha configurado en la interfaz de la red de cliente.
- Si una interfaz de red de cuadrícula está incluida en un grupo ha, no puede cambiar la dirección IP de red de cuadrícula de esa interfaz a una dirección que esté fuera de la subred configurada para el grupo ha.
- No puede cambiar la dirección IP de red de red de red por el valor de una dirección IP virtual existente asignada a un grupo ha configurado en la interfaz de red de red de red.

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.

Lo que necesitará

Debe tener 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 el sistema operativo Linux.

Dispositivos: en los dispositivos StorageGRID, si la red cliente o administrador no estaba configurada en el instalador del dispositivo StorageGRID durante la instalación inicial, la red no se puede agregar utilizando sólo 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 el procedimiento para configurar los enlaces de red en las instrucciones de instalación y mantenimiento del dispositivo.

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 quitar de la red de cuadrícula.

> No se permiten intercambios de direcciones IP. 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 administrar StorageGRID.

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.

```
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. 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 la selección, el mensaje muestra el nombre del nodo, el nombre de red (Grid, Admin o Cliente), el tipo de datos (IP/máscara, 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 infringen las reglas de las redes Grid, Admin y Client, como no utilizar subredes superpuestas.

   En este ejemplo, la validación devolvió errores.

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   En este ejemplo, se ha aprobado la validación.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

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.

   - **CANCEL**: No realice ningún cambio en la 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 organizar los cambios en la configuración, se genera un nuevo paquete de recuperación como resultado del cambio de configuración de la 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 va a agregar el nodo a una red administrativa o a una red cliente por primera vez, asegúrese de que ha añadido la interfaz como se describe en ""adición de interfaces a un 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.

Información relacionada

Linux: Añadir interfaces al nodo existente

Instale Red Hat Enterprise Linux o CentOS

Instalar Ubuntu o Debian

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Administre StorageGRID

Configurar las direcciones IP

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.

Lo que necesitará

- Debe tener 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'" permanezca seleccionado. 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 utilizando "'flecha arriba'" para recuperar los valores escritos previamente en el indicador 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 ha seleccionado cualquiera de los modos de selección "todos" en el paso 2, debe pulsar **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 are not
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
are not 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 do not 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 conservará después de aplicar los cambios en 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 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.

Información relacionada

Configurar las direcciones IP

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.

Lo que necesitará

- Debe tener 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 utilizando "'flecha arriba'" para recuperar los valores escritos previamente en el indicador 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:

```
Grid Network Subnet List (GNSL)
                                                    add 172.30.0.0/21
                                                    add 172.31.0.0/21
                                                    del 172.16.0.0/21
                                                    del 172.17.0.0/21
                                                    del 172.18.0.0/21
                                [      172.30.0.0/21 ]
                                [      172.31.0.0/21 ]
                                [     192.168.0.0/21 ]
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).

  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 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**, debe reiniciar el nodo Lo antes posible. después de la configuración provisional para minimizar las interrupciones.

- **CANCEL**: No realice ningún cambio en la 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 organizar los cambios en la configuración, se genera un nuevo paquete de recuperación como resultado del cambio de configuración de la cuadrícula.

12. Si la configuración se detiene debido a errores, están disponibles las siguientes opciones:
    - Para cancelar 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.

Información relacionada

Configurar las direcciones IP

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 puede cambiar la IP de red de cuadrícula utilizando el procedimiento para cambiar nodos individuales.

Lo que necesitará

- Debe tener la `Passwords.txt` archivo.

Para asegurarse de que la cuadrícula se inicia correctamente, debe realizar todos los cambios a la vez.

> Este procedimiento se aplica sólo a la red de cuadrícula. Este procedimiento no se puede utilizar para cambiar direcciones IP en las redes de administración o de 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 las instrucciones para administrar StorageGRID.

   > 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`.

```
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:
```

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:

```
=========================================================================
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 infringen las reglas de la red de cuadrícula, como no utilizar subredes superpuestas.

   En este ejemplo, la validación devolvió errores.

```
Validating new networking configuration... FAILED.

  DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
  DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

   En este ejemplo, se ha aprobado la validación.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

8. Una vez superada 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 de operación, ya sea manualmente o seleccionando **aplicar** en lugar de **fase**; 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.

> Toda la cuadrícula debe apagarse a la vez, para 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. Una vez que el grid se inicia 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

Administre StorageGRID

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:

- Instale Red Hat Enterprise Linux o CentOS
- Instalar 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.

Lo que necesitará

- Tiene acceso a las instrucciones para instalar StorageGRID en su plataforma Linux.
  - Instale Red Hat Enterprise Linux o CentOS
  - Instalar Ubuntu o Debian
- Usted tiene la `Passwords.txt` archivo.
- Tiene permisos de acceso específicos.

No intente añadir 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 agregar 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.

   ```
   INTERFACES_TARGET_nnnn=value
   ```

   Para *nnnn*, especifique un número único para cada uno `INTERFACES_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:

   ```
   INTERFACES_TARGET_01=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.

Lo que necesitará

- Tiene acceso a las instrucciones para instalar StorageGRID en su plataforma VMware.

Instale VMware

- Configuró StorageGRID 11.6.
- Tiene máquinas virtuales VMware Node de administrador y Gateway Node.
- Tiene una subred de red que no se está utilizando como red Grid, Admin o Client.
- Usted tiene la `Passwords.txt` archivo.
- Tiene permisos de acceso específicos.

> No intente añadir interfaces a un nodo mientras haya una actualización de software, un procedimiento de recuperación o un procedimiento de expansión activo.

Acerca de esta tarea

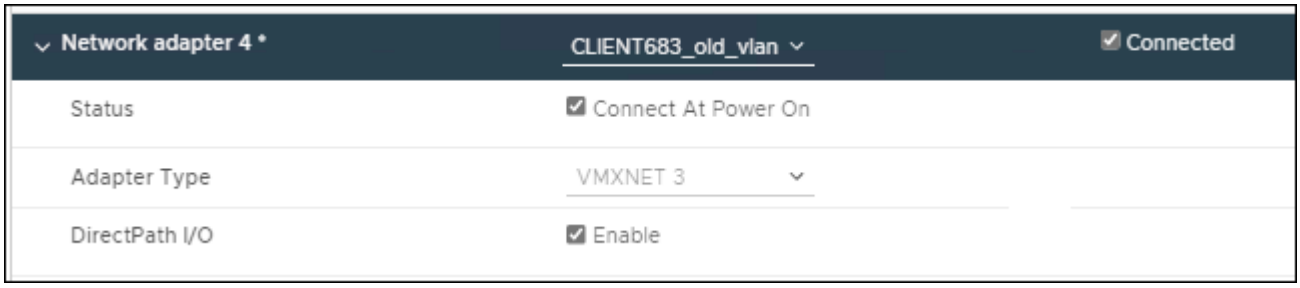
Siga estos pasos para añadir una o varias interfaces adicionales a un nodo de VMware después de instalar el nodo. Por ejemplo, es posible que desee agregar una interfaz troncal a un nodo de administración o puerta de enlace, de modo que pueda utilizar interfaces VLAN para separar el tráfico que pertenece 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 agregar 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 **conectado** y **conectar al encender**.



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.

Configure los servidores DNS

Puede agregar, quitar y actualizar servidores de sistema de nombres de dominio (DNS) para poder usar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener los permisos de mantenimiento o acceso raíz.
- Debe tener las direcciones IP de los servidores DNS para configurar.

Al especificar información del servidor DNS, se pueden utilizar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP para notificaciones por correo electrónico o SNMP y AutoSupport. Se recomienda especificar al menos dos servidores DNS.

> Proporcione entre dos y seis direcciones IP para los servidores DNS. En general, seleccione los servidores DNS a los que cada sitio puede acceder localmente en el caso de que la red sea Landing. Esto es para asegurar que un sitio de llanded siga teniendo acceso al servicio DNS. Después de configurar la lista de servidores DNS de toda la cuadrícula, puede Personalice aún más la lista de servidores DNS para cada nodo.

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. Seleccione **MANTENIMIENTO Red servidores DNS**.
2. En la sección servidores, agregue actualizaciones o elimine las entradas del servidor DNS, según sea necesario.

   La práctica recomendada es especificar al menos dos servidores DNS por sitio. Puede especificar hasta seis servidores DNS.

3. Haga clic en **Guardar**.

Modifique la configuración de DNS para un solo nodo de grid

En lugar de configurar el sistema de nombres de dominio (DNS) globalmente para toda la implementación, puede ejecutar un script para configurar DNS de forma diferente para cada nodo de cuadrícula.

En general, debe utilizar la opción **MAMAINTENANCE Network DNS Servers** en Grid Manager para configurar servidores DNS. Utilice la siguiente secuencia de comandos sólo si necesita usar servidores DNS diferentes para nodos de cuadrícula diferentes.

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`

Configure los servidores NTP

Puede agregar, actualizar o eliminar servidores de protocolo de tiempo de redes (NTP) para garantizar que los datos se sincronizan con precisión entre los nodos de grid en el sistema StorageGRID.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un navegador web compatible.
- Debe tener los permisos de mantenimiento o acceso raíz.
- Debe tener la clave de acceso de aprovisionamiento.
- Debe tener las direcciones IPv4 de los servidores NTP para configurar.

Acerca de esta tarea

El sistema StorageGRID utiliza el protocolo de hora de red (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 previamente roles NTP principales. Por este motivo, se recomienda especificar al menos dos nodos con roles NTP principales.

> 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.

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

"Límite de soporte para configurar el servicio de tiempo de Windows para entornos de alta precisión"

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.

Pasos

1. Seleccione **MANTENIMIENTO Red servidores NTP**.

2. En la sección Servers, añada la actualización o elimine las entradas del servidor NTP, según sea necesario.

   Debe incluir al menos 4 servidores NTP y especificar hasta 6 servidores.

3. En el cuadro de texto **frase de paso de aprovisionamiento**, introduzca la contraseña de aprovisionamiento del sistema StorageGRID y haga clic en **Guardar**.

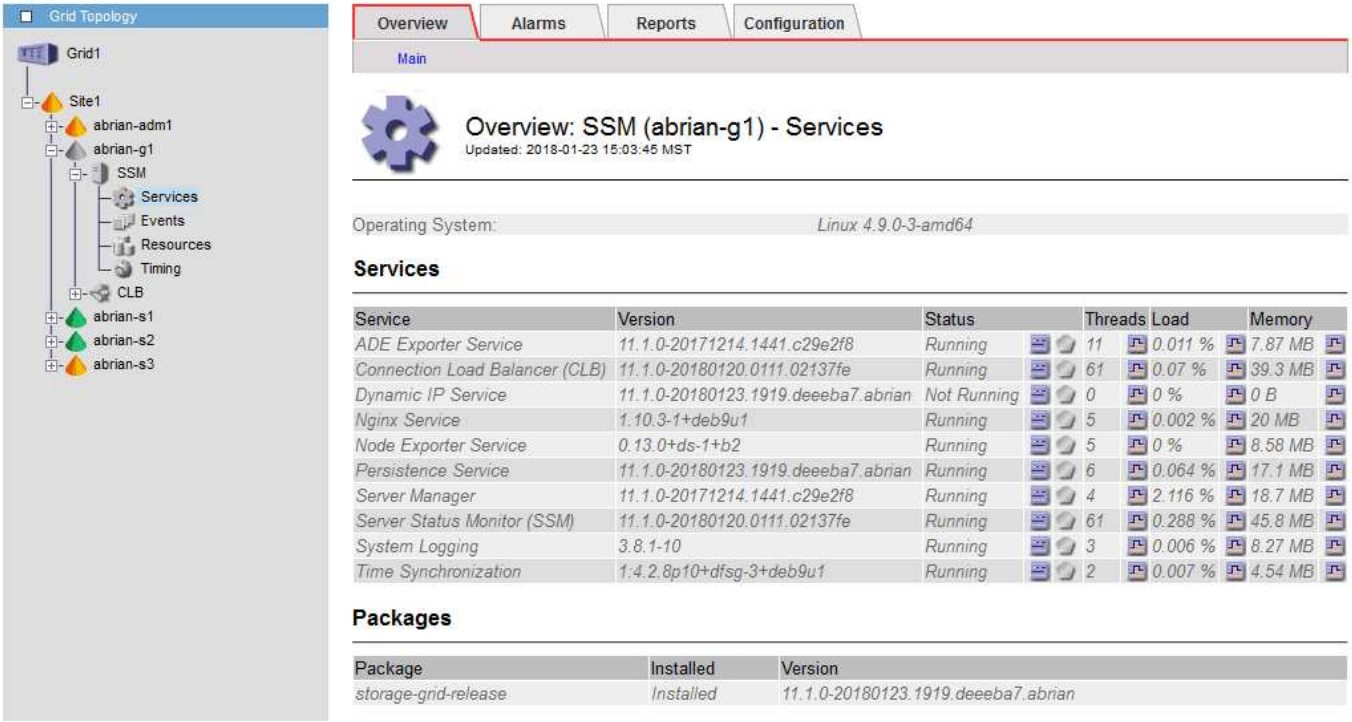
   El estado del procedimiento se muestra en la parte superior de la página. La página está deshabilitada hasta que se completen las actualizaciones de configuración.

   > Si todos los servidores NTP fallan en la prueba de conexión después de guardar los nuevos servidores NTP, no continúe. Póngase en contacto con el soporte técnico.

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.

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 uso y cuota de almacenamiento que se muestran en la consola para el 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 multicast (mDNS) está deshabilitado en las redes, puede que sea necesario ejecutar la utilidad de línea de comandos en cada nodo aislado.

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 may 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 IP dinámico es "'en ejecución'" después de ejecutar `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 middleware y a nivel de host

Algunos procedimientos de mantenimiento son específicos de las implementaciones de

StorageGRID para Linux o VMware o son específicos de otros componentes de la solución StorageGRID.

Linux: Migre el nodo de grid a un nuevo host

Puede migrar nodos StorageGRID de un host Linux a otro para realizar tareas de mantenimiento del host (como parches y reinicio del SO) sin afectar a la funcionalidad o disponibilidad del grid.

Se migran uno o más nodos de un host Linux (el «host de origen») a otro host Linux (el «host objetivo»). El host de destino debe haber sido preparado previamente para el uso de StorageGRID.

> Puede utilizar este procedimiento solo si ha planificado la implementación de StorageGRID para incluir soporte de migración.

Para migrar un nodo de cuadrícula a un host nuevo, se deben cumplir ambas condiciones:

- 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 puesta en marcha 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 (por ejemplo, dos nodos de puerta de enlace), no instale todas las instancias en el mismo host.

Para obtener más información, consulte «"requisitos de migración de nodos" en las instrucciones de instalación de StorageGRID del sistema operativo Linux.

Información relacionada

Implemente nuevos hosts Linux

Instale Red Hat Enterprise Linux o CentOS

Instalar Ubuntu o Debian

Linux: Exportar el nodo del host de origen

Apague el nodo de grid y lo exporte desde el host Linux de origen.

Ejecute el siguiente comando en el host Linux de origen.

1. Obtenga el estado de todos los nodos que actualmente se ejecutan en el host de origen.

```
sudo storagegrid node status all
```

```
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 deténtelo si está su estado Run `Running`.

```
sudo storagegrid node stop DC1-S3
```

```
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
```

```
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 command suggested in the output of the `export` comando.

   Este comando se ejecutará en el host de destino en el paso siguiente.

Linux: Importe el nodo en el host de destino

Después de exportar el nodo desde el host de origen, importe y valide el nodo en el host Linux 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 el siguiente comando en el host Linux de destino.

1. Importe el nodo en el host de destino.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

```
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
```

```
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.

Información relacionada

Instale Red Hat Enterprise Linux o CentOS

Instalar Ubuntu o Debian

Linux: Inicie el nodo migrado

Después de validar el nodo migrado, debe iniciar el nodo ejecutando un comando en el host Linux de destino.

Pasos

1. Inicie el nodo en el host nuevo.

```
sudo storagegrid node start DC1-S3
Starting node DC1-S3
```

2. En Grid Manager, compruebe que el estado del nodo es verde sin que se le hayan generado alarmas.

   > 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 los nodos adicionales de forma que no tendrá más de un nodo fuera de servicio.

   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 el estado Run of `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 configurado, el destino de un nodo de archivado no se puede cambiar.

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.

Lo que necesitará

Debe iniciar 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 copia de objeto única y no puede recuperarse la copia, el objeto se pierde y no se puede recuperar. Sin embargo, debe seguir el procedimiento para determinar si el objeto no está disponible de forma permanente para "'limpiar'" el sistema StorageGRID, para cancelar la solicitud del nodo de archivado y para purgar 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.

Lo que necesitará

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la dirección IP de un nodo de administrador.

Acerca de esta tarea

Este ejemplo solo se proporciona para su información; este procedimiento no puede ayudarle a identificar todas las condiciones de fallo que pueden 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/audit/export`

      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 no se puede recuperar un objeto de un nodo de archivado, el mensaje de auditoría ARCE (fin de recuperación de objeto de archivado) muestra ARUN (middleware de archivado 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 igual que el ID de volumen del nodo de archivado (o TSM "'nombre de nivel superior'") seguido del CBID del objeto (o TSM "'nombre de nivel bajo'"). 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 todavía 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 desde TSM.

Si las únicas copias del objeto se encuentran en cinta, la solicitud de «recuperación masiva» se cancela con un mensaje «"1 solicitudes canceladas»». Si hay 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 desde el 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 del objeto especifica que solo se debe realizar una copia y que ahora se ha perdido esa copia, el objeto no puede recuperarse. 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.

Procedimientos de los nodos de grid

Es posible que deba realizar procedimientos en un nodo de grid específico. Aunque puede realizar algunos de estos procedimientos desde Grid Manager, la mayoría de los procedimientos requieren que acceda a Server Manager desde la línea de comandos del nodo.

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.

> 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`

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.

Lo que necesitará

Debe tener 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.

Lo que necesitará

Debe tener 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.

```
Host Name                      190-ADM1
IP Address
Operating System Kernel        4.9.0          Verified
Operating System Environment   Debian 9.4     Verified
StorageGRID Webscale Release   11.1.0         Verified
Networking                                    Verified
Storage Subsystem                             Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.1.0         Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.1.0         Running
cmn                            11.1.0         Running
nms                            11.1.0         Running
ssm                            11.1.0         Running
mi                             11.1.0         Running
dynip                          11.1.0         Running
nginx                          1.10.3         Running
tomcat                         8.5.14         Running
grafana                        4.2.0          Running
mgmt api                       11.1.0         Running
prometheus                     1.5.2+ds       Running
persistence                    11.1.0         Running
ade exporter                   11.1.0         Running
attrDownPurge                  11.1.0         Running
attrDownSamp1                  11.1.0         Running
attrDownSamp2                  11.1.0         Running
node exporter                  0.13.0+ds      Running
```

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.

Lo que necesitará

Debe tener 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.

Lo que necesitará

Debe tener 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.

Lo que necesitará

Debe tener 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.

Lo que necesitará

Debe tener 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 la cuadrícula: '**service *serviceename* status** se informa del estado actual del servicio solicitado que se ejecuta en el nodo de la 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.

Lo que necesitará

Debe tener la `Passwords.txt` archivo.

Acerca de esta tarea

Cuando utilice estos pasos para «'detener administrativamente» un servicio, Server Manager 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

Coloque el dispositivo en modo de mantenimiento

Debe colocar el aparato en modo de mantenimiento antes de realizar procedimientos de mantenimiento específicos.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso de mantenimiento o acceso raíz. Para obtener más detalles, consulte las instrucciones para administrar StorageGRID.

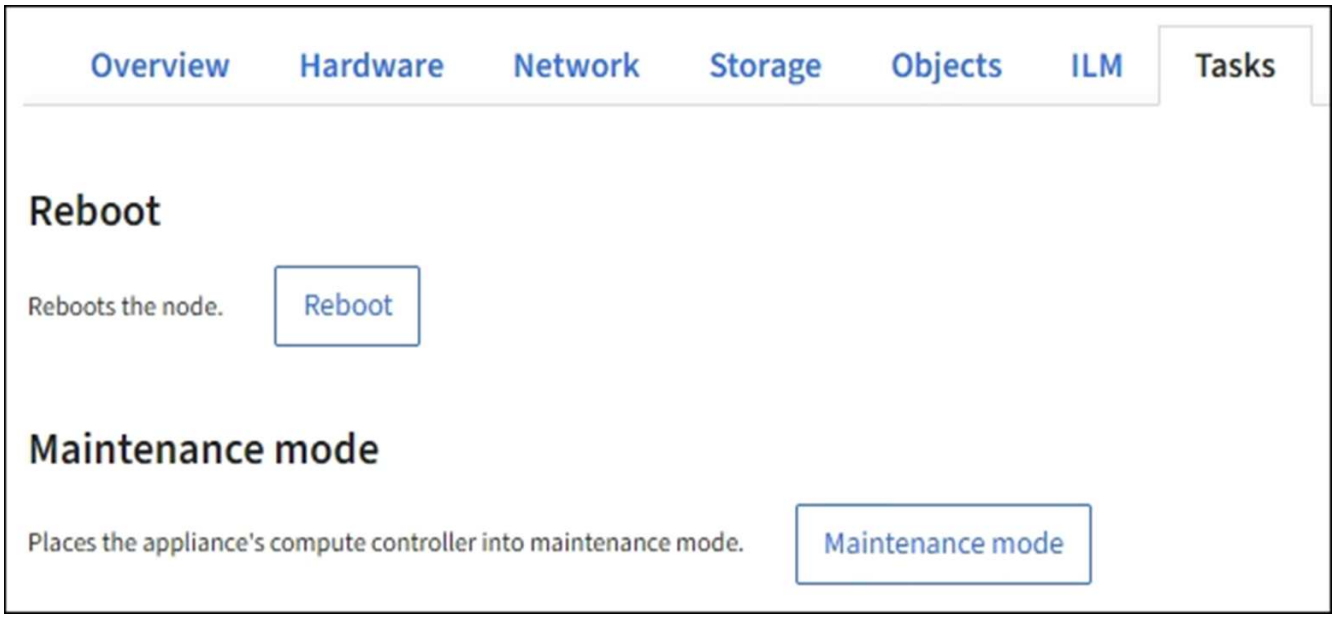
Acerca de esta tarea

En raras ocasiones, una vez que se coloca un dispositivo StorageGRID en modo de mantenimiento puede hacer que el dispositivo no esté disponible para el acceso remoto.

La contraseña de la cuenta de administrador y las claves de host SSH para un dispositivo StorageGRID en modo de mantenimiento siguen siendo las mismas que en el momento en que el dispositivo estaba en servicio.

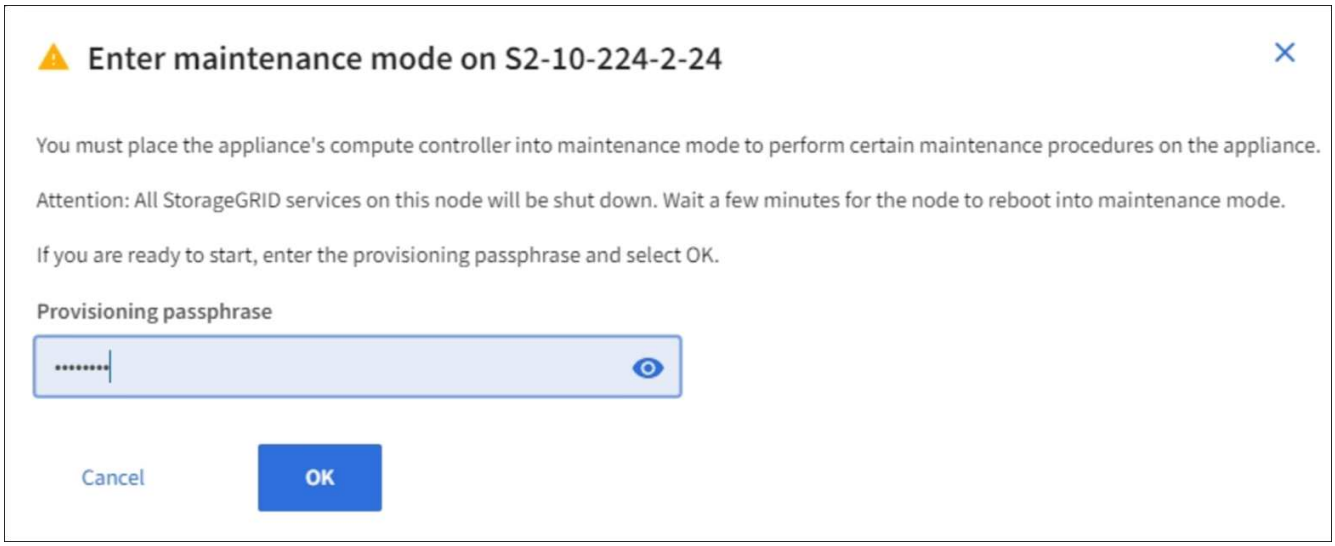
Pasos

1. En Grid Manager, seleccione **NODES**.
2. En la vista de árbol de la página Nodes, seleccione Appliance Storage Node.
3. Seleccione **tareas**.



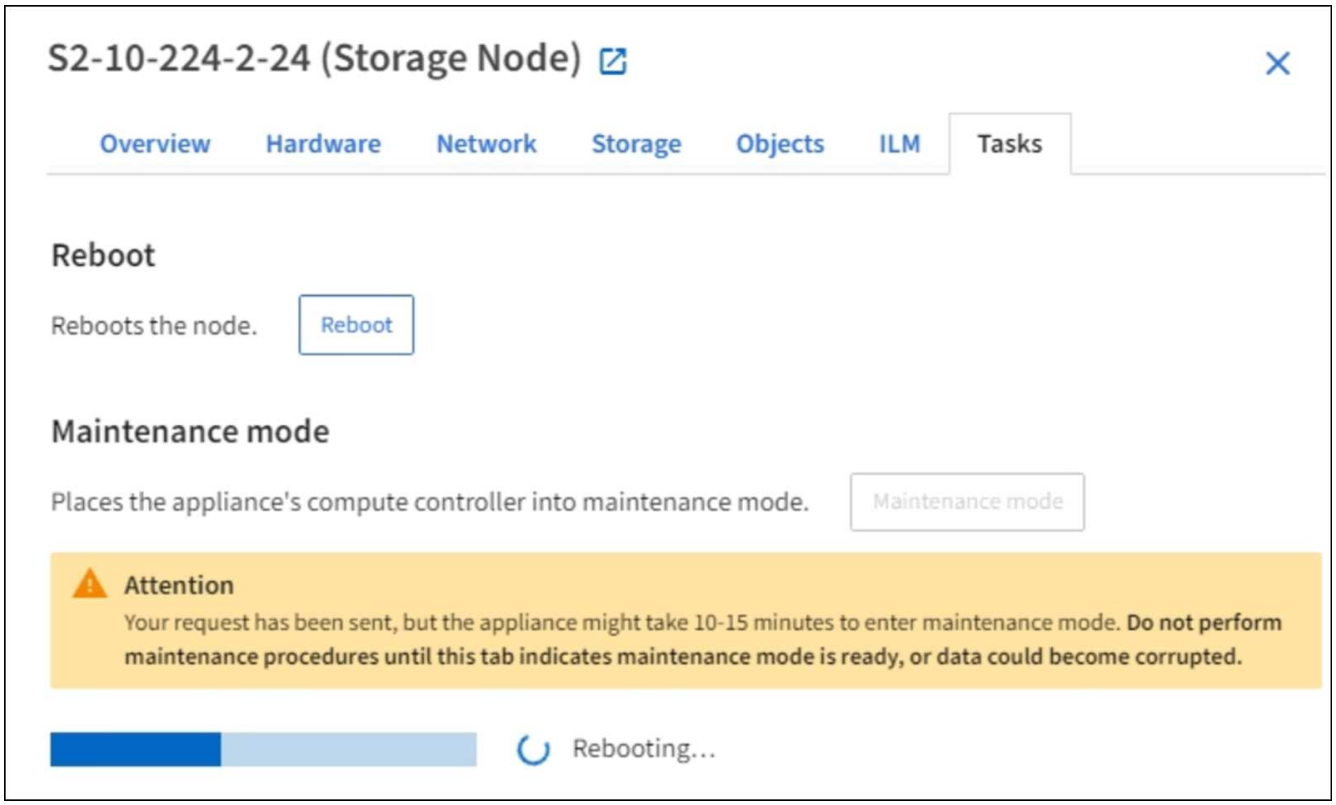
4. Seleccione **modo de mantenimiento**.

   Se muestra un cuadro de diálogo de confirmación.

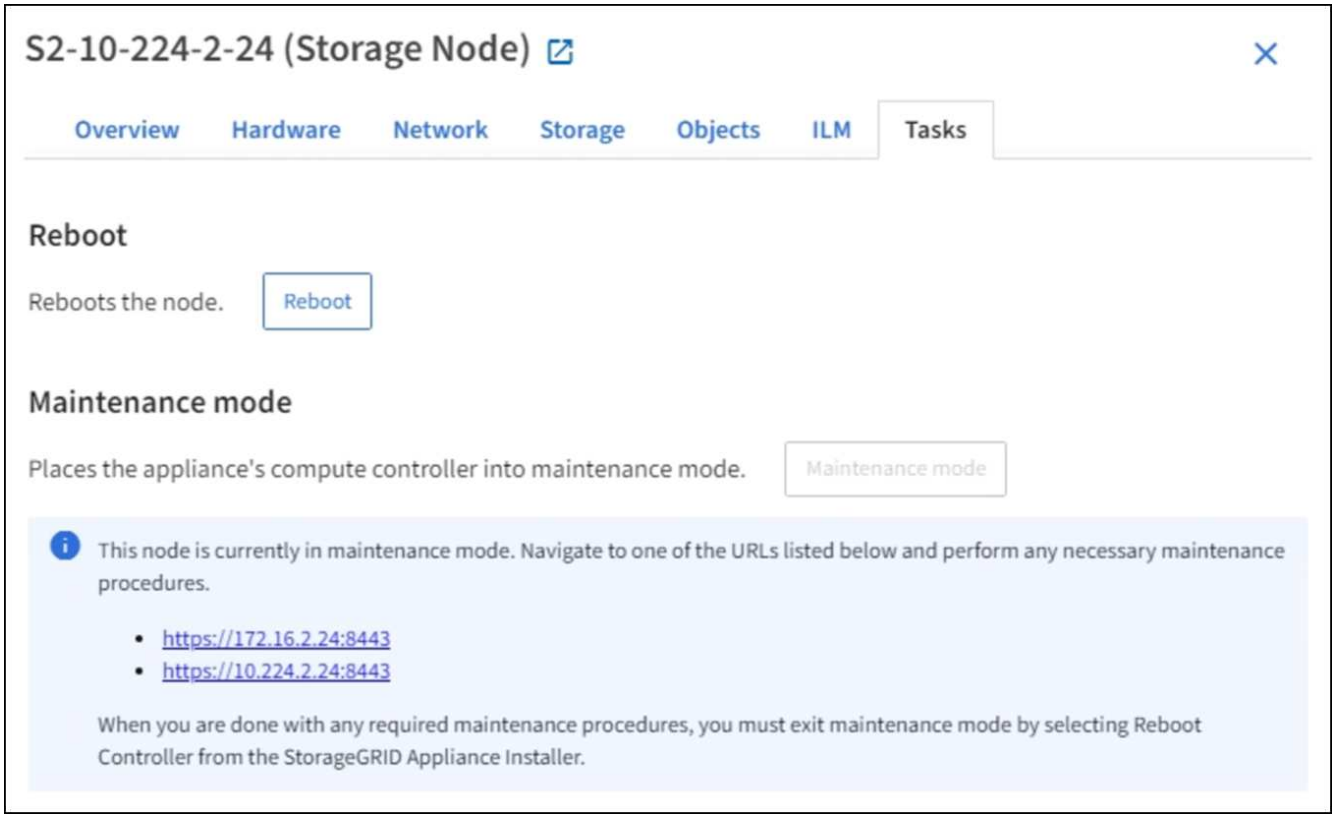


5. Introduzca la contraseña de aprovisionamiento y seleccione **Aceptar**.

   Una barra de progreso y una serie de mensajes, incluidos "solicitud enviada", "detención de StorageGRID" y "reinicio", indican que el dispositivo está llevando a cabo los pasos necesarios para entrar en el modo de mantenimiento.



Cuando el dispositivo se encuentra en modo de mantenimiento, un mensaje de confirmación enumera las URL que puede utilizar para acceder al instalador de dispositivos de StorageGRID.



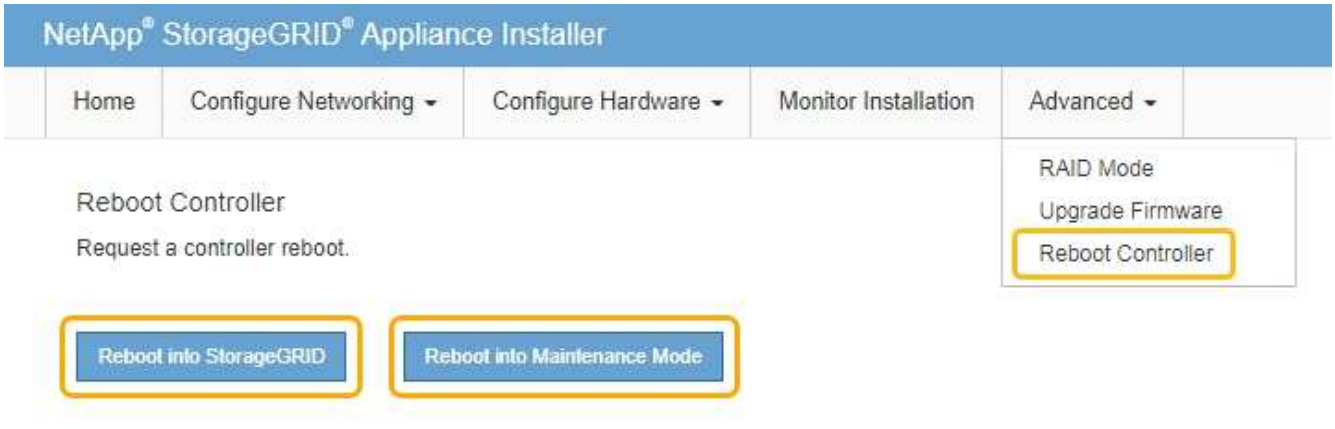
6. Para acceder al instalador de dispositivos de StorageGRID, busque cualquiera de las direcciones URL que se muestren.

Si es posible, utilice la dirección URL que contiene la dirección IP del puerto de red de administración del dispositivo.

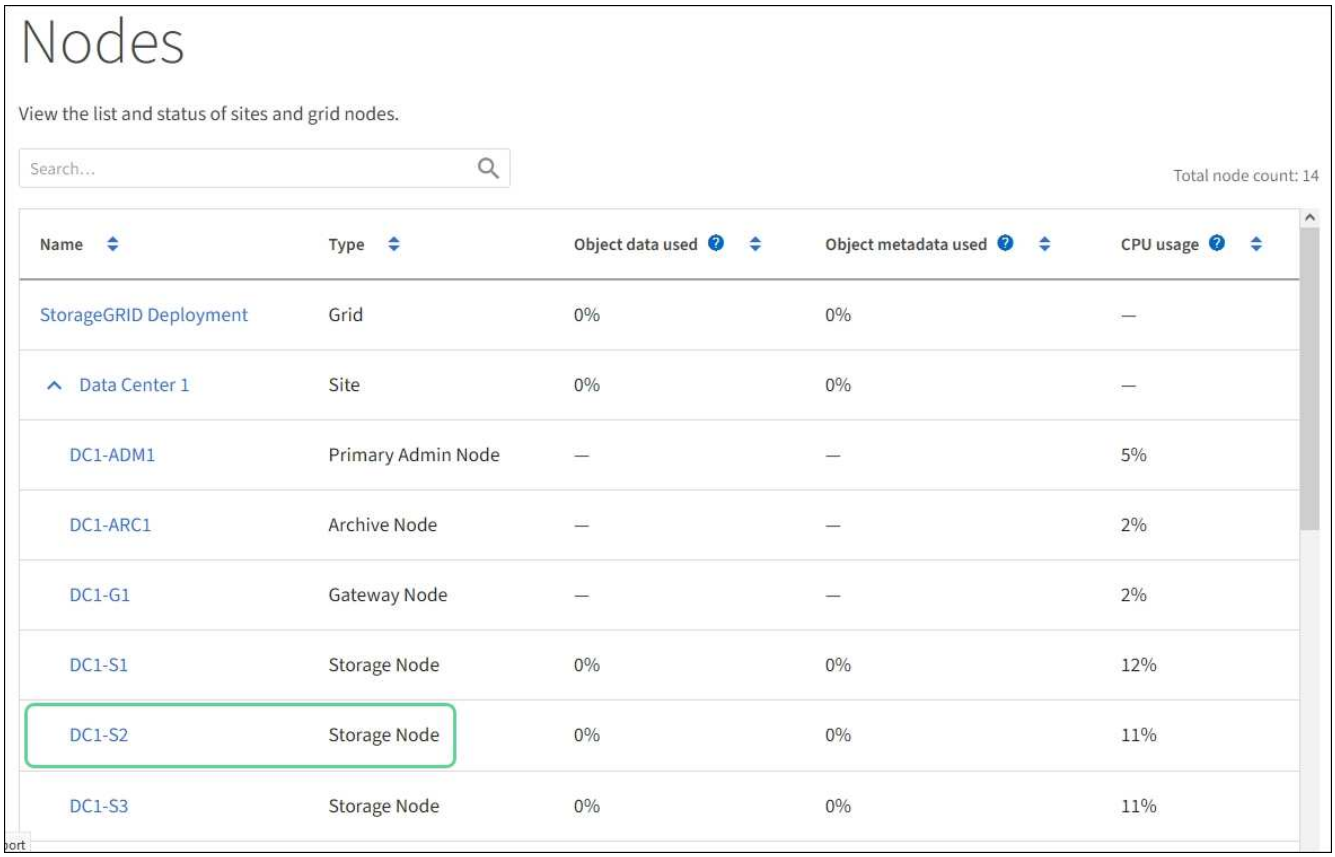
> Acceso `https://169.254.0.1:8443` requiere una conexión directa con el puerto de gestión local.

7. En el instalador de dispositivos StorageGRID, confirme que el dispositivo está en modo de mantenimiento.

8. Realice las tareas de mantenimiento necesarias.
9. Después de completar las tareas de mantenimiento, salga del modo de mantenimiento y reanude el funcionamiento normal del nodo. En el instalador del dispositivo StorageGRID, seleccione **Avanzado** > **Reiniciar controlador** y, a continuación, seleccione **Reiniciar en StorageGRID**.



El dispositivo puede tardar hasta 20 minutos en reiniciarse y volver a unirse a la cuadrícula. Para confirmar que el reinicio ha finalizado y que el nodo ha vuelto a unirse a la cuadrícula, vuelva a Grid Manager. La página **Nodes** debe mostrar un estado normal (no hay iconos a la izquierda del nombre del nodo) para el nodo del dispositivo, lo que indica que no hay alertas activas y que el nodo está conectado a la cuadrícula.



Fuerce el servicio para terminar

Si necesita detener un servicio inmediatamente, puede utilizar `force-stop` comando.

Lo que necesitará

Debe tener 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.

Lo que necesitará

Debe tener 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`

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 información sobre la configuración de puntos finales del equilibrador de carga, consulte las instrucciones para administrar StorageGRID.

Si el remasterp de puertos proporciona acceso al cliente, debe volver a configurarse el cliente para utilizar un puerto diferente configurado como extremo de equilibrio de carga si es posible, para evitar la pérdida del servicio. De lo contrario, si se elimina la asignación de puertos se producirá una pérdida de acceso al cliente y se debe programar adecuadamente.

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. Reiniciar el nodo.

   Siga las instrucciones para reiniciar un nodo de cuadrícula.

4. Repita estos pasos en cada nodo de administrador y nodo de puerta de enlace que tenga puertos reasignados en conflicto.

Información relacionada

Administre StorageGRID

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. 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.

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 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.

Reinicie el nodo de cuadrícula

Puede reiniciar un nodo de cuadrícula desde Grid Manager o desde el shell de comandos del nodo.

Acerca de esta tarea

Cuando reinicia un nodo de cuadrícula, el nodo se apaga y se reinicia. Todos los servicios se reinician automáticamente.

Si planea reiniciar nodos de almacenamiento, tenga en cuenta lo siguiente:

- Si una regla de ILM especifica un comportamiento de procesamiento del COMMIT doble o la regla especifica un equilibrio y no es posible crear de inmediato todas las copias necesarias, StorageGRID confirma de inmediato cualquier objeto recién ingerido en dos nodos de almacenamiento en el mismo sitio y evalúa ILM más adelante. Si desea reiniciar dos o más nodos de almacenamiento en un sitio determinado, es posible que no pueda acceder a estos objetos durante el reinicio.
- 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.

Información relacionada

Administre StorageGRID

Reinicie el nodo de cuadrícula desde Grid Manager

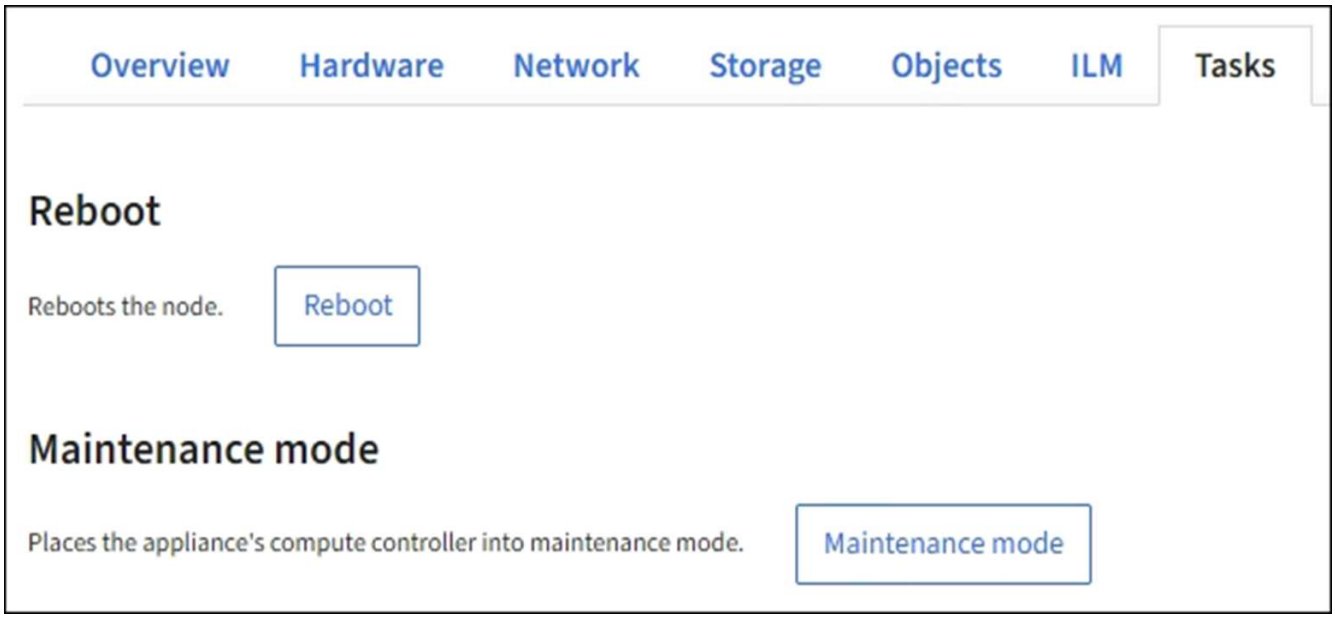
Reiniciar un nodo de cuadrícula desde Grid Manager emite el `reboot` en el nodo de destino.

Lo que necesitará

- Ha iniciado sesión en Grid Manager mediante un navegador web compatible.
- Tiene el permiso de mantenimiento o acceso raíz.
- Tiene la clave de acceso de aprovisionamiento.

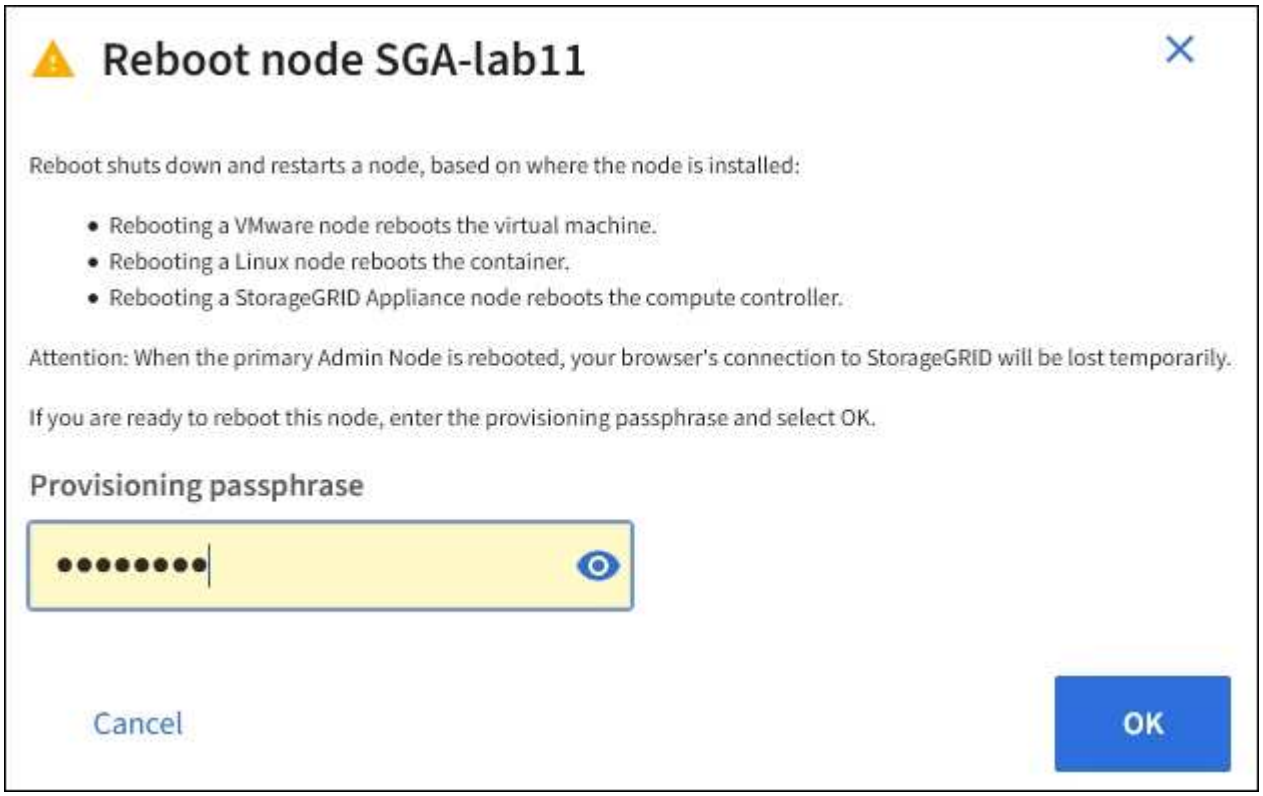
Pasos

1. Seleccione **NODES**.
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 haga clic en **Aceptar**.
6. Espere a que se reinicie el nodo.

El apagado de los servicios puede llevar cierto tiempo.

Cuando el nodo se está reiniciando, el icono gris (administrativamente abajo) aparece en el lado izquierdo de la página **Nodes**. Una vez que todos los servicios se han iniciado de nuevo y el nodo se ha conectado correctamente a la cuadrícula, la página * Nodes* debe mostrar un estado normal (no hay iconos a la izquierda del nombre del nodo), lo que indica que no hay alertas activas y que el nodo está conectado a la cuadrícula.

Reinicie el nodo de cuadrícula desde el shell de comandos

Si necesita supervisar más de cerca la operación de reinicio o si no puede acceder a Grid Manager, puede iniciar sesión en el nodo de cuadrícula y ejecutar el comando de reinicio de Server Manager desde el shell de comandos.

Debe tener la `Passwords.txt` archivo.

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.

Lo que necesitará

- Debe tener 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 el soporte técnico le indique explícitamente que lo haga.
- 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 procesamiento **Commit** dual (o si una regla usa la opción **balanced** y todas las copias necesarias no se pueden crear inmediatamente), StorageGRID confirma inmediatamente cualquier objeto recién ingerido a dos nodos de almacenamiento del mismo sitio y evalúa ILM más adelante. 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.

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 de dispositivo:
   - Para el dispositivo de servicios SG100 o SG1000
     i. Apague el aparato.
     ii. Espere a que se apague el LED de alimentación azul.
   - Para el dispositivo SG6000
     i. 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.

ii. Apague el aparato y espere a que se apague el LED de alimentación azul.

- Para el dispositivo SG5700

  i. 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.

  ii. Apague el aparato y espere a que todos los LED y la actividad de visualización de siete segmentos se detengan.

Información relacionada

Administre StorageGRID

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 de dispositivo:
   - Para el dispositivo de servicios SG100 o SG1000
     i. Apague el aparato.
     ii. Espere a que se apague el LED de alimentación azul.
   - Para el dispositivo SG6000
     i. 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.

     ii. Apague el aparato y espere a que se apague el LED de alimentación azul.
   - Para el dispositivo SG5700
     i. 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.

     ii. Apague el aparato y espere a que todos los LED y la actividad de visualización de siete segmentos se detengan.
7. Cierre la sesión del shell de comandos: `exit`

Información relacionada

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

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 los servicios en los nodos de administrador y los nodos de puerta de enlace de API en primer lugar, y 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 grid, no apague el host hasta que se hayan 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:
   - Para el dispositivo de servicios SG100 o SG1000
     i. Apague el aparato.
     ii. Espere a que se apague el LED de alimentación azul.
   - Para el dispositivo SG6000
     i. 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.

     ii. Apague el aparato y espere a que se apague el LED de alimentación azul.
   - Para el dispositivo SG5700
     i. 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.

     ii. 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.

Información relacionada

Servicios de aplicaciones SG100 y SG1000

Dispositivos de almacenamiento SG6000

Dispositivos de almacenamiento SG5700

Inicie nodos de grid

Siga esta secuencia para iniciar los nodos de cuadrícula después de un apagado completo.

> **Lo que necesite,#8217;más**
>
> 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 realizar los procedimientos de recuperación que reconstruyan los datos de Cassandra. Si lo hace, se puede producir la pérdida de datos.

Acerca de esta tarea

Si es posible, debe encender los nodos de grid en el siguiente 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

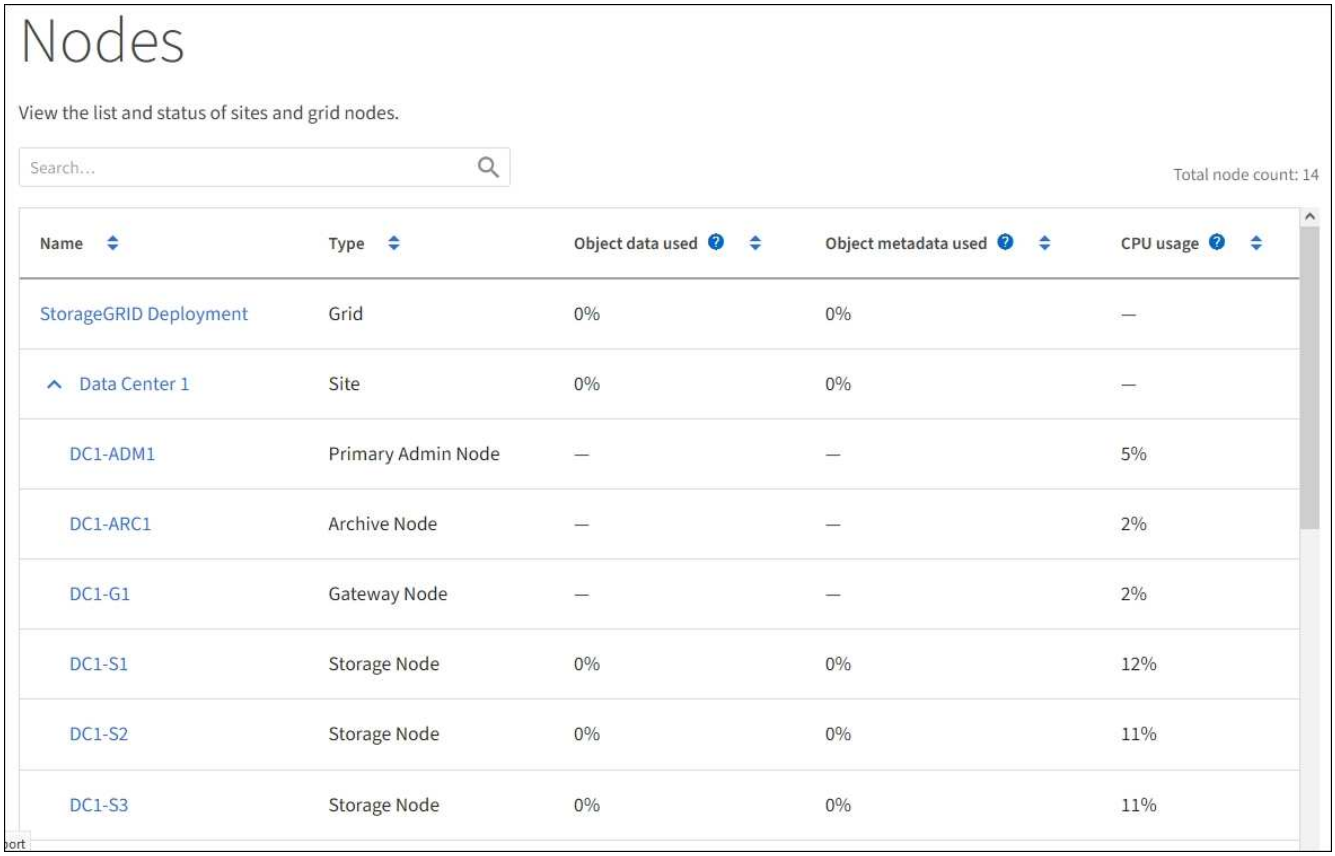
1. Encienda los hosts del nodo de administrador principal y los nodos de administrador que no son primarios.

   > 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.



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 al quitar 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 está en ejecución.

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.

Lo que necesitará

Debe tener 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.

Lo que necesitará

Debe tener 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

Acceda al archivo de registro 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.

Lo que necesitará

Debe tener 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`

Clonado de nodos de dispositivos

Puede clonar un nodo de dispositivo en StorageGRID para usar un dispositivo de diseño más reciente o más capacidades. La clonación transfiere toda la información del nodo existente al nuevo dispositivo, ofrece un proceso de actualización de hardware que es fácil de realizar y ofrece una alternativa al decomisionado y expansión para sustituir dispositivos.

Funcionamiento del clonado de nodos de dispositivos

El clonado de nodos de dispositivos le permite sustituir fácilmente un nodo de dispositivos (origen) existente en el grid por un dispositivo compatible (destino) que forma parte del mismo sitio lógico de StorageGRID. El proceso transfiere todos los datos

al dispositivo nuevo, situándolos en servicio para sustituir el nodo de dispositivo antiguo y dejar el dispositivo antiguo en estado previo a la instalación.

¿Por qué se debe clonar un nodo de dispositivo?

Puede clonar un nodo de dispositivo si necesita:

- Sustituya los aparatos que están llegando al final de su vida útil.
- Actualice los nodos existentes para aprovechar la tecnología de dispositivos mejorada.
- Aumente la capacidad de almacenamiento Grid sin cambiar el número de nodos de almacenamiento en el sistema StorageGRID.
- Mejore la eficiencia del almacenamiento, como, por ejemplo, cambiando el modo RAID de DDP-8 a DDP-16 o a RAID-6.
- Implementar de forma eficiente el cifrado de nodos para permitir el uso de servidores de gestión de claves externos (KMS).

¿Qué red StorageGRID se utiliza?

La clonación transfiere datos del nodo de origen directamente al dispositivo de destino mediante cualquiera de las tres redes de StorageGRID. La red de cuadrícula se utiliza normalmente, pero también puede utilizar la red de administración o la red de cliente si el dispositivo de origen está conectado a estas redes. Elija la red que se utilizará para clonar tráfico que ofrece el mejor rendimiento de transferencia de datos sin perjudicar el rendimiento de la red de StorageGRID y la disponibilidad de los datos.

Al instalar el dispositivo de repuesto, debe especificar direcciones IP temporales para la conexión StorageGRID y la transferencia de datos. Dado que el dispositivo de sustitución formará parte de las mismas redes que el nodo de dispositivo que sustituye, debe especificar direcciones IP temporales para cada una de estas redes en el dispositivo de reemplazo.

Compatibilidad con el dispositivo de destino

Los dispositivos de reemplazo deben ser del mismo tipo que el nodo origen que sustituyen y ambos deben formar parte del mismo sitio lógico de StorageGRID.

- Un dispositivo de servicios de sustitución puede ser diferente al nodo de administración o al nodo de puerta de enlace que va a sustituir.
  - Puede clonar un dispositivo de nodo de origen SG100 a un dispositivo de destino de servicios SG1000 para que tenga mayor capacidad para el nodo de administración o el nodo de puerta de enlace.
  - Puede clonar un dispositivo de nodo fuente SG1000 en un dispositivo objetivo de servicios SG100 para volver a instalar el SG1000 para una aplicación más exigente.

    Por ejemplo, si un dispositivo de nodo de origen SG1000 se está utilizando como nodo de administración y desea utilizarlo como nodo de equilibrio de carga dedicado.

  - La sustitución de un dispositivo de nodo de origen SG1000 por un dispositivo de destino de servicios SG100 reduce la velocidad máxima de los puertos de red de 100-GbE a 25-GbE.
  - Los aparatos SG100 y SG1000 tienen diferentes conectores de red. Puede que sea necesario cambiar el tipo de dispositivo reemplazando los cables o los módulos SFP.
- Un dispositivo de almacenamiento de reemplazo debe tener una capacidad igual o mayor que el nodo de almacenamiento al que desea reemplazar.

- Si el dispositivo de almacenamiento objetivo tiene la misma cantidad de unidades que el nodo de origen, las unidades del dispositivo objetivo deben tener mayor capacidad (en TB).
- Si planea utilizar el mismo modo RAID en el nodo de destino que se utilizó en el nodo de origen, O un modo RAID menos eficiente del almacenamiento (por ejemplo, al cambiar de RAID6 a DDP), las unidades del dispositivo de destino deben ser mayores (en TB) que las unidades del dispositivo de origen.
- Si la cantidad de unidades estándar instaladas en un dispositivo de almacenamiento de destino es menor que la cantidad de unidades en el nodo de origen, debido a la instalación de unidades de estado sólido (SSD), la capacidad de almacenamiento general de las unidades estándar en el dispositivo de destino (en TB). Debe satisfacer o superar la capacidad total de las unidades funcionales de todas las unidades del nodo de almacenamiento de origen.

  Por ejemplo, cuando se clona un dispositivo de nodo de almacenamiento de origen SG5660 con 60 unidades en un dispositivo de destino SG6060 o SG6060X con 58 unidades estándar, se deben instalar unidades más grandes en el dispositivo de destino SG6060 o SG6060X antes de realizar el clonado para mantener la capacidad de almacenamiento. (Las dos ranuras de unidad que contienen SSD en el dispositivo de destino no están incluidas en la capacidad total del almacenamiento del dispositivo).

  Sin embargo, si un dispositivo de nodo de origen SG5660 de 60 unidades está configurado con DDP-8 de los pools de discos dinámicos de SANtricity, configurar un dispositivo de destino SG6060 o SG6060X de 58 unidades con DDP-16 puede hacer que el dispositivo SG6060X o SG606060X sea un destino de clonado válido debido a su mejora en la eficiencia del almacenamiento.

Puede ver información acerca del modo RAID actual del nodo del dispositivo de origen en la página **NODES** de Grid Manager. Seleccione la ficha **almacenamiento** del dispositivo.

¿Qué información no se clona?

Las siguientes configuraciones de dispositivos no se transfieren al dispositivo de reemplazo durante la clonación. Debe configurarlos durante la configuración inicial del dispositivo de reemplazo.

- Interfaz BMC
- Enlaces de red
- Estado de cifrado de nodos
- SANtricity System Manager (para nodos de almacenamiento)
- Modo RAID (para nodos de almacenamiento)

¿Qué problemas evitan la clonación?

Si se encuentra alguno de los siguientes problemas durante la clonado, el proceso de clonado se detiene y se genera un mensaje de error:

- Configuración de red incorrecta
- Falta de conectividad entre los dispositivos de origen y de destino
- Incompatibilidad de dispositivos de origen y de destino
- Para los nodos de almacenamiento, un dispositivo de sustitución con capacidad insuficiente

Debe resolver cada problema para que la clonación continúe.

Consideraciones y requisitos para el clonado de nodos de dispositivos

Antes de clonar un nodo de dispositivo, debe comprender las consideraciones y los requisitos.

Requisitos de hardware para el dispositivo de sustitución

Asegúrese de que el aparato de sustitución cumple los siguientes criterios:

- El nodo de origen (dispositivo que se va a reemplazar) y el dispositivo de destino (nuevo) deben ser del mismo tipo de dispositivo:
  - Solo puede clonar un dispositivo Admin Node o un dispositivo Gateway Node en un dispositivo de servicios nuevo.
  - Solo puede clonar un dispositivo Storage Node en un dispositivo de almacenamiento nuevo.
- Para dispositivos de nodo de administración o de nodo de puerta de enlace, el dispositivo del nodo de origen y el dispositivo de destino no tienen que ser del mismo tipo de dispositivo; sin embargo, puede que sea necesario cambiar el tipo de dispositivo y sustituir los cables o módulos SFP.

  Por ejemplo, puede sustituir un dispositivo de nodo SG1000 por un SG100 o sustituir un dispositivo SG100 por un dispositivo SG1000.

- En los dispositivos de nodo de almacenamiento, el dispositivo de nodo de origen y el dispositivo de destino no tienen por qué ser del mismo tipo de dispositivo; sin embargo, el dispositivo de destino debe tener una mayor capacidad de almacenamiento que el dispositivo de origen.

  Por ejemplo, es posible sustituir un dispositivo de nodo SG5600 por un dispositivo SG5700 o SG6000.

Póngase en contacto con su representante de ventas de StorageGRID, para obtener ayuda a la hora de elegir dispositivos de reemplazo compatibles para clonar nodos de dispositivos específicos en la instalación de StorageGRID.

Prepare para clonar un nodo de dispositivo

Debe tener la siguiente información antes de clonar un nodo de dispositivo:

- Obtenga una dirección IP temporal para la red de red de su administrador de red para utilizarla con el dispositivo de destino durante la instalación inicial. Si el nodo de origen pertenece a una red de administrador o una red de cliente, obtenga direcciones IP temporales para estas redes.

  Las direcciones IP temporales suelen estar en la misma subred que el dispositivo de nodo de origen que se clona y no se necesitan una vez que finalice la clonado. Los dispositivos de origen y destino deben conectarse al nodo de administrador principal de la StorageGRID para establecer una conexión de clonado.

- Determine qué red se utilizará para clonar tráfico de transferencia de datos que ofrezca el mejor rendimiento de transferencia de datos sin perjudicar el rendimiento de la red de StorageGRID ni la disponibilidad de los datos.

  > El uso de la red de administrador de 1 GbE para la transferencia de datos de clones provoca una clonación más lenta.

- Determinar si se usará el cifrado de nodos con un servidor de gestión de claves (KMS) en el dispositivo de destino, de manera que pueda habilitar el cifrado de nodos durante la instalación inicial del dispositivo de

destino antes de realizar el clonado. Puede comprobar si el cifrado de nodos está habilitado en el nodo del dispositivo de origen como se describe en la instalación del dispositivo.

El nodo de origen y el dispositivo de destino pueden tener diferentes configuraciones de cifrado del nodo. El cifrado y el descifrado de datos se realizan automáticamente durante la transferencia de datos y cuando el nodo objetivo se reinicia y se une a la cuadrícula.

  - Servicios de aplicaciones SG100 y SG1000
  - Dispositivos de almacenamiento SG5600
  - Dispositivos de almacenamiento SG5700
  - Dispositivos de almacenamiento SG6000

- Determine si el modo RAID del dispositivo de destino debe cambiarse desde su configuración predeterminada, por lo que puede especificar esta información durante la instalación inicial del dispositivo de destino antes de realizar la clonación. Puede ver información acerca del modo RAID actual del nodo del dispositivo de origen en la página **NODES** de Grid Manager. Seleccione la ficha **almacenamiento** del dispositivo.

  El nodo de origen y el dispositivo de destino pueden tener diferentes ajustes de RAID.

- Planifique el tiempo suficiente para completar el proceso de clonación de nodos. Es posible que se necesiten varios días para transferir datos desde un nodo de almacenamiento operativo a un dispositivo de destino. Programe la clonación en el momento que minimice el impacto en su negocio.
- Solo debe clonar un nodo de dispositivo cada vez. La clonado puede evitar que ejecute otras funciones de mantenimiento de StorageGRID al mismo tiempo.
- Después de clonar un nodo de dispositivo, puede usar el dispositivo de origen que volvió a su estado de instalación previa como destino para clonar otro dispositivo de nodo compatible.

Clone el nodo del dispositivo

El proceso de clonado puede tardar varios días en transferir datos entre el nodo de origen (dispositivo que se va a reemplazar) y el dispositivo de destino (nuevo).

Lo que necesitará

- Instaló el dispositivo de destino compatible en un armario o rack, conectó todos los cables y aplicó la alimentación.
- Ha verificado que la versión del instalador de dispositivos StorageGRID en el dispositivo de reemplazo coincide con la versión de software del sistema StorageGRID, actualizando el firmware del instalador de dispositivos StorageGRID, si es necesario.
- Configuró el dispositivo de destino, incluida la configuración de conexiones StorageGRID, SANtricity System Manager (solo dispositivos de almacenamiento) y la interfaz BMC.
  - Al configurar las conexiones StorageGRID, utilice las direcciones IP temporales.
  - Al configurar los enlaces de red, utilice la configuración del enlace final.

> Deje el instalador de dispositivos StorageGRID abierto después de completar la configuración inicial del dispositivo de destino. Volverá a la página de instalador del dispositivo de destino después de iniciar el proceso de clonado del nodo.

- Opcionalmente, ha habilitado el cifrado de nodos para el dispositivo de destino.

- Opcionalmente ha configurado el modo RAID para el dispositivo de destino (solo dispositivos de almacenamiento).
- Consideraciones y requisitos para el clonado de nodos de dispositivos

  Servicios de aplicaciones SG100 y SG1000

  Dispositivos de almacenamiento SG5600

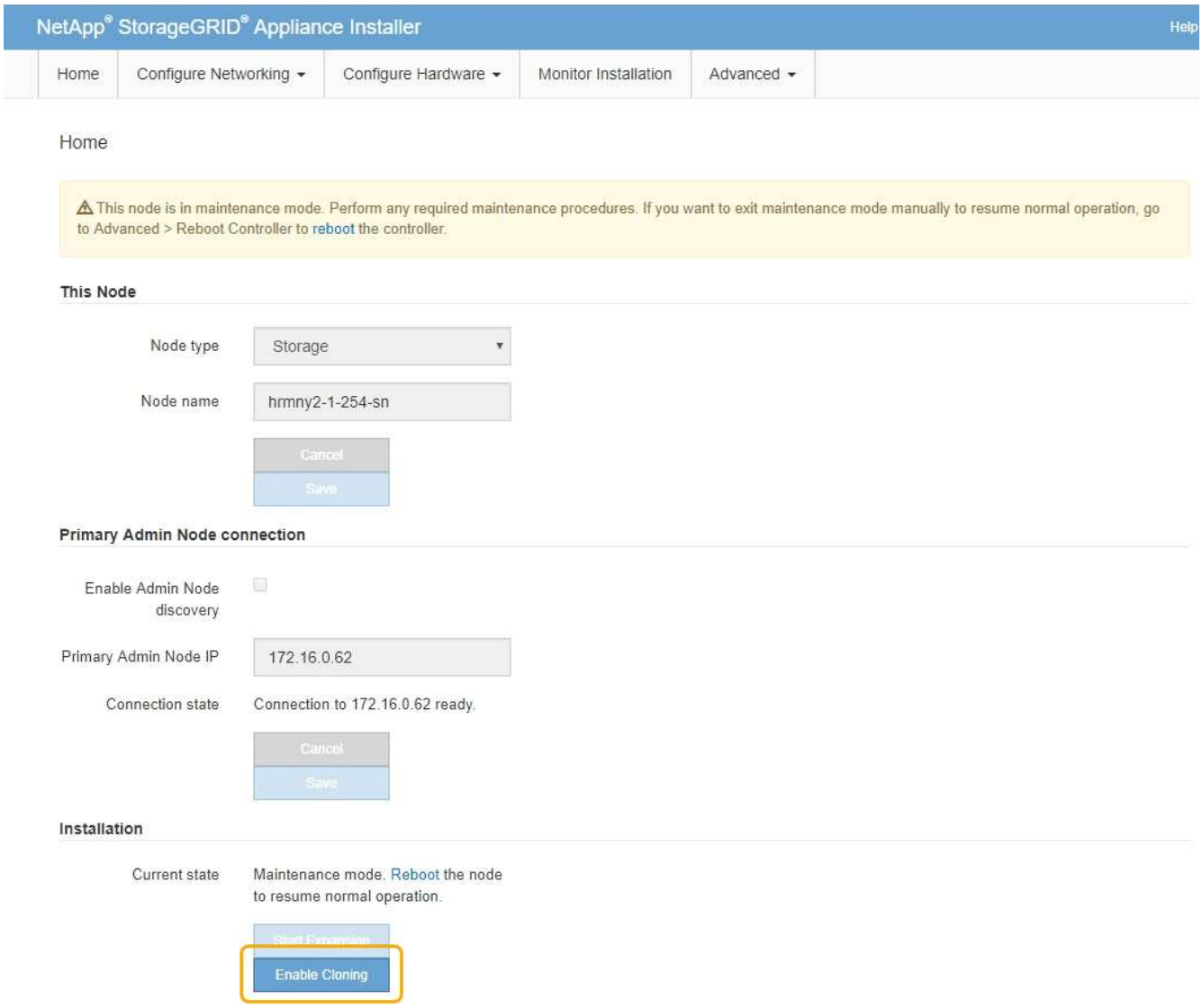
  Dispositivos de almacenamiento SG5700

  Dispositivos de almacenamiento SG6000

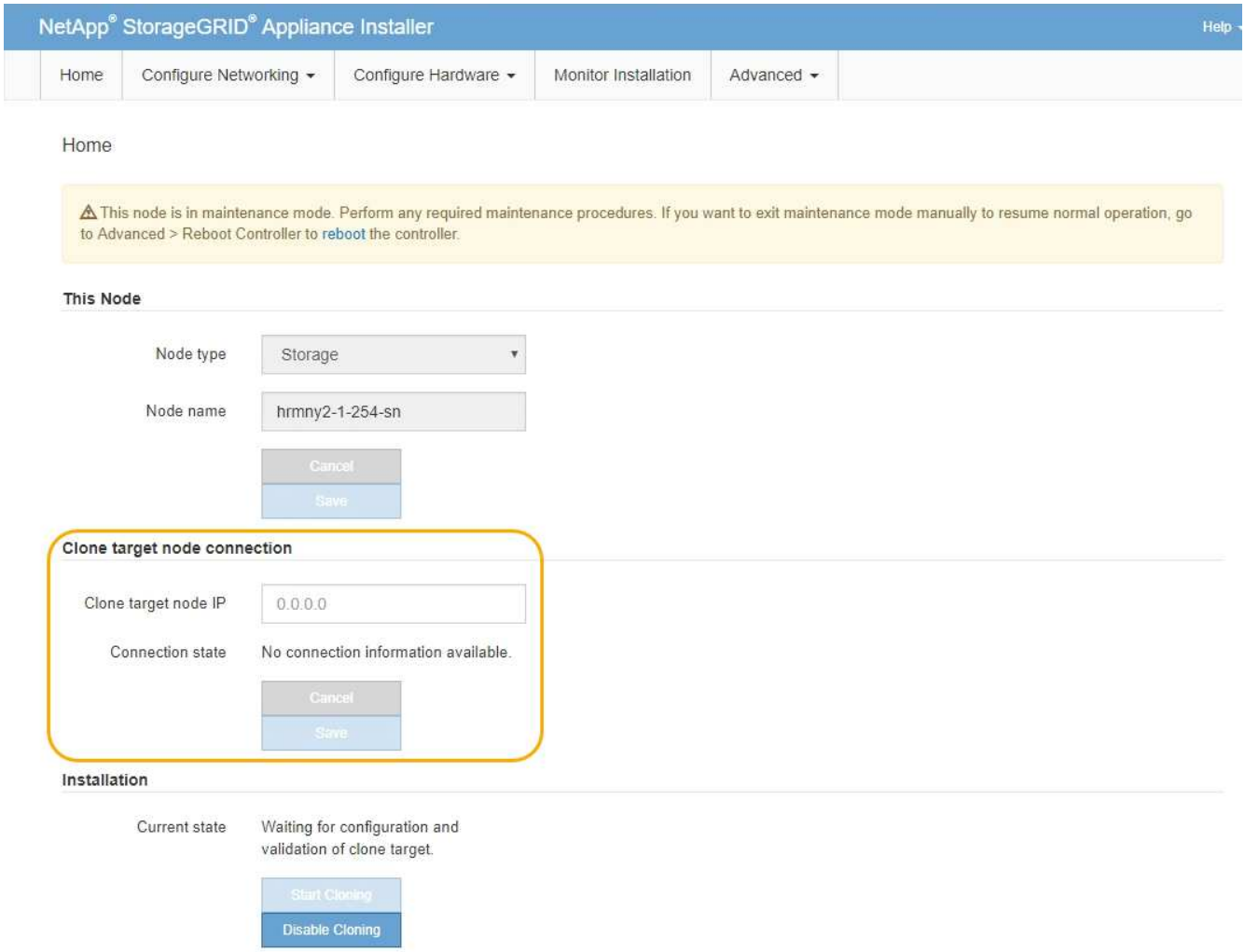
Solo debe clonar un nodo de dispositivo cada vez para mantener el rendimiento de la red StorageGRID y la disponibilidad de datos.

Pasos

1. Coloque el nodo de origen que está clonando en modo de mantenimiento.
2. En el instalador del dispositivo StorageGRID del nodo de origen, en la sección instalación de la página de inicio, seleccione **Activar clonación**.



La sección Primary Admin Node Connection se reemplaza por la sección Clone target node connection.

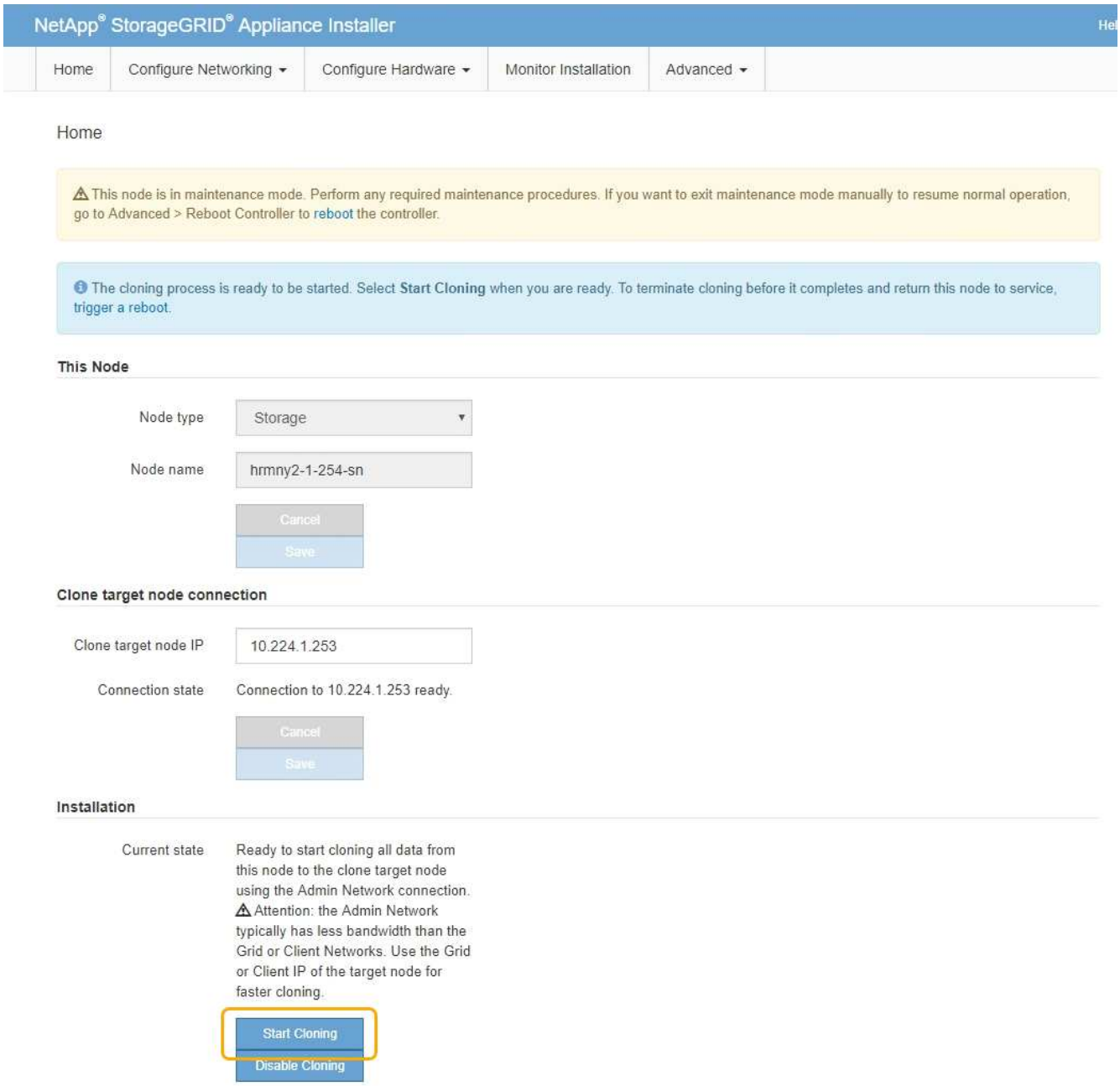


3. Para **Clone el nodo de destino IP**, introduzca la dirección IP temporal asignada al nodo de destino para que la red la utilice para clonar el tráfico de transferencia de datos y, a continuación, seleccione **Guardar**.

   Normalmente, introduzca la dirección IP para la red de cuadrícula, pero si necesita utilizar una red diferente para clonar tráfico de transferencia de datos, introduzca la dirección IP del nodo de destino en esa red.

   > El uso de la red de administrador de 1 GbE para la transferencia de datos de clones provoca una clonación más lenta.

   Después de configurar y validar el dispositivo de destino, en la sección instalación, **Iniciar clonación** se activa en el nodo de origen.



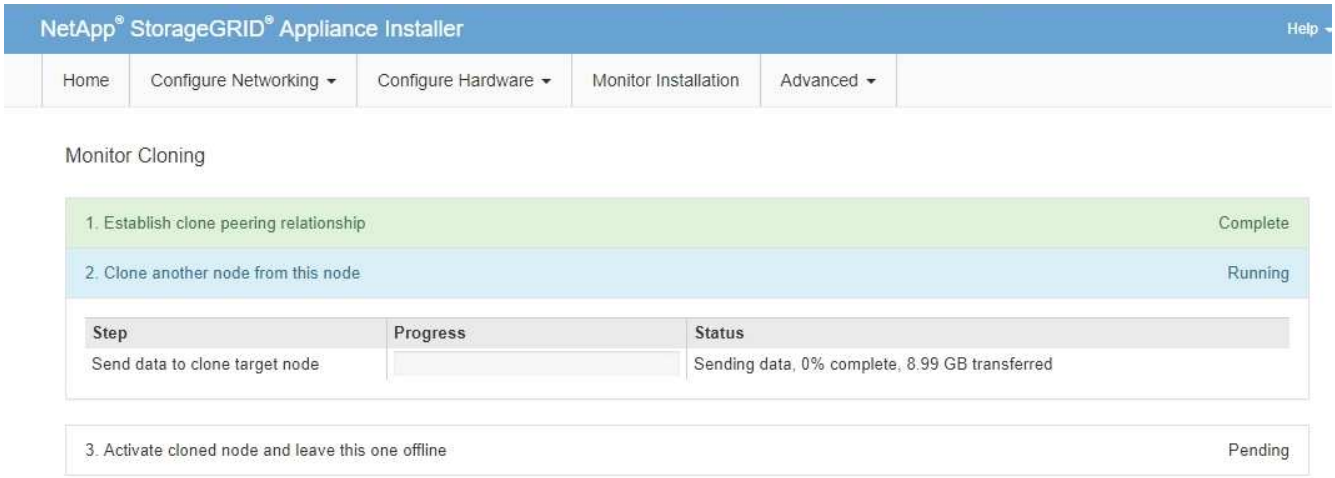
Si existen problemas que impiden la clonación, **Iniciar clonación** no está activado y los problemas que debe resolver se enumeran como **Estado de conexión**. Estos problemas se enumeran en la página inicial del instalador de dispositivos de StorageGRID tanto del nodo de origen como del dispositivo de destino. Sólo se muestra un problema a la vez y el estado se actualiza automáticamente a medida que cambian las condiciones. Resuelva todos los problemas de clonación para activar **Iniciar clonación**.

Cuando se activa **Iniciar clonación**, el **estado actual** indica la red StorageGRID que se seleccionó para clonar tráfico, junto con información acerca del uso de esa conexión de red.

Consideraciones y requisitos para el clonado de nodos de dispositivos

4. Seleccione **Iniciar clonación** en el nodo de origen.
5. Supervise el progreso de la clonación con el instalador de dispositivos de StorageGRID en el nodo de origen o de destino.

   El instalador de dispositivos StorageGRID en los nodos de origen y destino indica el mismo estado.



La página Monitor Cloning ofrece un progreso detallado de cada etapa del proceso de clonación:

- **Establecer relación de clonaciones** muestra el progreso de la configuración y la configuración de la clonación.
- **Clonar otro nodo de este nodo** muestra el progreso de la transferencia de datos. (Esta parte del proceso de clonación puede tardar varios días en completarse).
- **Activar el nodo clonado y dejar este fuera de línea** muestra el progreso de transferir el control al nodo de destino y colocar el nodo de origen en un estado de preinstalación, una vez finalizada la transferencia de datos.

6. Si necesita terminar el proceso de clonación y devolver el nodo de origen al servicio antes de finalizar la clonación, en el nodo de origen vaya a la página principal del instalador de dispositivos StorageGRID y seleccione **Avanzado Reiniciar controlador** y, a continuación, seleccione **Reiniciar en StorageGRID**.

   Si finaliza el proceso de clonación:

   - El nodo de origen sale del modo de mantenimiento y se vuelve a unir a StorageGRID.
   - El nodo de destino permanece en el estado previo a la instalación. Para reiniciar la clonación del nodo de origen, inicie de nuevo el proceso de clonación desde el paso 1.

Cuando finalice correctamente la clonación:

- Los nodos de origen y destino intercambian direcciones IP:
  - El nodo de destino utiliza ahora las direcciones IP asignadas originalmente al nodo de origen para las redes Grid, Admin y Client.
  - El nodo de origen ahora utiliza la dirección IP temporal asignada inicialmente al nodo de destino.
- El nodo de destino sale del modo de mantenimiento y se une a StorageGRID, sustituyendo el nodo de origen.
- El dispositivo de origen está en estado preinstalado, como si lo hubiera hecho lo preparó para su reinstalación.

> Si el dispositivo no vuelve a unirse a la cuadrícula, vaya a la página de inicio del instalador de dispositivos StorageGRID correspondiente al nodo de origen, seleccione **Avanzado Reiniciar controlador** y, a continuación, seleccione **Reiniciar en modo de mantenimiento**. Cuando el nodo de origen se reinicie en modo de mantenimiento, repita el procedimiento de clonado del nodo.

Los datos de usuario permanecen en el dispositivo de origen como opción de recuperación si se produce un problema inesperado en el nodo de destino. Una vez que el nodo de destino se ha vuelto a unir correctamente a StorageGRID, los datos del usuario en el dispositivo de origen están obsoletos y ya no se necesitan. Si lo desea, pida al soporte de StorageGRID que borre el dispositivo de origen para destruir estos datos.

Podrá:

- Utilice el dispositivo de origen como destino para las operaciones de clonado adicionales: No se requiere ninguna configuración adicional. Este dispositivo ya tiene la dirección IP temporal asignada que se especificó originalmente para el primer destino clonado.
- Instale y configure el dispositivo de origen como un nuevo nodo del dispositivo.
- Deseche el aparato de origen si ya no se utiliza con StorageGRID.

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 los 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.

Información relacionada

- Administre StorageGRID

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.

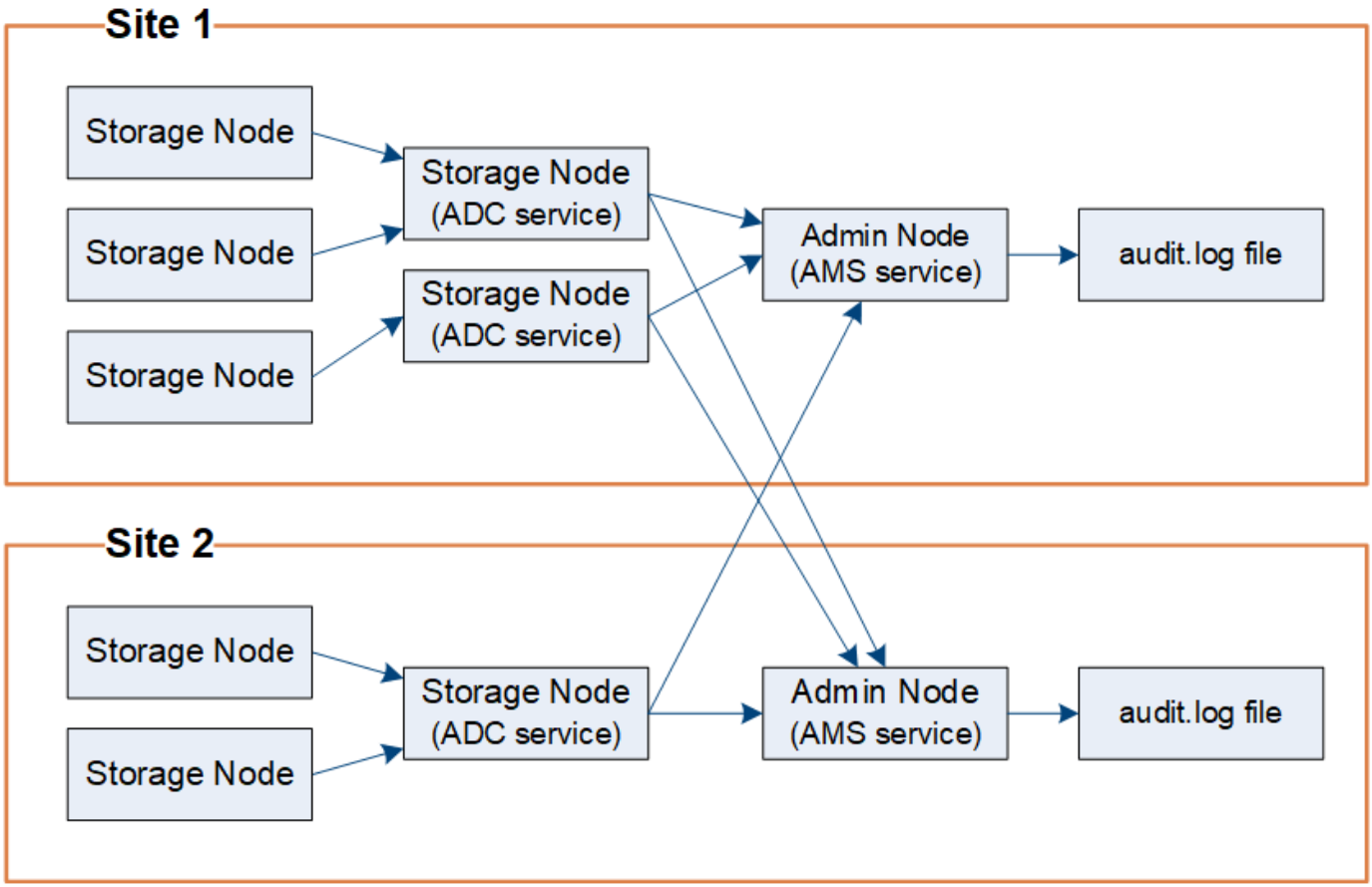
Flujo de mensajes de auditoría

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.

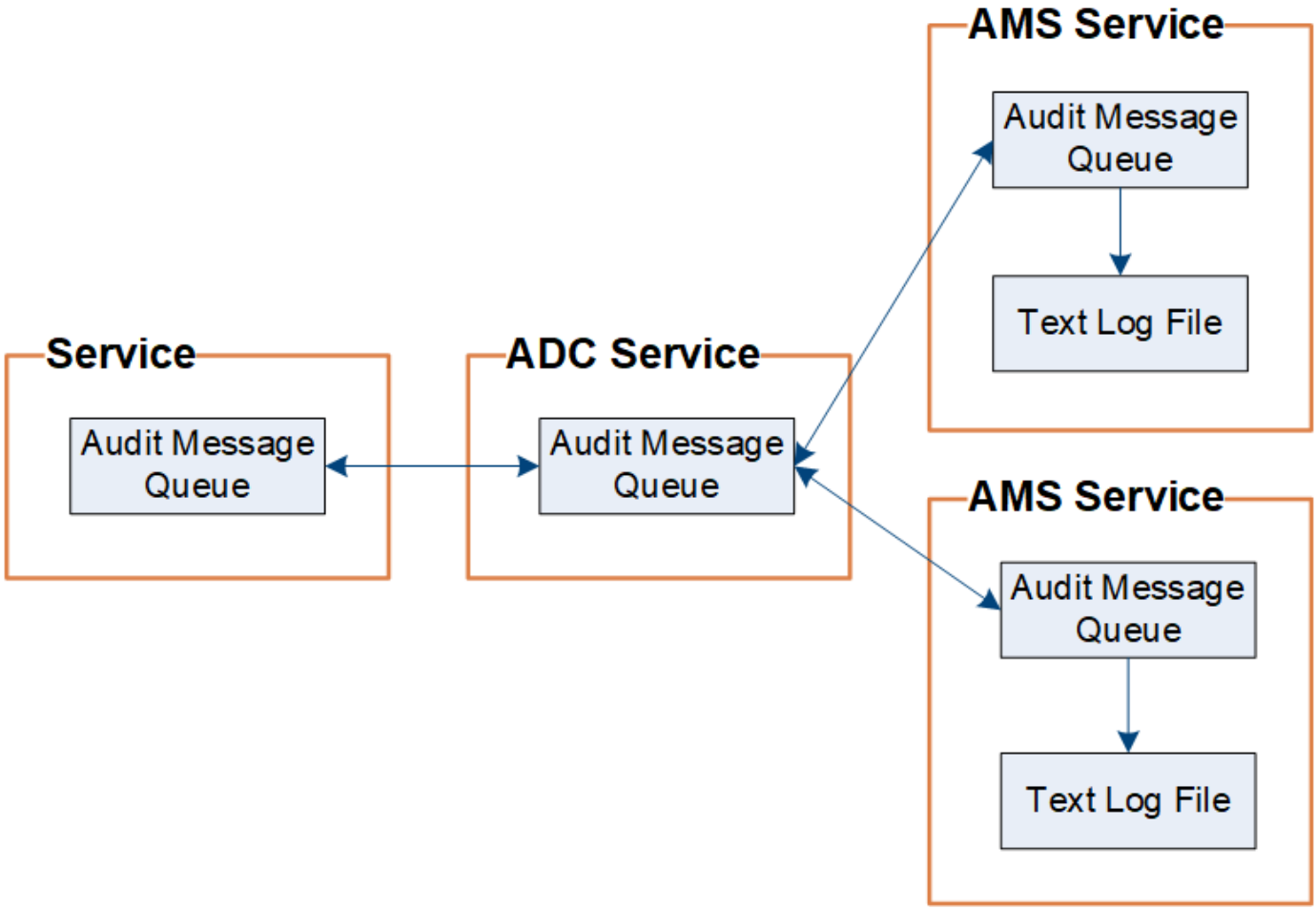
Cada nodo de administración almacena mensajes de auditoría en archivos de registro de texto; se asigna el nombre al archivo de registro activo `audit.log`.



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/audit/export` directorio. Esto ayuda a evitar la pérdida de un mensaje de auditoría durante el transporte.



La cola de mensajes de auditoría puede aumentar temporalmente debido a problemas de conectividad de red o capacidad de auditoría insuficiente. A medida que aumentan las colas, consumen más espacio disponible en cada nodo `/var/local/` directorio. Si el problema persiste y el directorio de mensajes de auditoría de un nodo 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/audit/export` 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 los 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 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. Para facilitar el acceso a los registros de auditoría, es posible configurar el acceso de clientes a recursos compartidos de auditoría de NFS y CIFS (CIFS está obsoleto). También es posible acceder a los archivos del registro de auditoría directamente desde la línea de comandos del nodo de administración.

Lo que necesitará

- Debe tener 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.

2. Vaya al directorio que contiene los archivos del registro de auditoría:

```
cd /var/local/audit/export
```

3. Ver el archivo de registro de auditoría actual o guardado, según sea necesario.

Información relacionada

Administre StorageGRID

Rotación del archivo de registro de auditoría

Los archivos de registros de auditoría se guardan en un nodo administrador `/var/local/audit/export` 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/audit/export` 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
```

Formatos de archivo y mensaje de registro de auditoría

Puede usar los registros de auditoría para recopilar información sobre el sistema y solucionar problemas. Debe comprender el formato del archivo de registro de auditoría y el formato general que se utiliza para los mensajes de auditoría.

Formato del archivo de registro de auditoría

Los archivos de registro de auditoría se encuentran en cada nodo de administrador y contienen una colección de mensajes de auditoría individuales.

Cada mensaje de auditoría contiene lo siguiente:

- Hora universal coordinada (UTC) del evento que activó el mensaje de auditoría (ATIM) en formato ISO 8601, seguido de un espacio:

  YYYY-MM-DDTHH:MM:SS.UUUUUU, donde *UUUUUU* 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]]
```

Con su formato predeterminado, los mensajes de auditoría de los archivos de registro de auditoría no son fáciles de leer ni interpretar. Puede utilizar el `audit-explain` herramienta para obtener resúmenes simplificados de los mensajes de auditoría en el registro de auditoría. Puede utilizar el `audit-sum` herramienta para resumir cuántas operaciones de escritura, lectura y eliminación se han registrado y cuánto tiempo duraron estas operaciones.

Información relacionada

Utilice la herramienta de explicación de auditoría

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.

Lo que necesitará

- Debe tener 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 mensajes de auditoría SPUT se generaron cuando el inquilino S3 con ID de cuenta 92484777680322627870 utilizó solicitudes PUT de S3 para crear un bloque llamado "bucket1" y añadió 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 procesar registros de auditoría sencillos o comprimidos. Por ejemplo:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

La `audit-explain` la herramienta también puede procesar varios archivos a la vez. Por ejemplo:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

Por último, la `audit-explain` la herramienta puede aceptar la entrada de una tubería, lo que le permite filtrar y preprocesar la entrada mediante `grep` comando u otros medios. Por ejemplo:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Como los registros de auditoría pueden ser muy grandes y lentos de análisis, puede ahorrar tiempo al filtrar 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.
2. Introduzca el comando siguiente, donde `/var/local/audit/export/audit.log` representa el nombre y la ubicación del archivo o archivos que desea analizar:

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   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 legibilidad, las marcas de tiempo no se muestran de forma predeterminada. Si desea ver las marcas de tiempo, use la Marca de hora (`-t`) opción.

Información relacionada

SPUT: S3 PUT

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.

Lo que necesitará

- Debe tener 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

Codificación	Descripción	Consulte
IDEL	ILM Initiated Delete: Registra cuando ILM inicia el proceso de eliminación de un objeto.	IDEL: Eliminación de ILM iniciada
SDEL	S3 DELETE: Registra una transacción realizada correctamente para eliminar un objeto o bloque.	SDEL: ELIMINACIÓN DE S3
SGET	S3 GET: Registra una transacción realizada correctamente para recuperar un objeto o enumerar los objetos de un bloque.	SGET: S3 GET
SHEA	S3 HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o bloque.	SHEA: CABEZA S3
SPUT	S3 PUT: Registra una transacción realizada correctamente para crear un nuevo objeto o bloque.	SPUT: S3 PUT
¡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 procesar registros de auditoría sencillos o comprimidos. Por ejemplo:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

La `audit-sum` la herramienta también puede procesar varios archivos a la vez. Por ejemplo:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

Por último, la `audit-sum` la herramienta también puede aceptar la entrada de una tubería, lo que le permite filtrar y preprocesar la entrada mediante la `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.
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/audit/export/audit.log` representa el nombre y la ubicación del archivo o archivos que desea analizar:

```
$ audit-sum /var/local/audit/export/audit.log
```

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 `audit-explain` Herramienta 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
```

Información relacionada

Utilice la herramienta de explicación de auditoría

Formato de mensaje de auditoría

Los mensajes de auditoría intercambiados dentro del sistema StorageGRID incluyen información estándar común a todos los mensajes y contenido específico que describe el evento o la actividad que se está reportando.

Si la información resumida proporcionada por el `audit-explain` y.. `audit-sum` 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 datos CSTR están rodeados por comillas dobles `" "`.

Información relacionada

Utilice la herramienta de explicación de auditoría

Utilice la herramienta de suma de auditoría

Auditar mensajes

Elementos comunes de los mensajes de auditoría

Tipos de datos

Ejemplos de mensajes de auditoría

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 de 32-bits sin signo que se representa como cuatro caracteres ASCII, como "ABCD".
IPAD	Se usa para direcciones IP.

Tipo	Descripción
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-SUST08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]* *\[TIME\(UI64\):11454
60025621595611246499\[SUST08\[SAIP\(IPAD\):"10.224.0 60025621595611246499.100
60025621595611246499"\[S3AI\(ECSTR\):"CSTR\\\\"[CSTR\]][CSTR\\]][CSTR]\\\\[CSTR][CSTR]\\\\[CSTR][
CSTR][CSTR\\\\\\\\"[CSTR][CSTR][CSTR][CSTR\\\\\\\\\\\[CSTR][CSTR][CSTR][CSTR][CSTR][CSTR\\\\\\\\\\
\[CSTR][CSTR][CSTR][CSTR][CSTR][CSTR][CSTR][CSTR\\\\\\\\\\\\\\\[KJC][KJC\\\
15552417629170647261 12281045 1543998285921845 10 30720
```

La `ATYP` elemento (subrayado en el ejemplo) identifica qué evento generó el mensaje. Este mensaje de ejemplo incluye el código DE mensaje SHEA ([ATYP(FC32):SHEA]), que indica que se generó mediante una solicitud de ENCABEZADO S3 correcta.

Información relacionada

Elementos comunes de los mensajes de auditoría

Auditar mensajes

Elementos comunes de los mensajes de auditoría

Todos los mensajes de auditoría contienen los elementos comunes.

Codificación	Tipo	Descripción
EN MEDIO	FC32	ID de módulo: Identificador de cuatro-caracteres del ID de módulo que generó el mensaje. Indica el segmento de código en el que se generó el mensaje de auditoría.
ANID	UI32	Node ID: El ID del nodo de grid asignado al servicio que generó el mensaje. A cada servicio se le asigna un identificador único en el momento en que se configura e instala el sistema StorageGRID. Este ID no se puede cambiar.
ASES	UI64	Identificador de sesión de auditoría: En versiones anteriores, este elemento indicó la hora a la que se inicializó el sistema de auditoría después de que se iniciara el servicio. Este valor de tiempo se midió en microsegundos desde la época del sistema operativo (00:00:00 UTC el 1 de enero de 1970). **Nota:** este elemento es obsoleto y ya no aparece en los mensajes de auditoría.
ASQN	UI64	Recuento de secuencias: En versiones anteriores, este contador se ha incrementado para cada mensaje de auditoría generado en el nodo de cuadrícula (ANID) y se ha restablecido a cero en el reinicio del servicio. **Nota:** este elemento es obsoleto y ya no aparece en los mensajes de auditoría.
AID	UI64	ID de seguimiento: Identificador que comparte el conjunto de mensajes activados por un solo evento.
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-humano que aparece al principio del mensaje de auditoría en la `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: Un 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.

Codificación	Tipo	Descripción
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, que puede 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 de S3, que registra la ingesta de un objeto en un bloque.

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-humano del atributo ATIM del mensaje de auditoría:

```
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.

Información relacionada

SPUT: S3 PUT

Elementos comunes de los mensajes de auditoría

Auditar los mensajes y el ciclo de vida del objeto

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 (bloque de S3) o S3KY (clave S3)
Vinculación de operaciones de Swift	WCON (Swift Container) y/o WOBJ (Swift Object)
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.

Configuración de políticas de gestión del ciclo de vida de la información

Con la política de ILM predeterminada (copia básica 2), los datos de objetos se copian una vez para obtener un total de dos copias. Si la política de ILM requiere más de dos copias, habrá un conjunto adicional de mensajes CBRE, CBSE y SCMT para cada copia adicional. Para obtener más información sobre las políticas de ILM, consulte la información sobre la gestión de objetos con la gestión del ciclo de vida de la información.

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.

Información relacionada

Gestión de objetos con ILM

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

Codificación	Nombre	Descripción	Traza	Consulte
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 activa de ILM incluye la regla de stock ILM, realiza 2 copias.

> 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]]
```

Para los objetos codificados de borrado, el campo LOCS incluye el ID de perfil de código de borrado y el ID del grupo de código 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 DE ELIMINACIÓN de objeto 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 GET Object 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 GET Object para un objeto almacenado en un bloque que no poseen. 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 genera dos mensajes de auditoría: Uno que realiza la autorización de la solicitud Select de S3 (el campo S3SR se establece 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**).

```
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]]
```

Información relacionada

Configurar los mensajes de auditoría y los destinos de registro

Auditar mensajes

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. Este listado alfabético le permite encontrar información sobre mensajes específicos.

Los códigos de cuatro caracteres utilizados en este capítulo son los valores del ATYP encontrados 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 de syslog externo para la información de auditoría, consulte Configurar los

Auditar categorías de mensajes

Debería estar familiarizado con las diversas categorías dentro de las cuales se agrupan los mensajes de auditoría. Estos grupos se organizan en función de la clase de actividad que representa el mensaje.

Mensajes de auditoría del sistema

Debería estar familiarizado con los mensajes de auditoría que pertenecen a la categoría de auditoría del sistema. Se trata de eventos relacionados con el propio sistema de auditoría, los estados del nodo de grid, la actividad de tareas en todo el sistema (tareas de grid) y las operaciones de backup de servicio, para que pueda solucionar los problemas potenciales.

Codificación	Título del mensaje y descripción	Consulte
ECMC	Falta el 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 codificados de borrado
ECOC	Fragmento de datos con código de borrado dañado: Indica que se ha detectado un fragmento de datos con código de borrado dañado.	ECOC: Fragmento de datos codificados con borrado dañado
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

Codificación	Título del mensaje y descripción	Consulte
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
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
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
ORLM	Object Rules met: Los datos del objeto se almacenan según las reglas de ILM.	ORLM: Se cumplen las reglas de objeto
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

Codificación	Título del mensaje y descripción	Consulte
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
VLST	El volumen iniciado por el usuario perdió: El `/proc/CMSI/Volume_Lost` se ejecutó el comando.	VLST: Volumen iniciado por el usuario perdido

Información relacionada

LKCU: Limpieza de objetos sobrescritos

Mensajes de auditoría del almacenamiento de objetos

Debería estar familiarizado con los mensajes de auditoría que pertenecen a la categoría de auditoría de almacenamiento de objetos. Estos son eventos relacionados con el almacenamiento y la gestión de 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
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

Codificación	Descripción	Consulte
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

Codificación	Descripción	Consulte
CBSE	Objeto Send End: La entidad de origen completó una operación de transferencia de datos de un nodo de cuadrícula a un nodo de cuadrícula.	CBSE: Fin de envío de objeto
CBRE	Fin de recepción de objetos: La entidad de destino completó una operación de transferencia de datos de Grid-node hacia Grid-node.	CBRE: Fin de recepción de objeto
SCMT	Confirmación del almacén de objetos: Un bloque de contenido se almacenó y verificó completamente, y ahora se puede solicitar.	SCMT: 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
SGET	S3 GET: Registra una transacción realizada correctamente para recuperar un objeto o enumerar los objetos de un bloque. **Nota:** Si la transacción opera en un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	SGET: S3 GET
SHEA	S3 HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o bloque.	Cliente S3	SHEA: CABEZA S3

Codificación	Descripción	Utilizado por	Consulte
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 Clientes 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

Codificación	Descripción	Utilizado por	Consulte
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
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

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.
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	Identificador del volumen en el que se archivaron los datos.Si no se encuentra una ubicación de archivo para el contenido, se devuelve un ID de volumen de 0.
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.

Codificación	Campo	Descripción
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.

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.

Codificación	Campo	Descripción
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 ha finalizado debido a la recepción de datos dañados o no válidos (puede indicar manipulación).

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.

Codificación	Campo	Descripción
CTDR	Dirección de transferencia	Indica si la transferencia CBID se inició mediante inserción o se inició con extracción: INSERCIÓN: La entidad emisora solicitó la operación de transferencia. PULL: La entidad receptora solicitó la operación de transferencia.
CTSR	Entidad de origen	El ID de nodo de la fuente (remitente) de la transferencia CBID.
CTD	Entidad de destino	El ID de nodo del destino (receptor) de la transferencia CBID.
CTSS	Recuento de secuencias de inicio	Indica el primer recuento de secuencias solicitado. Si la transferencia se realiza correctamente, comienza a partir del número de secuencias.
CTE	Recuento de secuencias finales esperadas	Indica el último recuento de secuencias solicitado. Si se realiza correctamente, la transferencia se considera completa cuando se ha recibido este recuento de secuencias.
TRANSFORMACIÓN DIGITAL	Estado de inicio de transferencia	Estado en el momento en que se inició la transferencia: SUCS: La transferencia se inició correctamente.

Este mensaje de auditoría significa que se ha iniciado una operación de transferencia de datos nodo a nodo en un único elemento de contenido, según lo identifica su identificador de bloque de contenido. La operación solicita datos de "Start Sequence Count" a "Contador de secuencia final esperado". El envío y la recepción de nodos se identifican mediante sus ID de nodo. Esta información se puede utilizar para realizar un seguimiento del flujo de datos del sistema y, cuando se combina con mensajes de auditoría de almacenamiento, para comprobar el número de réplicas.

CBSE: Fin de envío de objeto

Cuando se completa la transferencia de un bloque de contenido de un nodo a otro, la entidad de origen emite este mensaje.

Codificación	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión nodo a nodo.
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido que se está transfiriendo.
CTDR	Dirección de transferencia	Indica si la transferencia CBID se inició mediante inserción o se inició con extracción: INSERCIÓN: La entidad emisora solicitó la operación de transferencia. PULL: La entidad receptora solicitó la operación de transferencia.
CTSR	Entidad de origen	El ID de nodo de la fuente (remitente) de la transferencia CBID.
CTD	Entidad de destino	El ID de nodo del destino (receptor) de la transferencia CBID.
CTSS	Recuento de secuencias de inicio	Indica el recuento de secuencias en el que se inició la transferencia.
CTA	Recuento de secuencias finales reales	Indica que el último número de secuencias se ha transferido correctamente. Si el recuento de secuencia final real es el mismo que el recuento de secuencia de inicio y el resultado de la transferencia no se realizó correctamente, no se intercambiaron datos.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Resultado de la transferencia	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 ha finalizado debido a la recepción de datos dañados o no válidos (puede indicar manipulación).

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.

ECMC: Falta el fragmento de datos codificados 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.

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.

ECOC: Fragmento de datos codificados con borrado dañado

Este mensaje de auditoría indica que el sistema ha detectado un fragmento de datos con código de borrado dañado.

Codificación	Campo	Descripción
VCCO	ID DEL VCS	El nombre del VCS que contiene el fragmento dañado.
VLID	ID del volumen	El volumen RangeDB que contiene el fragmento con código de borrado dañado.
CCID	ID de fragmento	El identificador del fragmento codificado por borrado dañado.
TRANSFORMACIÓN DIGITAL	Resultado	Este campo tiene el valor 'NONE'. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje en particular. 'NINGUNO' se utiliza en lugar de 'UCS' para que este mensaje no se filtre.

ETAF: Error de autenticación de seguridad

Este mensaje se genera cuando se produce un error en un intento de conexión mediante la seguridad de la capa de transporte (TLS).

Codificación	Campo	Descripción
CNID	Identificador de conexión	Identificador único del sistema para la conexión TCP/IP a través de la cual falló la autenticación.
RUID	Identidad del usuario	Identificador dependiente del servicio que representa la identidad del usuario remoto.

Codificación	Campo	Descripción
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.

Codificación	Campo	Descripción
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 se canceló sin un error de reversión. • ROLF: La tarea de cuadrícula se ha anulado y no ha podido completar el proceso de reversión. • 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.

Codificación	Campo	Descripción
TVER	Versión de la tarea	Número que indica la versión de la tarea de cuadrícula.
TDSC	Descripción de la tarea	Una descripción legible por el usuario de la tarea de cuadrícula.
VATS	Válido después de la Marca de hora	El primer momento (UINT64 microsegundos a partir del 1 de enero de 1970 - tiempo UNIX) en el que es válida la tarea de la cuadrícula.
VBTS	Válido antes de la Marca de hora	La última hora (UINT64 microsegundos a partir del 1 de enero de 1970 - tiempo UNIX) en la que es válida la tarea de la cuadrícula.
TSRC	Origen	El origen de la tarea: • 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 la política de ILM activa actualmente se aplican al objeto.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	El CBID del objeto.
CMPA	Cumplimiento: Eliminación automática	Para objetos solo en bloques de S3 que cumplen con la normativa. 0 (falso) o 1 (verdadero), que indica si un objeto compatible debe eliminarse automáticamente cuando finalice su período de retención, a menos que el segmento se encuentre bajo una retención legal.
CMPL	Cumplimiento: Conservación legal	Para objetos solo en bloques de S3 que cumplen con la normativa. 0 (falso) o 1 (verdadero), que indica si el cubo está actualmente bajo un derecho.
CMPR	Cumplimiento: Período de retención	Para objetos solo en bloques de S3 que cumplen con la normativa. La duración del período de retención del objeto en minutos.
CTME	Cumplimiento de normativas: Tiempo de consumo	Para objetos solo en bloques de S3 que cumplen con la normativa. Tiempo de procesamiento del objeto. Puede agregar el período de retención en minutos a este valor para determinar cuándo se puede eliminar el objeto del bloque.
DMRK	Eliminar ID de versión del marcador	El código de versión del marcador de borrado creado al eliminar un objeto de un bloque con versiones. Las operaciones en bloques no incluyen este campo.
CSIZ	Tamaño de contenido	El tamaño del objeto en bytes.

Codificación	Campo	Descripción
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: En lo que respecta a los objetos codificados de borrado, el ID de perfil de codificación de borrado y el ID de grupo de codificación de borrado que se aplican 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.
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 cubos 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 encuentre una ubicación para una copia de objeto (replicada o codificada a borrado).

Codificación	Campo	Descripción
CBIL	CBID	El CBID afectado.
NOID	ID del nodo de origen	El ID de nodo en el que se han perdido las ubicaciones.
UUID	ID único universal	El identificador del objeto afectado del sistema StorageGRID.
EPR	Perfil de código de borrado	Para datos de objetos codificados mediante borrado. El código del perfil de código de borrado utilizado.

Codificación	Campo	Descripción
LLEYP	Tipo de ubicación	CLDI (Online): Para datos de objeto replicados CLEC (en línea): Para datos de objetos codificados con borrado CLNL (Nearline): Para los datos de objetos replicados archivados
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

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.
MPAT	RUTA de la solicitud	La ruta de la solicitud.
MPQP	Solicitar parámetros de consulta	Los parámetros de consulta para la solicitud.

Codificación	Campo	Descripción
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.

Codificación	Campo	Descripción
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 "near" 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.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Resultado	Este campo no tiene el valor NONE. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. NO SE utiliza NINGUNO en lugar de SUCS para que este mensaje no se filtre.
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.
CSIZ	Tamaño de contenido	El tamaño del objeto en bytes.

Codificación	Campo	Descripción
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: En lo que respecta a los objetos codificados de borrado, el ID de perfil de codificación de borrado y el ID de grupo de codificación de borrado que se aplican 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.

Codificación	Campo	Descripción
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.

El mensaje de auditoría ORLM se puede emitir varias veces para un solo objeto. Por ejemplo, se emite siempre que se produce 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.

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 S3 emite una transacción DE ELIMINACIÓN, se realiza una solicitud para eliminar el objeto o bloque 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 bloques 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 bloques 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 bloques 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. **Nota:** `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 DE ELIMINACIÓN. El resultado es siempre: SUCS: Exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
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 bloques no incluyen este campo.

Codificación	Campo	Descripción
S3SR	Subrecurso de S3	El bloque o subrecurso de objeto en el que se opera, si procede.
SACC	Nombre de cuenta de inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de cuenta de inquilino de S3 (propietario del bloque)	El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del bloque)	El ID de cuenta de inquilino del propietario del bloque de destino. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SGRP	Planta (grupo)	Si está presente, el objeto se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto.
SUSR	URN de usuario de S3 (remitente de solicitudes)	El ID de cuenta de arrendatario y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: `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 eliminó. Las operaciones en cubos y objetos en cubos 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 bloque. 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 bloques no incluyen este campo.
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP de control de coherencia, si está presente en la solicitud.
CNID	Identificador de conexión	Identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes. Las operaciones en bloques 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. **Nota:** `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).
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

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 bloques 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.
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.

Codificación	Campo	Descripción
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 cubos 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 bloques 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 bloques no incluyen este campo.

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. **Nota:** `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 bloques 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.
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.

Codificación	Campo	Descripción
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 cubos 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.

Codificación	Campo	Descripción
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. **Nota:** `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 solicitud DE restauración DE objetos POSTERIOR. 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 bloques no incluyen este campo.
S3SR	Subrecurso de S3	El bloque o subrecurso de objeto en el que se opera, si procede. Establezca «seleccionados» para una operación de selección de S3.

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.
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.
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 cubos 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 bloque. 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 bloques no incluyen este campo.
CMPS	Configuración de cumplimiento de normativas	La configuración de cumplimiento utilizada al crear el segmento, si está presente en LA solicitud PUT Bucket (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 bloques 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. **Nota:** `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).
LKEN	Bloqueo de objeto activado	Valor de la cabecera de la solicitud `x-amz-bucket-object-lock-enabled`, Si está presente en la solicitud PUT Bucket.

Codificación	Campo	Descripción
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 PONER objeto.
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 PONER objeto.
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 PONER objeto.
MTME	Hora de la última modificación	La Marca de hora de Unix, en microsegundos, indica cuándo se modificó por última vez el objeto.
TRANSFORMACIÓN DIGITAL	Código de resultado	Resultado de la transacción PUT. El resultado es siempre: 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	S3KY	El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en bloques 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.

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.
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.
ID	ID de carga	Sólo se incluye en los mensajes SPUT para operaciones de carga de varias partes completas. Indica que todas las piezas se han cargado y ensamblado.
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 cubos 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: "Habilitado" o "suspendido". Las operaciones de los 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 bloques 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, 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 bloques 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. **Nota:** `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.

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 bloques 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.
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.

Codificación	Campo	Descripción
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 cubos 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.

Nota: este mensaje debe ser monitoreado de cerca. Los errores de verificación del contenido pueden indicar intentos de sabotaje a través de contenido o 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.

Nota: el SVRU: Almacén de objetos verificar mensaje de auditoría desconocido debe ser monitoreado 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 las tesis de que puede indicar intentos de detectar fallos de contenido o 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, ya que 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 sólo se genera 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 apagado "con errores", porque el mensaje sólo se genera 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.

VLST: Volumen iniciado por el usuario perdido

Este mensaje se emite siempre que la `/proc/CMSI/Volume_Lost` se ejecuta el comando.

Codificación	Campo	Descripción
VOLL	Identificador de volumen inferior	El extremo inferior del rango de volumen afectado o un único volumen.
VOLU	Identificador del volumen superior	El extremo superior del rango de volumen afectado. Igual A VOLL si se trata de un volumen único.
NOID	ID del nodo de origen	El ID de nodo en el que se han perdido las ubicaciones.
LLEYP	Tipo de ubicación	'CLDI' (en línea) o 'CLNL' (Nearline). Si no se especifica, el valor predeterminado es 'CLDI'.
TRANSFORMACIÓN DIGITAL	Resultado	Siempre 'NINGUNO'. 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.

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. Este campo no incluye las operaciones en contenedores.
CSIZ	Tamaño de contenido	El tamaño del objeto eliminado en bytes. Este campo no incluye las operaciones en contenedores.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. **Nota:** `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. Este campo no incluye las operaciones en contenedores.
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. Este campo no incluye las operaciones de las cuentas y los contenedores.
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes. Este campo no incluye las operaciones de las cuentas y los contenedores.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. **Nota:** `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.

Codificación	Campo	Descripción
WCON	Contenedor Swift	El nombre del contenedor Swift. Las operaciones en cuentas no incluyen este campo.
WOBJ	Objeto Swift	El identificador del objeto Swift. Este campo no incluye las operaciones de las cuentas y los contenedores.
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. Este campo no incluye las operaciones de las cuentas y los contenedores.
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes. Este campo no incluye las operaciones de las cuentas y los contenedores.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. **Nota:** `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).

Codificación	Campo	Descripción
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 cuentas no incluyen este campo.
WOBJ	Objeto Swift	El identificador del objeto Swift. Este campo no incluye las operaciones de las cuentas y los contenedores.
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. Este campo no incluye las operaciones en contenedores.
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes. Este campo no incluye las operaciones en contenedores.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. **Nota:** `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.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.

Codificación	Campo	Descripción
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. Este campo no incluye las operaciones en contenedores.
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.

Cómo habilitar StorageGRID en su entorno

Obtenga información sobre cómo probar y habilitar las aplicaciones en su entorno de StorageGRID.

Vaya a la "storagegrid-enable" sitio de documentos para encontrar ejemplos y libros de cocina que se amplían en la documentación del producto en este sitio. El sitio **storagegrid-enable** también describe algunos pasos siguientes para evaluar e integrar con StorageGRID.

Se incluye la siguiente información:

- Listas de soluciones de terceros validadas para versiones anteriores y actuales de StorageGRID.
- Guías de características de productos. Por ejemplo, estas guías proporcionan información detallada para la creación de pools de almacenamiento en cloud.
- 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 StorageGRID de NetApp aquí:

- "Documentación de StorageGRID 11,7"
- "Documentación de StorageGRID 11.5"
- "Documentación de StorageGRID 11.4"
- "Documentación de StorageGRID 11.3"
- "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/ECMLP2879263

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.